ESCUELA MILITAR DE INGENIERÍA
MCAL. ANTONIO JOSÉ DE SUCRE
BOLIVIA

MANUAL DE ADMINISTRACIÓN

DISEÑO DEL CENTRO DE RESPUESTAS A INCIDENTES DE SEGURIDAD INFORMÁTICA BAJO ESTÁNDARES INTERNACIONALES.

CASO: DIRECCIÓN NACIONAL DE INFORMÁTICA – ESCUELA MILITAR DE INGENIERÍA.

MY. ING. ERICK ROLANDO PALENQUE RIOS

LA PAZ, 2016

ESCUELA MILITAR DE INGENIERÍA
MCAL. ANTONIO JOSÉ DE SUCRE
BOLIVIA

MANUAL DE ADMINISTRACIÓN

DISEÑO DEL CENTRO DE RESPUESTAS A INCIDENTES DE SEGURIDAD INFORMÁTICA, BAJO ESTÁNDARES INTERNACIONALES

CASO: DIRECCIÓN NACIONAL DE INFORMÁTICA – ESCUELA MILITAR DE INGENIERÍA

MY. ING. ERICK ROLANDO PALENQUE RIOS

Trabajo de grado, presentado como requisito para optar al título de Licenciado en Ingeniería de Sistemas.

TUTOR: ING. MSC. PATRICIA LÓPEZ AVENDAÑO

LA PAZ, 2016

ÍNDICE DE CONTENIDO

Pag.

ADMINISTRACIÓN DEL CENTROS DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA

1.1 INTRODUCCIÓN.

La tecnología de la computación electrónica ha modificado de manera importante la forma de trabajar de toda la humanidad. La dependencia que tenemos en la actualidad de las computadoras es evidente. Sin embargo, los sucesos han ocurrido con tal rapidez que se requiere de un análisis formal para comprobar la magnitud de esa dependencia. Una manera drástica, pero muy objetiva de ilustrarla, sería imaginar lo que podría suceder si de un momento a otro se desconectaran todas las computadoras en el mundo. Los efectos serían más graves que los causados por una guerra. De inmediato, quedaríamos sin transportes ni comunicaciones, los bancos cerrarían y no habría dinero disponible, las transacciones comerciales quedarían prácticamente anuladas, la mayoría de las empresas dejarían de prestar sus servicios y muchas otras detendrían su producción, grandes redes de suministros de energía eléctricas quedarían desactivadas, los suministros de agua dejarían de operar, millones de personas quedarían inactivas, etcétera.

De ahí la importancia de las computadoras. Y si bien no llegara a suceder dicha catástrofe, es innegable la frecuencia con que somos víctimas de los errores que se cometen en los centros de cómputo. ¿Quién no ha perdido horas esperando a que se restablezcan los servicios de algún banco a fin de cobrar un cheque?, ¿Cuántas veces no hemos acudido a aclarar un recibo de cobro emitido erróneamente? Miles de trámites han quedado pendientes por falta de información oportuna.

Por tanto, no es admisible que si la función de un centro de cómputo es simplificar las labores administrativas, éstas en muchos casos terminen por ser más complicadas.

1.2 Administración.

La administración se define como el proceso de crear, diseñar y mantener un ambiente en el que las personas al laborar o trabajar en grupos, alcancen con eficiencia metas seleccionadas.

Las personas realizan funciones administrativas de planeación, organización, integración de personal, dirección y control.

- ✓ La administración se aplica en todo tipo de corporación.
- ✓ Es aplicable a los administradores en todos los niveles de corporación.
- ✓ La administración se ocupa del rendimiento; esto implica eficacia y eficiencia.

La administración en la era de la información se caracteriza por la simplicidad, agilidad, flexibilidad, excelencia y mejora continua.

1.2.1 Énfasis en la Calidad.

Según Edwads Deming, calidad es ofrecer productos y servicios a bajo costo que satisfagan necesidades de los clientes.

Técnicas de calidad:

- ✓ Benchmarking.
- ✓ Outsourcing
- ✓ Reducción del ciclo del trabajo.

1.2.2 Énfasis de los Recursos Intangibles.

Se caracteriza por tomar en consideración los siguientes aspectos:

- ✓ Importa el conocimiento y la información
- ✓ Activos intangibles es el capital intelectual.
- ✓ Difícil de identificar. Componentes del capital intelectual:
- ✓ Capital humano.
- ✓ Capital organizativo.
- ✓ Capital tecnológico.
- ✓ Capital de relaciones.

1.3 El Proceso Administrativo.

El proceso administrativo se define como el proceso metodológico que implica una serie de actividades que llevará a una mejor consecución de los objetivos, en un

periodo más corto y con una mayor productividad.

El proceso administrativo se dice que es multidimensional, porque sus elementos son aplicables a todas las funciones del organismo en todos sus niveles: Planeación, Organización, Dirección y Control.

1.3.1 Planeación.

Algunas definiciones de la planeación como parte de su significado pueden ser:

- ✓ Proceso por el cual se obtiene una visión del futuro, en donde es posible determinar y lograr los objetivos, mediante la elección de un curso de acción.
- ✓ Proceso que permite la identificación de oportunidades de mejoramiento en la operación de la organización con base en la técnica, así como el establecimiento formal de planes o proyectos para el aprovechamiento integral de dichas oportunidades.
- ✓ Es la función que tiene por objetivo fijar el curso concreto de acción que ha de seguirse, estableciendo los principios que habrán de orientarlo, la secuencia de operaciones para realizarlo y las determinaciones de tiempo y números necesarios para su realización.
- ✓ "Hacer que ocurran cosas que de otro modo no habrían ocurrido". Esto equivale a trazar los planes para fijar dentro de ellos nuestra futura acción.
- ✓ Determinación racional de a dónde queremos ir y cómo llegar allá

1.3.2 Niveles de Planeación

La planeación considerada como uno de los principales elementos del proceso administrativo, es de fundamental importancia dentro de la estructuración de un Centro de Respuesta a Incidentes de Seguridad Informática; como tal considera los siguientes niveles:

1.3.2.1 Planeación Estratégica.

Se refiere a las estrategias a seguir en la construcción del Centro de Respuesta a

Incidentes de Seguridad informática. ¿Por qué construirlo?. Cuando se responde a este cuestionamiento, pueden inferirse los caminos a seguir para la construcción del mismo.

1.3.2.2 Planeación de Recursos.

Dentro de este ámbito deben considerarse los recursos económicos que va a requerir la construcción del Centro de Respuesta a Incidentes de Seguridad informática. ¿Cuánto dinero se va a ocupar? La planeación de recursos para un Centro de Respuesta a Incidentes de Seguridad Informática, es aquella que establece los objetivos y determina un curso de acción a seguir, de los siguientes elementos:

- ✓ Instalaciones: Edificios y acondicionamiento del mismo, plantas de emergencia, dispositivos de seguridad, etc.
- ✓ Equipo: Equipos para un Centro de Respuesta a Incidentes de Seguridad informática necesario para su funcionamiento, periféricos, etc.
- ✓ Materiales de producción: Materias primas para su funcionamiento, así como materiales directos e indirectos.

1.3.2.3 Planeación Operativa

La planeación operativa de un centro de Respuesta a Incidentes de Seguridad Informática consiste en realizar un detallado análisis de necesidades de la empresa y definir en base a estas necesidades una plataforma tecnológica con una infraestructura en hardware, software, personal operativo, etc. que soporte las operaciones de la empresa y se utilice como el medio de procesamiento de información.

Ésta determinará el ¿Cómo va a funcionar el Centro de Respuesta a Incidentes de Seguridad Informática?, ¿Qué Software será necesario? y ¿Qué cantidad de personal será necesaria?, etc.

1.3.2.4 Planeación de Personal.

¿Quiénes van a operar al Centro de Respuesta a Incidentes de Seguridad Informática?, ¿Cuáles serán sus funciones?, ¿Qué cantidad de personal será

necesaria?, etc.

1.3.2.5 Planeación de Instalaciones Físicas.

¿En dónde estará ubicado el Centro de Respuesta a Incidentes de Seguridad Informática?, ¿Cuántas secciones será necesario construir?, ¿En dónde se colocará el centro de carga?, ¿En donde serán ubicados los servidores?, ¿Qué condiciones de ventilación serán necesarias?, etc.

1.3.3 Principios de la Planificación.

Para planear eficientemente es necesario tomar en cuenta los siguientes principios:

1.3.3.1 Factibilidad.

Lo que se planee debe ser realizable

1.3.3.2 Objetividad y Cuantificación.

Cuando se planea es necesario basarse en datos reales y nunca en especulaciones u opiniones.

La planeación será más confiable en cuanto pueda ser cuantificada ósea, expresa en tiempo, dinero, cantidades y especificaciones (porcentajes, unidades, volumen).

1.3.3.3 Flexibilidad.

Al elaborar un plan este debe de afrontar situaciones imprevistas, y que proporcionen nuevos cursos de acción que se ajusten fácilmente a las condiciones.

1.3.3.4 Unidad.

Todos los planes específicos deben integrarse a un plan general y dirigirse a logros de los propósitos y objetivos generales.

1.3.3.5 Del cambio de Estrategias.

Cuando un plan se extiende en relación al tiempo, será necesario rehacerlo completamente.

1.3.4 Etapas de la Planeación

1.3.4.1 Propósitos.

Son las aspiraciones fundamentales o finalidades de tipo cualitativo que persiguen en forma permanente o semipermanente, un grupo social. Son los fines a los que se quiere llegar.

1.3.4.2 Investigación.

Consiste en determinar todos los factores que influyen en el logro de los propósitos, así de los medios óptimos para conseguirlos.

1.3.4.3 Premisas.

Son suposiciones que se deben considerar ante aquellas circunstancias o condiciones futuras que afectarán el curso en que va a desarrollarse el plan.

1.3.4.4 Objetivos.

Presentan los resultados que el Centro de Respuesta a Incidentes de Seguridad Informática espera obtener, son fines por alcanzar, establecidos cuantitativamente y determinados para realizarse transcurrido un tiempo específico.

1.3.4.5 Estrategias.

Son cursos de acción general o alternativas que muestran la dirección y el empleo general de los recursos y esfuerzos, para lograr los objetivos en las condiciones más ventajosas.

1.3.4.6 Políticas.

Son guías para orientar la acción, son criterios, lineamientos generales a observar en la toma de decisiones, sobre problemas que se repiten una y otra vez.

1.3.4.7 Programas.

Es un esquema donde se establece la secuencia de actividades específicas que

habrán de realizarse para alcanzar los objetivos, y el tiempo requerido para efectuar cada una de sus partes y todos aquellos eventos involucrados.

1.3.4.8 Presupuestos.

Los presupuestos son un elemento indispensable al planear, ya que a través de ellos se proyectan, en forma cuantificada, los elementos que se necesitan para cumplir con los objetivos.

Un presupuesto es un esquema escrito de tipo general y/o específico, que determina por anticipado, en términos cuantitativos (monetarios y/o no monetarios).

1.3.4.9 Procedimientos.

Establecen el orden cronológico y la secuencia de actividades que deben seguirse en la realización de un trabajo repetitivo.

El Administrador de Centros de Respuesta a Incidentes de Seguridad Informática

De acuerdo a los conceptos de Administración revisados hasta el momento podemos definir consecuentemente al Administrador de Centros de Respuesta a Incidentes de Seguridad Informática como la persona con la autoridad y responsabilidad de planificar, organizar, dirigir y controlar la seguridad de los recursos informáticos ante incidentes de seguridad de la institución con la finalidad de optimizar su uso y asegurar la calidad y permanencia del servicio dentro de la Escuela Militar de Ingeniería, así como la prestación del servicio ininterrumpido y seguro.

1.4 Centro de Respuestas a Incidentes de Seguridad Informática.

Un Centro de Respuesta a Incidentes de Seguridad Informática representa una entidad dentro de la organización, la cual tiene como objetivo contribuir a la mejora de la seguridad de los sistemas de información dentro de su ámbito, así como promover una cultura de seguridad y buenas prácticas en el uso de las nuevas tecnologías de forma que se minimicen los incidentes de seguridad y permita afrontar de forma activa las nuevas amenazas que pudieran surgir. El Centro de Respuesta a Incidentes de Seguridad Informática es responsable de prevención y rápida detección, identificación,

monitoreo y mitigación frente a amenazas de seguridad informática. Prácticamente todas las actividades de los demás departamentos se basan en la información que les proporciona dicho centro. La toma de decisiones depende en gran medida de la capacidad de respuesta del proceso de datos. Por lo anterior, casi no se escatima la inversión para proveerlo del equipo técnico (material y humano) necesario.

De hecho, en la mayoría de las organizaciones el Centro de Respuesta a Incidentes de Seguridad Informática, absorbe la mayor parte del presupuesto.

La importancia que tiene el centro de Respuesta a Incidentes de Seguridad Informática dentro de la organización, lo coloca en una posición que influye incluso en una gran parte de las decisiones administrativas y de proyección de las empresas.

Un centro de Respuesta a Incidentes de Seguridad Informática significa la culminación de la sistematización de la empresa. El análisis y diseño de sistemas de información implica un alto grado de de eficiencia administrativa dentro de la organización, de lo contrario difícilmente se podrían llevar a la práctica los diseños. Se puede afirmar que el centro de Respuesta a Incidentes de Seguridad Informática reclama que los mecanismos administrativos de la organización estén claramente establecidos.

Aún más, si no lo estuvieran, dicho centro está preparado para colaborar a fin de establecerlos. En otras palabras, el centro de Respuesta a Incidentes de Seguridad Informática predica la buena administración.

1.4.1 Misión de un Centro de Respuesta a Incidentes de Seguridad Informática

La computadora como herramienta de solución para problemas de cálculo de operaciones, investigación de procesos, enseñanza, etc. establece las bases para determinar el objetivo de un Centro de Respuesta a Incidentes de Seguridad Informática, es el de Proteger los activos de información críticos de la Escuela Militar de Ingeniería y promover el conocimiento en seguridad de la información de manera de prevenir y responder a incidentes de seguridad a los diferentes Departamentos y/o secciones de esta Casa de estudios Superiores.

Los diversos servicios que puede prestar un Centro de Respuesta a Incidentes de Seguridad Informática, pueden dividirse en áreas específicas de trabajo.

1.4.2 Elementos que Componen un Centro del Respuesta a Incidentes de Seguridad Informática.

Para tener una visión organizada de los componentes básicos de un Centro de Respuesta a Incidentes de Seguridad Informática como Sistema de Computación integral, podemos dividir sus elementos en dos categorías: hardware y software

1.4.2.1 Hardware

El hardware es el conjunto de elementos físicamente visualizables en un sistema integral de computación o Central de Tecnologías de Información. Es el equipo propiamente dicho. Bajo este término se incluye tanto a la computadora como a los equipos periféricos: impresoras, discos, monitores, unidades de respaldo, etc.

Llamamos entonces hardware al conjunto de dispositivos mecánicos y electrónicos que forman parte de la computadora. Es el primer elemento de un sistema de computación y comprende a toda la maquinaria y al equipamiento relacionado al mismo.

Contrasta con el elemento software, el cual puede ser descrito como el conjunto de instrucciones que le dicen a la computadora qué hacer.

También contrasta con los datos que son los hechos y cifras que se almacenan en el Hardware y son controlados por el software. El equipamiento de un sistema de computación y las instrucciones asociadas para hacerle funcionar pueden ser comparados con el funcionamiento de una orquesta, esta analogía es útil para entender el modo de trabajo de un sistema de computación. Los músicos y sus instrumentos están ligados al concepto de hardware, las partiuras son el software y dentro de éste, el sistema operativo actúa como el director de la orquesta.

El software bajo esta analogía puede ser cambiado de acuerdo al trabajo a realizar, de la misma manera en que los músicos cambian las partituras para producir música (información) diferente.

El director, como la parte controladora del sistema (sistema operativo), trabaja con el

software para obtener del sistema (computadora /orquesta) lo que la audiencia (usuario) desea.

1.4.2.2 Software

El software es el segundo elemento de un sistema de computación, está constituido por los programas, es decir por el conjunto de instrucciones que se suministran a la máquina para que resuelva algún problema.

Bajo el concepto de software entonces, se incluye al conjunto de instrucciones agrupadas en rutinas y programas junto con la documentación respectiva que indican cómo resolver problemas de naturaleza diversa en una computadora.

En síntesis, el software está formado por instrucciones para que la computadora trabaje. El conjunto o serie de instrucciones para realizar una tarea en particular se llama programa o programa de software.

Bajo esta categoría incluimos a los programas preparados por el usuario (software de aplicación) como así también a aquellos programas provistos por el fabricante del equipo o comprado a terceras partes, como son el sistema operativo (software de base) y los lenguajes de programación, utilitarios y los productos para automatización de oficina como procesadores de texto, planillas de cálculo y otros productos de software.

1.5 Forma de operar un Centro de Respuesta a Incidentes de Seguridad Informática.

Un Centro de Respuesta a Incidentes de Seguridad Informática, es el conjunto de recursos físico, lógicos, y humanos necesarios para la organización, realización y control de las actividades informáticas de una empresa. Las principales funciones que se requieren para operar un centro de Respuesta a Incidentes de Seguridad Informática son las siguientes:

- ✓ Proporcionar alertas tempranas frente a amenazas informáticas que puedan desestabilizar la tecnología y la seguridad de la Escuela Militar de Ingeniería.

- ✓ Controlar y minimizar cualquier tipo de daño a la organización y su información, junto con la preservación de evidencia sobre lo ocurrido y la documentación correspondiente.

- ✓ Revisar los resultados de los procesos e incorporar acciones correctivas conforme a instrucciones de su superior inmediato.

- ✓ Realizar las copias de respaldo (back-up) de la información y procesos que se realizan en el Centro de Respuesta a Incidentes de Seguridad Informática, conforme a parámetros preestablecidos.

- ✓ Prevenir que eventos similares puedan ocurrir en el futuro, de tal forma que puedan erradicarse las causas raíz del incidente.

- ✓ Mantener una base de conocimientos que permita registrar las lecciones aprendidas de estos sucesos, con el objetivo de que no se repitan y si esto sucede, se pueda contar con un antecedente de la solución o soluciones posibles.

- ✓ Velar porque el sistema computarizado se mantenga funcionando apropiadamente y estar vigilante para detectar y corregir fallas en el mismo.

- ✓ Realizar labores de mantenimiento y limpieza de los equipos del CSIRT.

- ✓ Mantener informado a la Dirección Nacional de Informática, sobre el funcionamiento del Centro de Respuesta a Incidentes de Seguridad Informática.

- ✓ Cumplir con las Políticas, normas, reglamentos y procedimientos establecidos por la Dirección Nacional de Informática, para el desarrollo de las funciones asignadas.

1.6 Principales Departamentos de un Centro de Respuesta a Incidentes de Seguridad Informática

Dentro de la Escuela Militar de Ingeniería, el Centro de Respuesta a Incidentes de Seguridad Informática CSIRT, cumple diversas funciones que justifican los puestos de

trabajo establecidos que existen en él, las cuales se engloban a través de los siguientes departamentos:

1.6.1 Administración del Propio Centro de Respuesta a Incidentes de Seguridad Informática.

Las funciones de Administración en un Centro de Respuesta a Incidentes de Seguridad Informática, engloban operaciones de supervisión, planificación, establecimiento de políticas de respuestas a incidentes de seguridad, control de proyectos, seguridad general de las instalaciones y equipos, presupuestos y recursos humanos.

1.6.2 Seguridad de la Información.

La función de la Sección Seguridad de la Información se enmarca al Monitoreo de las Operaciones que se desarrollan dentro de las Instalaciones de la Escuela Militar de Ingeniería, realizando un exhaustivo control de los dispositivos existentes y de esta manera notificar sobre los incidentes a presentarse en el desarrollo de las actividades académicas y/o administrativas.

1.6.3 Soporte Técnico.

El soporte, tanto para los usuarios como para el propio Centro de Respuesta a incidentes de seguridad informática, se ocupa de las Operaciones de infraestructura, la administración de sistemas, red y el desarrollo de software, la gestión de los equipos de teleproceso, el estudio y evaluación de las necesidades y rendimientos del sistema y, por último, la ayuda directa a usuarios.

1.6.4 Telecomunicaciones.

La Sección Telecomunicaciones de realizar la supervisión y control de los incidentes con tráfico de red en el perímetro, así como de mantener el contacto con los proveedores de los servicios de Internet para mantener un servicio continuo y eficiente y de esta manera poder contener los incidentes que se presenten en el perímetro.

1.6.5 Sección Jurídica.

La Sección Jurídica del Centro de Respuestas a Incidentes de Seguridad Informática,

estará complete relación con el desarrollo de las actividades realizando proporcionando el apoyo profesional de su especialidad en:

- ✓ Seguimiento a incidentes.
- ✓ Procesos Administrativos.
- ✓ Seguimiento Legal.
- ✓ Revisión de políticas y procedimientos para ajustarse al marco regulatorio

1.7 Planificación del Centro de Respuestas a Incidentes de Seguridad Informática

En la actualidad se le reconoce a un Centro de Respuesta a Incidentes de Seguridad Informática a un grupo de profesionales que recibe los informes sobre incidentes de seguridad, analiza las situaciones y responde a las amenazas.

De esta forma llegamos a realizar la siguiente pregunta ¿Cómo optimizar el funcionamiento del Centro de Respuesta a Incidentes de Seguridad Informática para proporcionar un servicio eficiente?

Los recursos con los que debe de contar un Centro de Respuesta a Incidentes de Seguridad Informática son: Recursos humanos, materiales, financieros, estructurales y tecnológicos; de los cuales este último se constituye como el más importante derivado de su explosiva evolución. Y es aquí donde radica la importancia de una correcta planificación de inversión y administración adecuada de los recursos informáticos.

1.7.1 Adquisición de Software y Hardware.

1.7.1.1 Selección de Software.

Los criterios para seleccionar software son:

1. **Software:** Conjunto de programas o listas de instrucciones codificadas los cuales le permiten a la computadora realizar una o varias funciones.

Varía de acuerdo al nivel:

- ✓ Básico. Sistema Operativo (Seleccionar por Standard Mundial).

- ✓ Soporte: Base de datos (Seleccionar por Standard Mundial).

2. **Proveedor**: Las características que debe tener el proveedor de informática son:

- ✓ Reconocido prestigio mundial y nacional.
- ✓ Soporte técnico en instalación.
- ✓ Ayuda en problemas.
- ✓ Personal especializado.
- ✓ Tiempo de atención.
- ✓ Comunicación rápida.
- ✓ Servicios de capacitación: cursos, material, expositor, costos.
- ✓ Cartera de clientes de software iguales al adquirido.
- ✓ Documentación: Facilidad de uso.

3. **Costos:** Se considerará lo siguiente:

- ✓ Condición de pago.
- ✓ Local.
- ✓ Inclusión de entrenamiento.
- ✓ Costos de mantenimiento.

1.7.1.2 Selección de Hardware.

Los criterios para seleccionar hardware son:

1. **Equipos:**

- ✓ La configuración debe estar acorde a las necesidades de la carga del

procesamiento de datos.

- ✓ Debe tener una capacidad de crecimiento vertical (en el mismo equipo), horizontal (con otros equipos).
- ✓ Fabricante de calidad (muy bueno), reconocido prestigio mundial.
- ✓ Tiempo de garantía.
- ✓ Tecnología de "punta" (Alta).

2. **Proveedor:** Debe tener las siguientes características:

- ✓ Reconocido prestigio local.
- ✓ Soporte de mantenimiento: personal especializado, stock de repuestos.
- ✓ Tiempo de atención, local apropiado, comunicación rápida.
- ✓ Cartera de clientes con equipos equivalentes a los adquiridos.
- ✓ Tiempo de entrega oportuno.

3. **Precios:** Se debe considerar lo siguiente:

- ✓ Condiciones de pago.
- ✓ Detallado por componentes de la configuración.
- ✓ Descuentos por volumen.
- ✓ Costo de mantenimiento.

1.7.1.3 Adquisición de Software

El software para Computadores se puede clasificar en los siguientes tipos:

- ✓ **Sistema Operacional**: Es el conjunto de programas que controla las actividades operativas de cada Computadora y de la Red.
- ✓ **Paquete de Usuario Final:** Mediante los cuales el usuario de un manera sencilla elabora sus procesos, por ejemplo, hojas de calculo, manejadores de bases de datos, procesadores de palabras, etc.

- ✓ **Paquete de Sistemas Aplicativos:** En los que a diferencia de los anteriores, el usuario es simplemente quien los usa.

- ✓ **Software Autorizado:** Se considera como Software autorizado, tanto los sistemas operacionales como aquellos paquetes de usuario final y de sistemas aplicativos, que el departamento de sistemas ha instalado, previo visto bueno para su adquisición y con la Autorización legal del proveedor para su uso.

La selección del modelo y capacidades del hardware requerido por determinada dependencia, debe ir de acuerdo con el plan estratégico y sustentado por un estudio elaborado por Dirección Nacional de Informática, en el cual se enfatizan las características y volumen de información que ameritan sistematización y diferencian los tipos de equipos que se adjudican a las diversas áreas usuarias. Todo estudio determina una configuración mínima para el Computador y los aditamentos o dispositivos electrónicos anexos como unidades externas, impresoras, tarjetas y módems para comunicaciones, elementos para backups en cintas magnéticas, etc.; de acuerdo con las necesidades del usuario, así como una evaluación del costo aproximado de la inversión.

1.7.1.4 Consideraciones Generales para la Adquisición de Software y Hardware.

Para realizar cualquier adquisición de Software o Hardware, se deberán considerar los siguientes puntos:

- ✓ Solicitud de propuesta. Todo sistema se origina en base a una solicitud que hace el usuario al centro de Respuesta a Incidentes de Seguridad Informática, intentando satisfacer una necesidad específica.

Los parámetros sobre los cuales debe medirse dicha solicitud son los objetivos y las políticas, los cuales debe fijar el usuario, aunque puede ser que el departamento de análisis le brinde ayuda en su clarificación. Ambos parámetros deben quedar establecidos por escrito.

- ✓ **Evaluación de propuesta**.

  Previamente debe llevarse a cabo una investigación con el propósito de establecer con seguridad el tipo de Software y Hardware requerido para su

implementación, posteriormente se integra toda la información obtenida de dicha investigación y así poder establecer la operatividad de los sistemas a adquirirse.

- ✓ **Financiamiento.**

  Para el caso de Centros de Respuesta a Incidentes de Seguridad Informática destinados a la educación superior pública las Fuentes de financiamiento estarán a disposición de la Escuela Militar de Ingeniería a través del Departamento Administrativo Financiero.

- ✓ **Negociación de Contrato.**

  La negociación de contrato debe incluir todos los aspectos de operación del Software y del Hardware a implementarse. Aspectos tales como:
  Actualizaciones, innovaciones, capacitación, asesoría técnica, etc.

Permisos y Licencias.

El uso de Software no autorizado o adquirido ilegalmente, se considera como pirata y una violación a los derechos de autor.

El uso de Hardware y de Software autorizado está regulado por las siguientes normas:

- ✓ Toda dependencia podrá utilizar UNICAMENTE el hardware y el software que la Dirección Nacional de Informática a través del Departamento responsable, le haya instalado y oficializado mediante el "Acta de entrega de equipos y/o software".

- ✓ Tanta el hardware y software, como los datos, son propiedad de la Escuela Militar de Ingeniería su copia o sustracción o daño intencional o utilización para fines distintos a las labores propias de la compañía, será sancionada de acuerdo con las políticas, normas y reglamentos internos.

- ✓ La Dirección Nacional de Informática a través del Departamento responsable, llevara el control del hardware y el software instalado, basándose en el número de serie que contiene cada uno.

- ✓ Periódicamente, la Dirección Nacional de Informática a través del Departamento responsable, efectuará visitas para verificar el software utilizado en cada dependencia. Por lo tanto, el detectar software no instalado por esta dependencia, será considerado como una violación a las Políticas y normas de seguridad internas de la Escuela Militar de Ingeniería.

- ✓ Toda necesidad de hardware y/o software adicional debe ser solicitada por escrito a la Dirección nacional de Informática, quien justificará o no dicho requerimiento, mediante un estudio evaluativo a través del Departamento responsable.

- ✓ El Departamento responsable, dependiente de la Dirección Nacional de Informática, instalará el software en cada computador y entregará al área usuaria los manuales pertinentes los cuales quedaran bajo la responsabilidad del Jefe del departamento y/o sección respectivo.

- ✓ Los trámites para la compra de los equipos aprobados por el Departamento de Sistemas, así como la adecuación física de las instalaciones serán realizadas por la dependencia respectiva.

- ✓ La prueba, instalación y puesta en marcha de los equipos y/o dispositivos, serán realizada por el departamento de sistemas, quien una vez compruebe el correcto funcionamiento, oficializara su entrega al área respectiva mediante el "Acta de Entrega de Equipos y/o Software".

Derechos de Autor y Licencia de uso de software.

El Copyright, o los derechos de autor, son el sistema de protección jurídica concebido para titular las obras originales de autoría determinada expresadas a través de cualquier medio tangible o intangible.

Las obras literarias (incluidos los programas informáticos), musicales, dramáticas, plásticas, gráficas y escultóricas, cinematográficas y demás obras audiovisuales, así como las fonogramas, están protegidos por las leyes de derechos de autor.

El titular de los derechos de autor tiene el derecho exclusivo para efectuar y autorizar las siguientes acciones:

- ✓ Realizar copias o reproducciones de las obras.
- ✓ Preparar obras derivadas basadas en la obra protegida por las leyes de derechos de autor.
- ✓ Distribuir entre el público copias de la obra protegida por las leyes de derechos de autor mediante la venta u otra cesión de la propiedad, o bien mediante alquiler, arrendamiento financiero o préstamo.
- ✓ Realizar o mostrar la publicidad de la obra protegida por las leyes de derechos de autor.
- ✓ Importar el trabajo, y realizar actos de comunicación pública de las obras protegidas.

1.8 Instalaciones Físicas del Centro de Respuesta a Incidentes de Seguridad Informática

Se establece a continuación criterios ideales para establecer la correcta y segura disposición física del centro de Respuesta a Incidentes de Seguridad Informática en las organizaciones:

1.8.1 Edificio, área y espacio.

1.8.1.1 Edificio.

Es trascendental la ubicación del edificio y su construcción misma para la operación eficiente del Centro de Respuesta a Incidentes de Seguridad Informática y como primera medida, debe considerarse si se trata de un edificio nuevo de construir o uno ya existente a adecuarse, para ello se mencionan los siguientes puntos:

- ✓ Realizar un estudio de la zona a fin de evitar estar expuestos al peligro por sismos, contaminación, incendio, explosión, inundación, radiaciones, interferencia de radar, vandalismo, disturbios sociales, así como riesgos provocados por las industrias cercanas y todo lo que pueden ocasionar problemas con el equipo de procesamiento de datos y archivos.

- ✓ Seleccionar la parte más segura dentro del edificio para el centro de Respuesta a Incidentes de Seguridad Informática y contar con facilidades de energía eléctrica, acometidas telefónicas, aire acondicionado, servicios públicos y salida de emergencia adecuada.

- ✓ Cuando el acceso al Centro de Respuesta a Incidentes de Seguridad Informática deba efectuarse a través de otros departamentos, será necesario prever el paso de las máquinas a través de diferentes puertas, ventanas, pasillos, montacargas, etc.

- ✓ Se deben definir claramente las rutas de acceso del personal para la carga de documentos, respaldos en unidades magnéticas, elaboración de reportes, etc., cuidando que no existan sobre el piso escalones, rampas, cables, etc.

- ✓ La construcción del piso debe soportar el peso de los equipos que serán instalados. Las designaciones típicas de los equipos IBM no rebasan de los 340kg/m2.

- ✓ La puerta de acceso al centro de Respuesta a Incidentes de Seguridad Informática debe tener 95cm. de ancho mínimo y abrir hacia afuera.

- ✓ Se deben de usar materiales de construcción no combustible y resistente al fuego.

- ✓ Recubrir las paredes con pintura lavable, con el objeto de que no se desprenda polvo y sea fácil su limpieza.

- ✓ Construir el mínimo de ventanas exteriores (o ninguna) a fin de evitar interferencias.

- ✓ Si el falso plafón se utiliza como pleno para el retorno del aire acondicionado, deberá pintarse el techo real con pintura de aceite o sintética de color claro.

1.8.1.2 Área y Espacio

Se recomienda que en el área del Centro de Respuesta a Incidentes de Seguridad

Informática existan separadores de aluminio y cristal o cuartos independientes para la instalación de todo el equipo y debemos considerar lo siguiente:

- ✓ La configuración definitiva del sistema a instalar: el procesador, impresoras, estaciones de trabajo, módems, multiplexores y demás periféricos.
- ✓ Es necesario plantear la secuencia de conexión de los equipos para los direccionamientos de los mismos.
- ✓ Se recomienda la ubicación de la consola del sistema como máximo a 6 metros de distancia del rack del procesador y que sea visible el panel de control del mismo.
- ✓ Por el polvo que desprenden las impresoras y el ruido que hacen al imprimir, se deben instalar en un cuarto independiente junto con una estación de trabajo a un metro de distancia de la impresora del sistema para facilitar el suministro de los reportes.
- ✓ Se debe tener en cuenta el espacio a ocupar del equipo adicional como son: Comunicaciones, módems, teléfonos, nobreak, un archivo mínimo, cintas de respaldo, una mesa de trabajo, mueble para manuales y papelería, además del espacio para futuro crecimiento.

1.9 Energía Eléctrica y Tierra Física

1.9.1 Instalación Eléctrica

La instalación eléctrica es un factor fundamental para la operación y seguridad de los equipos en el que se debe completar el consumo total de corriente, el calibre de los cables, la distribución efectiva de contactos, el balanceo de las cargas eléctricas y una buena tierra física.

Una mala instalación provocaría fallas frecuentes, cortos circuitos y hasta que se quemen los equipos.

La instalación eléctrica para el área de sistemas, debe ser un circuito exclusivo tomado de la sub-estación o acometida desde el punto de entrega de la empresa distribuidora

de electricidad, usando cables de un solo tramo, sin amarres o conexiones intermedias. Para el cálculo de la línea se debe tomar un factor de seguridad de 100% en el calibre de los conductores para una caída máxima de voltaje de 2%.

Se debe construir una tierra física exclusiva para esta área, la cual se conecte a través de un cable con cubierta aislante al centro de carga del área del Centro de Respuesta a Incidentes de Seguridad Informática.

1.9.1.1 Construcción de la Tierra Física

- ✓ Se deberá elegir un jardín o lugar en donde exista humedad, en caso contrario es necesario colocar un ducto que aflore a la superficie para poder humedecer el fondo.
- ✓ Hacer un pozo de 3 metros de profundidad y 70 centímetros de diámetro.
- ✓ En el fondo se debe colocar una capa de 40 cm. de carbón mineral sobre la cual descansará una varilla copperwel.
- ✓ Encima del carbón se deberá agregar una capa de sal mineral de 5 cm. y otra de pedacería de aluminio y cobre de 40 cm., cubriéndose después con tierra hasta la superficie.
- ✓ El tablero principal para el equipo del computador se debe proveer trifásico y con doble bus de tierra, (5 hilos), uno para el neutro eléctrico y otro para proveer tierra física a las maquinas.
- ✓ Como una medida de seguridad deberá instalarse en un lugar próximo a la puerta un control para cortar la energía a todo el equipo de Respuesta a Incidentes de Seguridad Informática en cualquier situación de emergencia, y deberá estar debidamente señalizado.
- ✓ El espacio próximo al control de interruptores debe permanecer libre de obstáculos para su fácil operación.
- ✓ Se deberá tener tantos circuitos como máquinas estén indicadas que deben

llevar conector, esto es: La unidad central de proceso, impresoras, unidades de control de discos, cintas, comunicaciones, pantallas, etc.. La protección de estos circuitos debe ser interruptor termomagnético. Se deben tener circuitos extras para cubrir ampliaciones con las características de los circuitos trifásicos y monofásicos.

Todos los conductores eléctricos hacia el centro de carga de la sala deben instalarse bajo tubería metálica rígida y de diámetro adecuado, debidamente conectadas a tierra. Los circuitos a cada unidad deben estar en tubo metálico flexible, en la proximidad de la maquina que alimentarán, para evitar trasferencia de energía radiante de los mismos, a los cables de señal del computador y por otra para evitar peligros de incendio.

Los circuitos de la unidad central de proceso, impresoras, unidades de control de discos, cintas, comunicaciones, se debe rematar con conectores tipo industrial a prueba de agua y explosión Rusell & Stollo equivalente.

Todos los interruptores deben estar debidamente rotulados para su rápida operación por parte del personal autorizado.

Para las conexiones de los contactos polarizados 125 VCA 3 hilos, debe utilizarse el código de colores:

FASE	:	Negro, rojo o azul
NEUTRO	:	Blanco o gris
TIERRA FÍSICA	:	Verde

Al efectuar los cálculos de la instalación eléctrica al tablero del equipo, los conductores, reguladores de tensión, interruptores termomagnéticos, etc., se deben calcular teniendo en cuenta la corriente de arranque de cada máquina, la cual generalmente es superior a la nominal.

Dicha corriente de arranque debe poder ser manejada sin inconvenientes, por todos

los elementos constitutivos de la instalación. Se debe considerar una expansión del 50% como mínimo.

1.9.1.2 Línea Eléctrica Independiente para Servicios

El uso de herramientas eléctricas para la limpieza o cualquier otro trabajo (aspiradora, taladro, pulidora, etc.) dentro del área de Respuesta a Incidentes de Seguridad Informática o en sus proximidades, implica las necesidades de que estas sean utilizadas conectándolas en una línea eléctrica que no sea utilizada por las máquinas componentes del sistema, para evitar las perturbaciones electromagnéticas que pudieran producir, las cuales afectan el trabajo que realiza el computador.

1.9.1.3 Placa Contra Transientes Eléctricos

En construcciones nuevas de locales para Centros de Respuesta a Incidentes de Seguridad Informática, es necesario prever una placa de aluminio de 1 metro cuadrado, ahogada en concreto, debajo del piso falso y frente al tablero principal de distribución eléctrico a las diferentes máquinas del sistema.

Estas placas deberán unirse eléctricamente al tablero de distribución eléctrico, de modo que forme una capacidad contra el plano de tierra del piso falso. La línea de conexión entre la placa con transientes con el tablero de distribución, no debe exceder de 1.5 metros de largo.

1.9.1.4 Regulador de Voltaje

Es indispensable la instalación de un regulador de voltaje para asegurar que no existan variaciones mayores al ±10% sobre el valor nominal especificado, que dé alta confiabilidad, protección total de la carga y rechace el ruido eléctrico proveniente de la línea comercial contaminada por motores, hornos, etc., éste deberá soportar la corriente de arranque con baja caída de tensión y estar calculado para las necesidad es del sistema y la ampliación futura que se estime necesaria. La regulación debe ser rápida efectuando la corrección para cualquier variación de voltaje o de carga entre 1 y 6 ciclos.

Las variaciones que soportan los equipos son las siguientes:

Tolerancia de voltaje	Tolerancia de frecuencia
115 volts +10% -10%	60 Hz. +-1/2 Hz.
208 volts	+6% -8%

Se requiere instalar un arrancador electromagnético con estación de botones, para proteger los equipos que no estén soportados por el UPS, de sobretensiones al momento de cortes de energía momentáneos y que estén únicamente con regulador de voltaje, el cual al momento de cualquier corte eléctrico, des-energizará los equipos y cuando regrese la corriente eléctrica, no entrará de lleno a los mismos si no hasta que una persona active el botón de arranque.

1.9.1.5 Fuente Ininterrumpida de Energía (UPS)

Para proteger de fallas de energía eléctrica comercial y evitar pérdida de información y tiempo en los procesos de Respuesta a Incidentes de Seguridad Informática de los equipos, se requiere de un UPS el cual abastezca eléctricamente como mínimo al equipo procesador, la impresora del sistema y la consola del sistema.

El uso de una fuente interrumpida de energía evita fallas en los sistemas de Respuesta a Incidentes de Seguridad Informática entregando una tensión:

a) De amplitud y frecuencia controlada.

b) Sin picos ni ciclos faltantes.

c) En fase y redundante con la línea externa, independiente del comportamiento de la red comercial.

El UPS en condiciones normales de energía comercial funciona como un regulador de voltaje, y en una baja o corte de energía, entra la carga de las baterías (Battery Backup) de un modo sincronizado que le es transparente al funcionamiento de los equipos.

Una vez restablecida la energía, las baterías se recargan automáticamente.

1.9.1.6 Estática

Una de las fallas más difíciles de detectar en los equipos es ocasionada por la electricidad estática producida por la fricción entre dos materiales diferentes y la consiguiente descarga de este potencial. Los materiales que son más propensos a producir estática son aquellos que están hechos de resina, plásticos y fibras sintéticas.

El simple hecho de arrastrar una silla sobre el piso nos ocasionará que tanto la silla como la porción del piso sobre el que se arrastró queden cargadas de electricidad estática. Si aquella silla o esta persona son aproximadas a una mesa metálica conectadas a tierra como los equipos, ocasionará que se produzca una descarga que puede ser o no sensible a una persona, pero sí será sensible a los equipos.

Para reducir al mínimo la estática, se recomienda las siguientes medidas:

- ✓ Conectar a tierra física tanto el piso falso como todos los equipos existentes.
- ✓ El cable para la tierra física deberá ser recubierto y del mismo calibre que el de las fases y el neutro.
- ✓ La humedad relativa deberá estar entre 45% +/- 5% para que las cargas estáticas sean menos frecuentes.
- ✓ Se recomienda usar cera antiestática en el piso.
- ✓ Si existieran sillas con ruedas, se recomienda que estas sean metálicas.

1.10 Aire Acondicionado y Humedad.

Los fabricantes de los equipos de Respuesta a Incidentes de Seguridad Informática presentan en sus manuales los requerimientos ambientales para la operación de los mismos, aunque estos soportan variación de temperatura, los efectos recaen en sus componentes electrónicos cuando empiezan a degradarse y ocasionan fallas

frecuentes que reduce la vida útil de los equipos.

Se requiere que el equipo de aire acondicionado para el Centro de Respuesta a Incidentes de Seguridad Informática sea independiente por las características especiales como el ciclo de enfriamiento que deberá trabajar día y noche aún en invierno y las condiciones especiales de filtrado.

La alimentación eléctrica para este equipo debe ser independiente por los arranques de sus compresores que no afecten como ruido eléctrico en los equipos. La determinación de la capacidad del equipo necesario debe estar a cargo de personal competente o técnicos de alguna empresa especializada en aire acondicionado, los que efectuarán el balance térmico correspondiente como es:

1. **Para Calor Sensible.**

Se determinan ganancias por vidrio, paredes, particiones, techo, plafón falso, piso, personas, iluminación, ventilación, puertas abiertas, calor disipado por las máquinas, etc.

2. **Para Calor Latente.**

Se determina el número de personas y la ventilación.

La inyección de aire acondicionado debe pasar íntegramente a través de las máquinas y una vez que haya pasado, será necesario que se obtenga en el ambiente del salón una temperatura de 21ºC +/ 2ºC y una humedad relativa de 45% +/- 5%, así como también en la cintoteca.

Es necesario que el equipo tenga controles automáticos que respondan rápidamente a variaciones de +/- 1ºC y +/- 5% de humedad relativa.

Estas características de diseño también han demostrado ser de un nivel de confort bueno y aceptado par la mayoría de las personas.

Se recomienda mantener las condiciones de temperatura y humedad las 24 horas del día y los 365 días del año, puesto que las cintas, disquetes, papel, etc., deben estar en las condiciones ambientales indicadas antes de ser utilizados.

Debe tenerse en cuenta que una instalación de aire acondicionado debe proveer como mínimo el 15% de aire de renovación por hora, por el número de personas que en forma permanente consumen oxígeno y expelen anhídrido carbónico, si no se considera, al cabo de un tiempo de operación comienzan a manifestarse malestares como dolor de cabeza, cansancio o agotamiento y disminuyen en el rendimiento del personal.

No deben usarse equipos de aire acondicionado de ventana que no regulen la humedad ni filtren el aire, porque los gases de la combustión de motores y polvo es aspirado y enviado al centro de Respuesta a Incidentes de Seguridad Informática.

El polvo y gases corrosivos pueden provocar daños en el equipo, una concentración alta de gases tales como dióxido de sulfuro, dióxido de nitrógeno, ozono, gases ácidos como el cloro, asociados con procesos industriales causan corrosión y fallas en los componentes electrónicos.

Este tipo de problemas son usuales en las ciudades muy contaminadas, por lo que se debe tener en cuenta en el diseño del aire acondicionado instalar filtros dobles o de carbón activado de tal manera que forme un doble paso de filtro de aire, con objeto de evitar causarle daño a las máquinas del sistema y degradaciones en sus componentes electrónicos. Todos los filtros que se usen no deberán contener materiales combustibles.

Para mantener constante la humedad relativa es necesario que el equipo de aire acondicionado se le adiciones un humidificador en el ducto de inyección principal. Un higrómetro de pared en el ambiente de la sala debe controlar al humidificador para el arranque y parada del compresor únicamente. Las unidades manejadoras de aire deberán trabajar en forma continua. El termostato y el higrómetro deberán responder a variaciones de 1ºC y 5% de humedad relativa.

Una alta humedad relativa puede causar alimentación de papel impropia, accionamiento indebido de los detectores de humo e incendio, falta de confort para el operador y condensación sobre ventanas y paredes cuando las temperaturas exteriores son inferiores a las del centro de Respuesta a Incidentes de Seguridad Informática.

Una baja humedad relativa crea la facilidad para que con el movimiento de personas, sillas rodantes, papel y mobiliarios generen la electricidad estática. El mejor método de distribución de aire para el Centro de Respuestas a incidentes de seguridad informática es el de usar el piso falso para la salida de aire y el plafón falso para el retorno mismo. Debe preverse una renovación de aire mayor al 15 %.

1.11 Iluminación y Acústica

1.11.1 Iluminación

Es muy importante contar con buena iluminación en toda el área, que facilite la operación de los equipos y para el mantenimiento de los mismos. Si es posible, se deben instalar todas las estaciones de trabajo alineadas en paralelo, de tal forma que las lámparas en el techo queden directos a los costados de las pantallas.

Para evitar la fatiga de la vista es necesario instalar lámparas fluorescentes blancas compatibles con la luz del día y pintar la oficina con colores tenues y el techo blanco para activar la reflexión.

Debe evitarse que lleguen los rayos directos del sol, para observar con claridad las distintas luces y señales de la consola y tableros indicadores de los equipos. Los circuitos de iluminación no se deben tomar del mismo tablero eléctrico que para alimentar los equipos de Respuesta a Incidentes de Seguridad Informática.

El nivel de iluminación corresponde a 40 watts por metro cuadrado de superficie de salón, usando lámparas fluorescentes.

1.11.2 Acústica.

El total del nivel de ruido en el Centro de Respuesta a Incidentes de Seguridad Informática, es acumulado por todos los ruidos del salón es afectado por los arranques físicos de los motores de los equipos y los movimientos en la operación. Para proveer una mayor eficiencia y una operación confortable, se recomienda aplicar material acústico en paredes y techos del salón, como son texturas a base de tirol o recubrimientos de enjarres.

1.12 Piso Falso.

El piso falso de la facilidad de distribuir el aire acondicionado de una manera más eficiente para el enfriamiento de los equipos, ocultar el cableado de instalación eléctrica y distribuir el cableado de sentilde; a las necesidades requeridas así como sus cambios de posición y mantenimientos. Se pueden mencionar algunas de las ventajas al usar el piso falso:

- ✓ Permite un espacio entre el piso real y el piso falso, que se puede usar como cámara plena para el aire acondicionado, facilita la distribución y salida del mismo donde se requiera.

- ✓ Proveer una superficie uniforme y plana que cubra todos los cables de señal de interconexión, cajas, cables y boas de alimentación de energía eléctrica, líneas telefónicas y de comunicaciones, etc.

- ✓ Permite cambios de distribución de los equipos o ampliaciones de los mismos con el mínimo de costo y tiempo.

- ✓ Es construido por paneles antiestáticos por una densa barrera termoacústica, envuelto con lámina electrogalvanizada, proporcionando solidez para un soporte de cargas óptimo resistente a la humedad y al fuego.

- ✓ La base guarda uniformidad estructural para soportar cargas distribuidas en un área mínima de 40cm cuadrados.

- ✓ Los pisos falsos metálicos, presentan la facilidad de ser conectados a tierra en diferentes puntos, lo cual ayuda a descargar la estática que se produce en las superficies.

El piso falso debe ser de módulos intercambiables de 61x61 cm. Y pueden ser construidos de acero, aluminio, hierro, etc. En el caso de los pisos de madera, la parte inferior de las losas deberá quedar recubierta con la termina metálica, de tal forma que al descansar sobre los pedestales la placa haga contacto físico y forme un plano de tierra elevado, que facilite la descarga electrostática. Esto implica que los pedestales deberán ser conecta dos a tierra, lo cual se comprobará previamente a la instalación

de sistema.

La carga de algunos equipos en sus puntos de apoyo pueden ser de hasta 455 kg. (1000 lbs.), por lo que le piso falso debe ser capaz de soportar cargas concentradas de 455 kg. en cualquier punto con una máxima deflexión de 2mm.

Si el espacio entre el piso real y el piso falso se usa como cámara plena, es necesario que tanto el firme del piso como el de las paredes que limitan la cámara no desprendan polvo en absoluto y sean tratadas deberá estar sellada lo más herméticamente posible, para evitar fugas de aire o para evitar que entre polvo y basura. Es necesario un escalón o rampa de acceso al centro de Respuesta a Incidentes de Seguridad Informática para igualar los niveles de piso, por seguridad el escalón o rampa deberá ser del mismo material del piso falso y estar recubierta con hule estriado perpendicular a la dirección de circulación o acceso, y en caso de la rampa tener una elevación menor de 12º.

1.13 Ductos y Cableado de Señal

En un Centro de Respuesta a Incidentes de Seguridad Informática donde existe gran variedad de cables necesarios para el funcionamiento y comunicación de los procesadores con sus equipos periféricos, tanto por seguridad como por cuidar los acabados en la decoración interior, los ductos son un factor de gran importancia para ocultar los cables de señal. Aún contando con piso falso en el centro de Respuesta a Incidentes de Seguridad Informática se deben distribuirlos cables a través de canaletas o ductos especiales para cables reducen los costos de instalación dando una apariencia ordenada y facilidad para el mantenimiento. Existen varios tipos de ductos son:

PVC, el cual es igual para la canalización aparente, METALICOS, NORYL, POLYCARBONATO, etc., (los últimos dos soportan temperaturas arriba de los 125°C).

El sistema modular de cableado de comunicación permite conducir cables para voz, datos, video, fibra óptica y electricidad en canales independientes y cuenta con toda la gama de conectores RJ-11, RJ-45, F. TWINAX. BNC. TOKEN-RING. RCA, etc., tanto en PLUG, JACK, ADAPTADOR O RECEPTACULO. Nunca deberá conducir señal y

electricidad por la misma tubería o ducto.

1.13.1 Cable Coaxial.

El tipo de cable para la conducción de señal de datos coaxial o twinaxial provee un alto rango de inmunidad a las interferencia electromagnéticas y de radiofrecuencia, lo cual es de suma importancia contaminados o zonas con interferencias, también alcanza distancias más grandes para la transmisión de señal en comparación con el cable de partrenzado (twisted pair).

1.13.2 Cable Par Trenzado (Twisted Pair):

Hoy en día el sistema de cableado estructurado ha dado las facilidades de convertir un departamento, área o edificio en inteligente, donde cada oficina cuente con los servicios de señal que necesite utilizando el cableado de par trenzado (twisted pair). Este cableado estructurado consiste en un sistema de distribuidores donde en uno le llega las señales de voz, datos o video de los equipos o procesadores y el otro distribuidor es la concentración de todos los cables que llegan de las oficinas y en este se realiza el patcheo de la señal o servicio requeridos.

1.13.3 Cable de Fibra Óptica:

La fibra óptica es el medio de transmisión de hoy y del futuro, es de alto grado de inmunidad a las interferencias electromagnéticas y cumple con el ancho de banda requerido para las aplicaciones de alta velocidad de datos.

La fibra óptica es últimamente aplicada como medio de transmisión entre los pisos de un edificio como BACKBONE.

1.14 Seguridad

La seguridad es un factor de suma importancia al planear la instalación física de un centro de Respuesta a Incidentes de Seguridad Informática. Esta consideración se refleja en la elección de las normas a considerar para la ubicación del procesador, materiales utilizados para su construcción, equipo de detectores y protección contra incendios, sistema de aire acondicionado, instalación eléctrica, sistema de control de

acceso y el entrenamiento al personal u operadores.

1.14.1 Situación del Área del Procesador

- ✓ El área de los procesadores no debe situarse encima, debajo o adyacente a áreas donde se procesen, fabriquen o almacenen materiales inflamables, explosivos, gases tóxicos, sustancias radio activas, etc..

- ✓ No debe existir material combustible en el techo, paredes o piso y debe ser resistente al fuego (mínimo una hora).

- ✓ Todas las canalizaciones, ductos y materiales aislantes, deben ser no combustibles y que desprendan polvo.

1.14.2 Almacenamiento de Información.

- ✓ Cualquier información almacenada en el centro de proceso, como listados, diskettes, cintas, etc.., debe estar guardados en gavetas metálicas o resistentes al fuego.

- ✓ La sintética deberá estar construida con un rango de resistencia al fuego de por lo menos dos horas y debe ser utilizada sólo para este fin.

- ✓ Se deberá contar con un lugar seguro e independiente del centro de proceso para custodiar los dispositivos magnéticos de respaldo, ya sea en bóvedas o en cajas fuertes, de preferencia en otro edificio.

1.14.3 Equipos Contra Incendios

- ✓ La mejor prevención contra incendios consiste en emplear materiales no combustibles o en su defecto, tratarlos con pinturas, impregnaciones u otros que impidan o retarden su inflamación.

- ✓ Debe instalarse un sistema de detección de humo e incendio distribuido por toda el área, tanto debajo del piso falso, en las salidas de aire acondicionado, en el falso plafón como las visibles en el techo. Este sistema de detección debe activar una alarma, la que avisara al personal para efectuar el plan de

contingencia ya establecido.

- ✓ Deben emplearse suficientes extintores portátiles de bióxido de carbono. Este es el agente recomendado para el equipo eléctrico (fuego clase "C"). La ubicación de los extinguidores debe estar marcada en el techo y ser accesible a las personas que trabajan en el área. Además, deben poder ser retirados con facilidad en caso de necesidad.

  Estos extintores deben ser inspeccionados una vez por año como mínimo y las instrucciones para su uso deben ser colocadas al lado de los mismos e incluidas en el programa de seguridad.

- ✓ Es aconsejable colocar una boca de agua con manguera a una distancia efectiva del centro de proceso, como agente extintor secundario para escritores, sillas, muebles, etc. (fuego clase "A").

1.14.4 Luces de Emergencia

Se recomienda el uso de luces de emergencia alimentadas del UPS (Uninterruptible Power Supply) o con baterías, que automáticamente se encienden ante una falta de energía eléctrica comercial.

1.14.5 Seguridad del Personal

- ✓ El Centro de Respuesta a Incidentes de Seguridad Informática debe estar construido y amueblado de manera que no se presenten lugares de peligro para el personal, como son: puertas enteras de vidrio sin indicadores en el mismo, lámparas de vidrio sin una protección adecuada, éct.

- ✓ Las salidas deben estar claramente marcadas y los pasillos del salón que los conducen, deben permanecer sin obstrucciones.

- ✓ Las áreas de servicios recomendadas para todos los sistemas y equipos auxiliares deben ser siempre respetadas.

1.14.6 Seguridad Contra Inundaciones

- ✓ Si el Centro de Respuesta a Incidentes de Seguridad Informática en la planta baja o en el sótano, es importante que se considere y elimine cualquier posibilidad de inundación.

- ✓ Eleve 20cm. su piso normal y verifique que en el área y sus alrededores haya buen sistema de drenaje y que este funcione adecuadamente.

- ✓ Coloque una protección adicional en las puertas a fin de evitar que se introduzca en el agua, en caso de que ésta subiera arriba de los 20cm o hasta el nivel del piso falso.

1.14.7 Seguridad para el Acceso al Centro de Respuesta a Incidentes de Seguridad Informática

- ✓ El Centro de Respuesta a Incidentes de Seguridad Informática debe tener una sola entrada para controlar el acceso a la instalación. Las puertas adicionales para salida de emergencia sólo podrán ser abiertas desde adentro y deberán estar siempre cerradas. Esta puerta de acceso única, permitirá tener un mejor control del paso al Centro de Respuesta a Incidentes de Seguridad Informática, tanto del personal como visitantes.

- ✓ Dependiendo de factores tales como el edificio en donde está instalado el Centro de Respuesta a Incidentes de Seguridad Informática, albergue otras funciones, es primordial el hecho de evitar el libre acceso a áreas restringidas. La identificación de las personas deberá ser total, antes de permitirles el paso hacia áreas más críticas.

- ✓ Excepto para el personal de servicio, no se debe permitir que cualquier visitante tenga acceso al Centro de Respuesta a Incidentes de Seguridad Informática o sus alrededores.

  Si esto es requerido o necesario, dicho visitante deberá ser acompañado por

el personal responsable autorizado o de vigilancia durante su permanencia en área. Tanto el personal de servicio como los visitantes deberán ser llamados para revisión de cualquier objeto de mano que pretendan introducir al área restringida como: maletas, bolsas, portafolios, bultos, etc.

- ✓ El acceso puede ser mejor controlado por medio de cerraduras electromecánicas operadas a control remoto, previa identificación de la persona. Existen cerraduras eléctricas que se pueden abrir con tarjetas magnéticas programables o tableros de control con password (clave de acceso), cuya clave puede ser cambiada periódicamente y es posible registrar automáticamente las entradas, intentos de violación e inferir cuando se está haciendo mal uso de una clave confidencial.

- ✓ También existe dispositivos de monitoreo a base de cámaras de T.V. en circuito cerrado, de modo que una persona de vigilancia pueda estar checando simultáneamente todas aquellas áreas que son de fácil acceso desde el exterior del edificio y poder notificar oportunamente al vigilante más cercano sobre lo que considera sospechoso y que es necesario interceptar. Una comunicación directa entre todos los puntos de vigilancia mencionados y el puesto de monitoreo, es indispensable.

- ✓ La vigilancia personal es de los mejores medios de seguridad por lo que el personal deberá ser instruido para que vigile a cualquier persona que no conozca y que se encuentre dentro de la instalación y que en adición sepa que no está autorizada para permanecer ahí. Cuando menos una persona de cada turno deberá ser asignada como responsable de la seguridad interna.

1.15 Mantenimiento Preventivo

Es muy importante saber las condiciones de operación de los equipos y prevenir riesgos y efectos de problemas que puedan afectar la operación de los mismos, por lo que se recomienda que periódicamente se elaboren los calendarios y se realice el mantenimiento preventivo oportunamente. Se recomienda contar con una póliza de mantenimiento de servicio de algún proveedor o con personal altamente capacitado

para la realización del mantenimiento preventivo.

- ✓ Se deberá revisar las especificaciones en el manual de operación de cada equipo.
- ✓ Para los procesadores de datos se deberán revisar: los errores del disco duro, cambiar los filtros de aire o en su defecto lavarlos, revisar la configuración del rack, limpiar las cabezas lectoras de las unidades, revisar cables flojos, remover y aspirar el polvo que pueda tener, revisar puertas abiertas, etc.
- ✓ Para las impresoras y demás periféricos revisar las bandas, engranes rodillos, motores, etc., se deberán cambiar partes muy gastadas.
- ✓ Para el piso falso y plafones, se deberán mantener aspirados y limpios sobre todo si se usan como cámara plena de aire acondicionado para que no suelte polvo para los equipos.
- ✓ El aire acondicionado por sus condiciones de uso que es exclusivo para el Centro de Respuesta a Incidentes de Seguridad Informática y su funcionamiento es de las 24:00 hrs. del día todo el año, se requiere de un mantenimiento preventivo del compresor filtros de aire de la menejadora, etc.
- ✓ Los detectores de humo e incendio probarlos para que activen el sistema de alarmas y estén en condiciones de operación para cuando se requiera.
- ✓ La instalación eléctrica, UPS´s y reguladores, checar que proporcionen los voltajes correctos, cables flojos o de falso contacto, interruptores, etc.

1.16 Cableado Estructurado

Manual INEI de Cableado Estructurado [p. 7-12, 39-65]

1.17 Aspectos Legales Relacionados con el Desarrollo y uso de Software.

Probablemente este tipo de preguntas son algunas de las cuestiones con la que tenemos que lidiar en la administración eficiente de un centro de Respuesta a Incidentes de Seguridad Informática. El software informático con el que se elabora en un centro de Respuesta a Incidentes de Seguridad Informática a diario, nos debe de

garantizar un buen uso de la información que se maneja en la empresa. Es responsabilidad del encargado del Centro de Respuesta a Incidentes de Seguridad Informática, así también la de realizar una auditoría del software utilizado, verificar licencias de productos, y un adecuado uso y manejo de software. Al software ilegal se le conoce también como software pirata.

Existen alrededor de cinco modalidades o categorías básicas de software ilegal:

1.17.1 Hurto de software

Esta modalidad tiene lugar cuando dentro de la organización se hacen copias adicionales de un programa para uso de sus empleados. El intercambio de Flash Memory entre amigos y asociados fuera del entorno laboral también se incluye en esta categoría.

1.17.2 Carga en disco duro

Algunos vendedores de equipos cargan copias no autorizadas de software en los discos duros de los equipos que ponen a la venta, como incentivo para que los usuarios finales les compren sus equipos a ellos y no a otros comerciantes.

1.17.3 Falsificación

Se trata de la copia y venta ilegal de software protegido por los derechos de la ley copyright, de una manera ideada para que parezca que el producto es legítimo. Algunas técnicas de falsificación de software llegan a ser muy sofisticadas y llegan a ser muy significativos esfuerzos para copiar exactamente la presentación, logotipo y métodos anti falsificación como los hologramas. También pueden ser muy grotescas, como por ejemplo discos con etiquetas manuscritas en bolsas de plástico que se venden en la calle.

1.17.4 Piratería en Boletines Electrónicos (BBS)

Ésta modalidad de piratería se produce cuando los usuarios conectados mediante módem a un boletín electrónico público o semiprivado, cargan en sus equipos software protegido por los derechos que copyright. No debe confundirse ése delito con compartir software de dominio público o con cargar “shareware”. El shareware es

software que puede estar o no protegido por los derechos de copyright, pero que generalmente es ofrecido por sus autores sin cargo o por una tarifa simbólica para su utilización sin limitaciones.

1.17.5 Alquiler de Software

Ésta modalidad se produce cuando el software se alquila ilegalmente a usuarios finales, que por lo general copian de forma permanente el software alquilado en los discos duros de sus equipos y devuelven la copia original a la arrendadora. Como hemos mencionado el software ilegal nos puede producir problemas de tipo legal, así como problemas de inseguridad en el manejo de información.

Desventajas del uso ilegal de Software

- ✓ Virus, pérdida de información, discos alterados, o programas defectuosos.
- ✓ Documentación inadecuada.
- ✓ Carencia de soporte técnico de productos disponibles solo para usuarios registrados legalmente.
- ✓ Falta de actualizaciones de programas de computación ofrecidas solo para usuarios registrados legalmente.
- ✓ En la mayoría de sus casos pérdida de garantías de pólizas referentes al software.
- ✓ Posibles sanciones por las autoridades correspondientes.

1.18 Administración del Riesgo.

Problemas más Comunes en un Centro de Respuesta a Incidentes de Seguridad Informática

El objetivo principal del presente acápite consta en la preparación del alumno en la identificación plena y fácil de los principales y más comunes problemas que se presentan en un centro de Respuesta a Incidentes de Seguridad Informática tanto en el

software (SW), como en el hardware (HW).

1.18.1 Hardware

Los principales problemas que se presentan con el HW, y los más comunes son:

- ✓ Defectos de fabricación y/o daños físicos que puedan tener durante su transporte.
- ✓ Que el manual de uso este en otro idioma ajeno al que manejamos.
- ✓ Las piezas que pudiera ser dañadas no son muy comunes y por tanto difíciles de conseguir.
- ✓ Cuando se trabaja con conexión a red, es muy común que por falta de conocimiento den órdenes que la puedan bloquear o provocar que ésta se caiga.
- ✓ Que las impresoras deben recibir trato especial porque la configuración de estas es muy específica.

1.18.2 Software

Los principales problemas que presenta el SW son entre otros:

- ✓ Los archivos necesarios para su instalación no están contenidos en el CD de instalación.
- ✓ El ambiente en que se desarrolla no es compatible con el sistema operativo que está siendo usado por el PC.
- ✓ El idioma, no siempre está en el que nosotros hablamos y por tanto nos es difícil su manejo.
- ✓ Algunas órdenes, comandos u operaciones son muy complejos y puede producir que al darlas de manera equivoca bloquee el equipo.
- ✓ El problema principal y más común que puede ser causa de más problemas que ningún otro factor es la falta de experiencia y la ignorancia.

1.18.3 Seguridad en los Accesos por Software

Siendo muchas las amenazas que pueden sufrir los ordenadores y las redes, es muy variado el software disponible.

Las amenazas	Soluciones
Virus que infectan las aplicaciones	Antivirus
Sniffers que capturan los datos y contraseñas que circulan por una red	
Cortafuegos, que ejercen un control sobre los accesos al sistema	
Programas que revientan los passwords	Herramientas para encriptar, codificar ficheros o mandar correo electrónico seguro
Caballos de Troya que se instalan en nuestro ordenador y toman el control	Programas que verifican la integridad de un sistema avisando cuando pasa "algo raro"
Espías que se ocultan en el ordenador e informan a terceros	Programas que analizan los ficheros .log de acceso a un sistema.
Gusanos que saltan de ordenador en ordenador	Detectores de vulnerabilidades que identifican puntos débiles de un sistema.

Los buenos y los malos son los usuarios no el software; imagine un software para detectar contraseñas, normalmente el informático de la empresa puede utilizarlo para detectar contraseñas de sus propios usuarios y avisar a aquellos que han puesto contraseñas fáciles de detectar. Pero también pueden utilizarlo un hacker para acceder a los documentos.

Las contraseñas fáciles de adivinar ponen en peligro la seguridad informática.

1.19 Análisis de Riesgos.

Las Universidades que utilizan sistemas de información llegan a ser, casi inevitablemente, dependientes de ellos, lo cual es un arma de doble filo, pues se corre el riesgo de que un fallo provoque el caos.

Realizar un análisis de riesgos es el primer paso que debe darse para conseguir la seguridad adecuada. Permite detectar los puntos débiles sobre los que aplica o reforzar medidas de seguridad.

1.19.1 Principales Riesgos

Los principales riesgos a los que se enfrenta un sistema, sus posibles consecuencias y medidas de seguridad son: los errores humanos, fallos de los equipos, robo de la información o equipos, virus, sabotaje, fraude, desastres naturales, entre otros.

1.19.2 Medidas de Seguridad

- ✓ Medidas de seguridad activa. Son aquellas cuyo objetivo es anular o reducir los riesgos existentes o sus consecuencias para el sistema.

- ✓ Medidas de seguridad pasiva. Están destinadas a estar preparado si llega a producirse el desastre.

1.20 El Plan de Contingencias.

El Plan de Contingencias constituye una presentación formal y responsable de acciones específicas a tomar cuando surja un evento o condición que no esté considerado en el proceso normal de operación de un Centro de Respuesta a Incidentes de Seguridad Informática.

Es decir, se trata de un conjunto de procedimientos de recuperación para casos de desastre; es un plan formal que describe pasos apropiados que se deben seguir en caso de un desastre o emergencia. Materializa un riesgo, ya que se pretende reducir el impacto de éste.

El Plan de Contingencia contempla tres tipos de acciones las cuales son:

- ✓ La Prevención, conformada por el conjunto de acciones a realizar para prevenir cualquier contingencia que afecte la continuidad operativa, ya sea en forma parcial o total, del centro de Respuesta a Incidentes de Seguridad Informática, las instalaciones auxiliares, recursos, información procesada, en tránsito y almacenada. De esta forma se reducirá su impacto, permitiendo restablecer a la brevedad posible los diferentes servicios interrumpidos.

- ✓ Detección. Deben contener el daño en el momento, así como limitarlo tanto como sea posible, contemplando todos los desastres naturales y eventos no considerados.

- ✓ Recuperación. Abarcan el mantenimiento de partes críticas entre la pérdida del servicio y los recursos, así como su recuperación o restauración.

El procedimiento para la elaboración del Plan de Contingencias sugiere seguir los planteamientos establecidos por el Instituto Nacional de Estadística e Informática (INEI) que en anexo se adjunta al presente documento.

1.21 Administración del Cambio.

El cambio se encuentra por todas partes y siempre está presente. Acompaña siempre al hombre en las estaciones, en su ambiente social y en sus procesos biológicos. Desde los primeros momentos de su vida, el individuo aprende a afrontar el cambio adaptándose a él.

El cambio en el trabajo es cualquier alteración que ocurre en el ambiente de trabajo. Por fortuna, muchos de los cambios organizacionales que ocurren día con día son de poca importancia. Afecta a unos cuantos, son de índole incremental y son más o menos predecibles. Por ejemplo, a medida que evolucionan los procedimientos o se incorporan nuevos miembros a un grupo de trabajo, el resto de los empleados generalmente no necesita modificar todos los aspectos de su trabajo ni adquirir comportamientos totalmente diferentes. En este caso es fácil lograr un nuevo equilibrio. Sin embargo, una amplia diversidad de fuerzas puede ocasionar cambios más profundos que atañen a la organización en su totalidad. Muchos de ellos se han vuelto muy comunes, a medida que se han vuelto tan flexibles la economía, la competencia y el ritmo del cambio tecnológico.

Ejemplo de ello son la fusión de algunas empresas, la adquisición apalancada, así como la subsecuente reestructuración organizacional y los desastres naturales como el derrame de petróleo o el escape de gas. Crisis como éstas, sin importar si son positivas o negativas, exigen que los administradores guíen a los empleados durante el choque emocional que los acompaña hasta que alcanzan un nuevo equilibrio.

1.21.1 Estrés

El estrés es un término general que se aplica a las presiones que la gente sufre en su vida. El estrés laboral es casi inevitable en muchos trabajos. Cuando la presión empieza a acumularse, ocasiona un efecto negativo en nuestras emociones, en nuestro proceso de pensamiento y en nuestra condición física. Si el estrés se vuelve excesivo, los empleados presentan diversos síntomas de estrés que pueden perjudicar su desempeño en el trabajo y su salud e incluso deteriorar su capacidad de hacer frente al ambiente. Los que lo sufren pueden sentir nerviosismo y ser víctimas de una preocupación crónica. A veces se tornan poco cooperativos o consumen alcohol y drogas en forma excesiva. Aunque esos problemas también se deben a otras causas, son síntomas comunes del estrés.

El estrés también produce trastornos físicos, porque el sistema interno del organismo cambia para superarlo. Algunos problemas físicos aparecen al cabo de poco tiempo, otros tienen una evolución más lenta. Cuando el estrés dura mucho tiempo puede ocasionar además enfermedades degenerativas del corazón, lo riñones, los vasos sanguíneos y de otras partes del cuerpo. Es, pues, importante que el estrés, tanto en el trabajo como fuera de él, sea mantenido a un nivel bastante bajo para que las personas puedan tolerarlo sin riesgo de trastornos o enfermedades.

Cada vez se cuenta con más evidencia de que, en algunas situaciones, una organización puede ser legalmente responsable del efecto psíquico y físico que el estrés del trabajo tenga en empleados. Las condiciones inadecuadas de trabajo, los conflictos constantes con supervisores o el hostigamiento intencional de los compañeros algunas veces dan origen a neurosis, angustia e incluso suicidio.

El estrés puede ser temporal o a largo plazo, ligero o severo, según la duración de sus causas, la fuerza de éstas y la capacidad de recuperación que tenga el empleado. Si el estrés es temporal y moderado, la mayor parte de las personas pueden controlarlo o, por lo menos, recuperarse rápidamente de sus efectos.

1.21.2 Formas de Ejercer Autoridad.

La manera en que el líder ejerce la autoridad que le fue asignada, es un factor

determinante en el buen funcionamiento de una organización, debido a que es la persona en quien recae la responsabilidad de hacer cumplir los objetivos propuestos. Existen diferentes tipos de líderes, pero todos deben de coincidir de alguna manera en su manera de proceder.

El buen líder deberá ser exigente y considerado, deberá atender las necesidades de sus empleados, deberá ser responsable y deberá claro está, ser dinámico.

1.21.2.1 Modelo de Contingencia de Fiedler

Este modelo se basa en la distinción previa entre orientación hacia los empleados y hacia el trabajo, y sugiere que el estilo del liderazgo más apropiado depende de sí la situación general es favorable, desfavorable o está en una etapa intermedia para el líder. Muestra que la eficacia de un líder está determinada por la interacción de la orientación hacia el empleado y tres variables situacionales como lo son:

- ✓ Las relaciones del líder con los miembros del grupo.- Están determinadas por la manera en que el grupo acepte al líder.
- ✓ La estructura del trabajo.- Refleja el grado de especificidad en que debe realizarse una tarea.
- ✓ La posición de poder del líder.- Describe el poder organizacional que deriva de la posición que ocupa el líder. Por Ejemplo.- el poder para contratar y despedir, para otorgar aumentos.

Este modelo recomienda que las relaciones entre los trabajadores y los líderes sean óptimas para un mejor desempeño de las actividades que se llevan dentro del Centro de Respuesta a Incidentes de Seguridad Informática. El modelo de Fiedler, ha sido muy criticado, a pesar de ello representó una gran contribución al análisis del estilo de liderazgo. Por ejemplo, obliga a los gerentes a:

- ✓ Analizar su situación, el personal, el trabajo y la organización.
- ✓ Ser flexibles en la aplicación de las diversas habilidades dentro de un estilo general de liderazgo

- ✓ Considerar los elementos que modifican sus puestos para obtener congruencia con el estilo que prefieran.

1.21.2.2 Modelo de Liderazgo Situacional de Hersey y Blanchar

Este modelo sugiere que el factor más importante que afecta la selección del estilo de un líder es el Nivel de Desarrollo (madurez) del subordinado. Los gerentes evalúan a los empleados según los criterios siguientes:

- ✓ Conocimiento del puesto.
- ✓ Habilidades y Capacidad.
- ✓ Aceptación de Responsabilidades.
- ✓ Capacidad para actuar independientemente.

La competencia para desempeñar un trabajo determinado y el compromiso para hacerlo puede variar entre los empleados, y por lo tanto, los niveles de desarrollo exigen respuestas diferentes de los líderes. Hersey y Blanchard utilizan una combinación de tareas y relaciones para crear cuatro estilos principales de liderazgo:

- ✓ Indicar.
- ✓ Vender.
- ✓ Participar.
- ✓ Delegar.

Esto da como resultado los diferentes estilos de liderazgo que un gerente debe de tomar según sea la situación. Los modelos anteriores nos mostraron ¿qué roles puede tomar un líder?, ¿cuál debe ser su comportamiento?, etc., ¿Pero qué pasa si no hay líderes?

Sus títulos del Liderazgo (Recurso/Naturaleza)

Trabajo:

- ✓ Satisfacción intrínseca.

- ✓ Retroalimentación de la tarea misma.
- ✓ Rutina, tareas predecibles. Organización:
- ✓ Grupos unidos de trabajo.
- ✓ Planes explícitos, metas y procedimientos.
- ✓ Toma de decisión descentralizada. Empleados:
- ✓ Orientación profesional.
- ✓ Habilidad, experiencia, adiestramiento y conocimientos.
- ✓ Capacidad para auto administrarse. Auto liderazgo:

Es un sustituto único para el liderazgo. Sus impulsos son:

- ✓ Llevar a la persona a desempeñar tareas naturalmente motivantes.
- ✓ Impulsarla a realizar un trabajo requerido pero no naturalmente reconfortante.

El papel único de Liderazgo del Supervisor

Los supervisores son líderes que ocupan posiciones en el nivel gerencial más bajo en las organizaciones. También son el punto de contacto directo con la mayoría de los empleados de una organización. Existen diferentes puntos de vista del papel que puede tomar el supervisor:

- ✓ Persona Clave en la Administración: Toman decisiones, controlan el trabajo, interpretan la política de la empresa y generalmente son las personas clave en el proceso de realización del trabajo. Están estratégicamente localizados en la cadena de autoridad y comunicación por lo que pueden bloquear cualquier información.
- ✓ Supervisor en Posición Intermedia: Se encuentran entre la gerencia y los empleados. Los gerentes esperan de ellos el control de la producción,

disciplina, menores desperdicios. Por otro lado los empleados esperan que interprete sus temores y deseos ante la gerencia.

- ✓ Supervisor Marginal: Quedan fuera o al margen de las principales actividades e influencias que afectan al departamento. Son poco aceptados por los gerentes y al mismo tiempo ignorados por los trabajadores.

- ✓ Otro Trabajador: Se dice que es otro trabajador porque sigue siendo otro empleado. El centro de la toma de decisiones está en otro lado, por lo que los supervisores simplemente son los encargados de ver que se cumpla con las decisiones.

- ✓ Especialista en el Comportamiento: Su especialidad es el comportamiento humano.

1.22 Necesidades

Los buenos administradores se han dado cuenta que si protegen y atienden las necesidades de un empleado, éste será más productivo y claro está, más eficiente.

Los cambios en el trabajo, si se presentan de manera brusca o no se manejan con cuidado, pueden perjudicar dichas necesidades y por ello afectar de manera considerable a los empleados.

1.22.1 Reacciones al Cambio

El cambio en el trabajo se hace más complicado por el hecho que no produce un ajuste directo. En lugar de ello este ajuste funciona por medio de las actitudes de los empleados para producir una reacción que está condicionada a los sentimientos que estos últimos tienen hacia el cambio. Reacción del grupo al cambio:

Aunque cada persona interprete el cambio en forma individual, frecuentemente muestra su apego al grupo uniéndose a él de cierta manera uniforme, como una reacción al cambio. Básicamente el grupo reacciona con el sentimiento de "todos estamos juntos en esta empresa, cualquier cosa que le suceda a uno de nosotros nos afecta a todos".

1.22.2 Costos y Beneficios

Todos los cambios acarrean costos, por ejemplo; un nuevo procedimiento de trabajo puede requerir la molestia de aprender nuevas maneras de hacerlo. Temporalmente puede perturbar el trabajo y disminuir la motivación. Todo esto representa un costo no solamente económico, sino también un costo psicológico y social. Cada cambio hace necesario un análisis costo-beneficio muy preciso, los cambios no se justifican a menos que los beneficios excedan sus costos. La meta de una organización siempre será obtener más beneficios con el menor costo posible. Casi cualquier cambio, por ejemplo, implica alguna pérdida psicológica debido a la tensión que provoca en el individuo durante la adaptación. Las personas reaccionan de manera distinta ante el cambio. Algunas percibirán únicamente las ventajas o beneficios y otras verán sólo lo que el cambio les cueste a ellas.

1.22.3 Costos Psíquicos y Salud

En algunos casos los costos psíquicos del cambio pueden ser tan fuertes que perjudiquen la salud mental y hasta la salud física del empleado. Cada uno de nosotros posee cierto nivel de tolerancia al cambio. Cuando se rebasa, aparecen las respuestas relacionada con el estrés. Causando un estrés acumulativo que finalmente llega a saturar el sistema de una persona.

1.22.4 Costos Psíquicos de la Promoción

Un tipo importante de cambio es la promoción o la transferencia. Los empleados frecuentemente solicitan este tipo de movimientos como una forma de crecimiento personal o para obtener reconocimientos se les pide que aprendan nuevas habilidades y entablen nuevas amistades. Se cambian a otros papeles y a veces a diferentes grupos de trabajo, su posición social puede cambiar también. Todas estas acciones implican costos psíquicos porque requieren que los empleados enfrenten nuevas situaciones.

1.22.5 Costos Psíquicos y Renunciación de los Empleados

Algunas de las promociones requieren cambios a otros sitios. Estos cambios suelen representar altos costos psíquicos por que exigen mayores ajustes. También implican

cambios de las familias de los empleados, por lo que enfrentarlos muchas veces se torna todavía más difícil. Las empresas que necesitan reubicar a su personal han descubierto que también deben prestar especial atención a las necesidades humanas de sus empleados con el fin de disminuir los costos psíquicos.

1.22.6 Resistencia al Cambio

Naturaleza y efectos. La resistencia al cambio son los comportamientos del empleado tendientes a desacreditar, retardar o impedir la realización de un cambio en el trabajo. Los empleados se oponen al cambio porque constituye una amenaza contra sus necesidades de seguridad, de interacción social, de estatus o de autoestima. La percepción de la amenaza proveniente del cambio puede ser real o imaginaria, deliberada o espontánea, grande o pequeña. Cualquiera que sea su naturaleza, los empleados tratarán de protegerse contra los efectos del cambio. Sus acciones pueden incluir desde quejas, morosidad intencional y resistencia pasiva hasta ausentismo, sabotaje y lentitud en la realización del trabajo. Todos los empleados tienden a resistirse al cambio por los costos psíquicos que lo acompañan. Esa actitud se encuentra por igual entre gerentes y entre trabajadores. Puede encontrarse la misma resistencia al cambio en el oficinista y en el obrero. Es algo que no respeta ni tipo de ropa ni de trabajo. Si bien el ser humano tiende a resistir al cambio, esas inclinaciones la contrarresta el deseo de nuevas experiencias y de recibir los premios que acompañan al cambio.

No todos los cambios encuentran resistencia, pues algunos son buscados activamente por los empleados. Una lección que los administradores han de aprender es que: El cambio será un éxito o un problema, según la habilidad con que se administre para atenuar en lo posible la resistencia. Otra lección mencionada por el presidente de la Honeywell, es que "el cambio se realiza con mucha lentitud y exige un alto precio en cuanto a planeación y recursos". La inseguridad y el cambio son condiciones que demuestran que el efecto de la reacción en cadena puede manifestarse en el funcionamiento de la organización. Se trata de una situación en la que el cambio (u otra condición) que afecte directamente a una sola persona o unas cuantas, puede llevar a una reacción de muchos, aún de cientos o miles, porque existen en él intereses comunes. El hecho de que un grupo sea inteligente no necesariamente

significa que comprenderá mejor y aceptará el cambio. Muchas veces sucede lo contrario en vista de que el grupo utiliza su inteligencia para racionalizar más los motivos de su resistencia al cambio. La inteligencia también puede utilizarse a favor o en contra del cambio, de cómo sea introducido éste.

1.22.7 Clases de Resistencia.

Existen tres tipos de resistencia, que producen actitudes hacia el cambio, distintas en cada empleado. Las clases de resistencia son:

- ✓ **Resistencia Lógica:** Con bases en el pensamiento racional y científico. Surge del tiempo y el esfuerzo que se requiere para ajustarse al cambio, incluyendo las labores que deben aprenderse en el nuevo empleo. Estos representan costos reales que deben soportar los empleados. Aún cuando a la larga el cambio puede ser favorable para ellos, los costos a corto plazo deben pagarse primero.

- ✓ **Objeciones Lógicas y racionales:**

  - o Tiempo requerido para adecuarse.
  - o Esfuerzo adicional para aprender.
  - o Posibilidad de condiciones menos deseables.
  - o Costos económicos del cambio.
  - o Factibilidad técnica del cambio puesta en duda.

- ✓ **Resistencia Psicológica**: De acuerdo con las emociones, los sentimientos y las actitudes. Es lógica en términos de las actitudes y los sentimientos individuales de los empleados respecto al cambio.

  Pueden temer a lo desconocido, desconfiar del liderazgo de la gerencia, o sentir amenazada su seguridad. Aún cuando la gerencia considere que no existe justificación de esos sentimientos, éstos son reales y deben conocerse.

- ✓ **Actitudes Psicológicas y Emocionales:**
  - Temor a lo desconocido.
  - Escasa tolerancia al cambio.
  - Desagrado hacia la gerencia u otro agente de cambio.
  - Falta de confianza en otros.
  - Necesidad de seguridad.
- ✓ **Resistencia Sociológica:** Con base a los intereses y los valores del grupo. Los valores sociales son poderosas fuerzas del ambiente a las que debe atenderse con cuidado. Representan coaliciones políticas, valores opuestos de los sindicatos, y aún juicios distintos de comunidades diversas. Los administradores necesitan hacer que las condiciones del cambio sean lo más favorables posibles para manejar con éxito las resistencias sociológicas. Factores sociológicos; intereses de grupo:
  - Coalición política.
  - Valores de grupo de oposición.
  - Criterios anticuados y estrechos
  - Intereses establecidos.
  - Deseo de conservar amistades existentes.

Evidentemente, las tres clases de resistencia deben manejarse con eficiencia si se espera que los empleados cooperen con el cambio. Si los administradores se preocupan solamente por los aspectos técnicos y lógicos del cambio, habrá fracasado en su responsabilidad social y humana. Si la Dirección no puede ganarse todo el apoyo, tal vez requiera usar su autoridad; sin embargo, debe reconocer que no siempre conviene usarla, pues de hacerlo pierde su efecto. Posibles beneficios de la

resistencia. Puede constituir un estímulo para que la gerencia reexamine las propuestas del cambio y corrobore que son adecuadas. También puede identificar áreas específicas en las que un cambio podría causar mayores dificultades, de tal manera que la gerencia realice actividades correctivas antes de que surjan problemas más serios.

1.22.7 Implantación Exitosa del Cambio

En vista que la gerencia es la iniciadora de muchas modificaciones, y principalmente es responsable de llevarlas a cabo con éxito, frecuentemente se les llama Agente de Cambio; aunque no sólo promueve el cambio, sino también lo propicia. El grado de cambio que se necesita en la empresa depende del ambiente en que esta funciona. Los ambientes estables requieren menos cambios, mientras que los ambientes dinámicos exigen más. Ocasionalmente los ambientes dinámicos pueden producir cambios tan rápidos que sorprenden a los empleados.

Algunas organizaciones también reconocen la necesidad de desarrollar la capacidad de la gente para aprender de la experiencia del cambio. A este proceso se le llama "aprendizaje de doble circuito". Donde el primer circuito es cuando se refleja la información actual que se ha reunido, y el segundo es cuando se preparan a los participantes a administrar los cambios futuros aún más eficazmente. El conocimiento del comportamiento en la administración del cambio mejora considerando que el cambio está constituido de los tres pasos siguientes:

- ✓ Descongelamiento
- ✓ Cambio
- ✓ Recongelamiento

El descongelamiento significa que es preciso desechar las viejas ideas y prácticas para aprender otras nuevas. El cambio es también el paso en que se aprenden las nuevas ideas y prácticas, de manera que el empleado pueda pensar y actuar en muchas formas diferentes. El recongelamiento significa que lo que se ha aprendido se integra en la práctica cotidiana. Además de ser aceptadas intelectualmente, las

nuevas prácticas quedan incorporadas en el comportamiento habitual. Para mostrar con más claridad los tres pasos nos será de gran utilidad la curva de aprendizaje en la organización la cual nos señala los tres pasos anteriores; dicha curva es el período de adaptación que sigue al cambio y específicamente significa que habrá una declinación temporal de la efectividad antes de que el grupo alcance un nuevo equilibrio. Los empleados necesitan "descongelarse" y "recongelarse" para adaptarse al cambio, durante este período los empleados tratan de integrarse al cambio, y es probable que sean menos eficientes que antes. La curva del aprendizaje del cambio en la organización: Utilización de las fuerzas del grupo. Un cambio eficiente debe dirigirse al grupo, al igual que a los individuos. Generalmente más de una persona está implicada, pero lo más importante es el hecho de que el grupo sea un instrumento para atraer fuerte presión a sus miembros para que haya un cambio en ellos. El comportamiento del individuo se aferra firmemente al grupo al que pertenece, por lo que cualquier cambio en las fuerzas del grupo alentará modificaciones en la conducta de cada uno de sus miembros. La idea es ayudar al grupo a unirse con la gerencia para propiciar el cambio deseado.

- ✓ Liderazgo para el cambio. Un liderazgo inteligente refuerza el clima de apoyo psicológico para el cambio, en tal caso, el líder presenta a éste con base en los requerimientos impersonales de la situación, más que en las bases personales. Las peticiones ordinarias de cambio deben estar acordes con los objetivos y las normas de la organización, solamente un líder de fuerte personalidad podrá utilizar razones personales para el cambio sin provocar resistencia. Es más probable que el cambio resulte exitoso si los líderes que los introducen tienen grandes expectativas para lograrlo. Es decir si la meta es lograr el éxito de algún cambio éste vendrá al cabo de un período estimado de tiempo, si por lo contrario sino se espera gran éxito, éste no vendrá por más que el personal se esfuerce para lograrlo.

- ✓ Recompensas compartidas. Otra manera de propiciar el apoyo de los empleados al cambio es asegurarse de que ellos obtendrán la suficiente recompensa en la nueva situación. Las recompensas a los empleados llevan

el mensaje siguiente: "Nos interesas. Queremos que tú y nosotros nos beneficiemos con el cambio"

- ✓ Protección a los Empleados. Además de hacer que los empleados participen en las recompensas del cambio, debe garantizarles beneficios ya existentes. Es esencial esa protección a sus trabajadores contra la posible baja de ingresos originada por la introducción de nuevas tecnologías, otros ofrecen nueva capacitación y demoran la instalación de maquinaria que ahorre mano de obra hasta que la rotación normal de personal pueda cubrir el despido de trabajadores. Cuando se realiza un cambio también se garantizan los derechos de antigüedad, las oportunidades de desarrollo y otros beneficios.

- ✓ Comunicación. La comunicación es indispensable para mejorar el apoyo al cambio. Aún cuando solamente una o dos personas de un grupo de diez resultarán afectadas por él, todas deben estar informadas para que se sientan seguras y mantengan el nivel de cooperación en el grupo. La resistencia al cambio puede reducirse ayudando a los empleados a reconocer la necesidad de cambio, y a participar y beneficiarse de él. En resumen, los cinco pasos que se recomiendan a la gerencia para lograr un cambio exitoso, son:

- Hacer solamente los cambios necesarios y útiles. Evitar cambios innecesarios.
- Cambiar por evolución, no por revolución (esto es, gradual, no dramáticamente).
- Reconocer los posibles efectos del cambio e introducirlo al mismo tiempo que se atienden las necesidades humanas del personal.
- Compartir con los empleados los beneficios del cambio.
- Diagnosticar los problemas que quedan después del cambio, y atenderlos.

1.23 Motivación.

Un empleado motivado se desarrolla de forma más eficiente en su trabajo, y el trabajo de un buen líder es darle los motivos necesarios para que el trabajador perciba un

buen ambiente en la organización, lo que le permitirá superarse.

Un modelo de motivación incluye los siguientes aspectos:

- ✓ Ambiente.
- ✓ Oportunidad.
- ✓ Necesidades.
- ✓ Tensión.
- ✓ Esfuerzo.
- ✓ Metas.
- ✓ Comportamiento.
- ✓ Incentivos.
- ✓ Recompensas.
- ✓ Satisfacción de necesidades.

1.23.1 Impulsos Motivacionales

Cada persona tiende a desarrollar ciertos impulsos motivacionales como un producto del medio cultural en el que vive, y estos impulsos afectan la manera en que los individuos ven sus trabajos y manejan sus vidas.

1.23.1.1 Motivación para el Logro

La motivación para el logro es el impulso que tienen algunas personas para superar los retos y obstáculos a fin de alcanzar sus metas.

1.23.1.2 Motivación por Afiliación

La motivación por afiliación es un impulso por relacionarse con las personas en un medio social.
Estas personas trabajan mejor cuando los felicitan por sus actividades favorables.

1.23.1.3 Motivación por Competencia

La motivación por competencia es un impulso por realizar un trabajo de calidad. Estos empleados motivados por la competencia buscan dominar su trabajo, desarrollar habilidades para la solución de problemas.

1.23.1.4 Motivación por Poder.

La motivación por poder es un impulso por influir en las personas y cambiar las situaciones. Los individuos motivados por el poder desean crear un impacto en sus organizaciones y están dispuestos a correr riesgos para lograrlo.

1.23.2 Interpretación de los Modelos Motivacionales:

- ✓ Micro motivación: Es la motivación en el puesto y dentro de la organización. Se centra en la motivación dentro de una organización individual. La idea es cambiar las condiciones dentro de la empresa a fin de incrementar la productividad de los empleados, es decir, motivar a los trabajadores.
- ✓ Macro motivación: El área de interés que se centra en las condiciones del medio fuera de la empresa que influyen en el desempeño en el trabajo, básicamente es un modelo macro motivación. Este medio externo podría tener una gran influencia sobre el desempeño, por ejemplo, apoya la sociedad al trabajo, o se centra en el tiempo libre como un valor primordial? Percibe a los trabajadores de la empresa como ambiciosos alineados o como importantes contribuyentes de la sociedad?, Aumenta la tasa de impuestos conforme se obtiene más dinero debido a una promoción, con lo que se limita el poder de compra?. Todas estas condiciones del medio afectan las recompensas que se obtienen en el trabajo.

- ✓ En vista de que existen dos medios (dentro y fuera de la empresa) que afectan la motivación, ambos deben mejorarse para lograr una mayor motivación. Si las condiciones del puesto no son atractivas, es posible que la motivación sea débil, no importa qué tanto apoyo se reciba del medio externo; aunque también puede ocurrir lo contrario. Si las condiciones del medio no apoyan un mejor desempeño del puesto, la motivación tiende a ser débil, aún cuando las condiciones del puesto sean favorables.

La Dirección no puede por sí sola resolver los problemas de motivación. Debe contar con el apoyo de la sociedad.

1.24 La Ética en los Sistemas de Información

La Ética en la informática estudia la forma de transparentar y idoneizar los métodos que son utilizados para transformar la información, los mecanismos que permiten realizar las transformaciones, la valoración de los modos de comunicación más apropiados entre las personas y los que hacen de la información su filosofía de vida.

La informática como recurso, fundado en la lógica y las matemáticas debe estar sustentada en lo religioso, lo ético y lo económico, produciendo una escala de valores de hechos y formas de comunicación dentro de una sociedad democrática.

Actualmente, los flujos de información o fuentes, como redes informatizadas y medios de radiodifusión, han trastocado los valores naturales, y actúan en forma deficitaria cuando deben responder a los principios éticos y morales naturales de la vida.

El peligro que ello significa, no solo pasa por la transformación o modernización de los sistemas de información, pasa porque no se ha respetado al ser humano en sí, con sus defectos y virtudes y se ha permitido ir chocando contra la ley natural de la vida.
Este enorme cambio tecnológico que se ha producido en el mundo y que nos cuesta adaptarnos a él, no ha tenido en cuenta las necesidades principales del ser, y está destruyendo en forma avanzada a las generaciones que se deben adoptar a ella.

Los problemas que plantea la difusión acelerada de la información no son en esencia diferentes a los que plantea el desarrollo de toda ciencia. Son problemas morales que han ido sumergiendo a una sociedad en una profunda corrupción; debido a las políticas neoconservadoras y poco claras que han tapado la transparencia y la honestidad de las antiguas generaciones.

1.24.1 Los Valores Éticos en los Sistemas de Información

Analizando la influencia de la ética en los sistemas de información como se mencionó anteriormente, se pueden sacar muchas conclusiones debido a la enorme cantidad de campos que la misma abarca ya que el ser éticos y que los medios de comunicación lo sean depende de cada uno, depende de la sociedad en conjunto.

Es por ello, que la información debe ser clara y precisa, trasparente y real posible, no nos pueden vender algo que no haya sido rectificado y tiene el sello de calidad. Tampoco hay que dejar de lado que la información es una herramienta fundamental para el conocimiento del ser humano. Mientras tanto esa información se maneje dentro de los parámetros morales y se respeten los principios éticos que dentro de un marco normativo es aceptado por la sociedad, entonces estaremos llevado por el camino correcto, y esa información estará basada en la verdad y le permitirá al ser humano enriquecerse intelectualmente, tomando esa información como elemento de su propio conocimiento siéndole útil para la convivencia con los demás.

Por todo esto se deberán asimismo modificar los sistemas de gestión, aspirando a la calidad total de la información simplificando la administración monopólica de los sistemas de información y restableciendo la Ética y la Moral en la función pública y privada. Los recursos humanos deberán resultar de selecciones que aseguren idoneidad y excelencia para la función. Para garantizar calidad en la gestión se realizarán controles independientes y eficaces que permitan reducir al más bajo nivel posible de corrupción.

Pero lo más importante y concluyendo con este concepto será necesario y de suma utilidad que para poder respetar y seguir los pasos de un marco normativo correcto la sociedad y los sistemas e información en su conjunto deberán hacer cumplir los siguientes requisitos, para que podamos luchar contra la corrupción y empezar a trasparentar los lados oscuros de la Administración pública y privada.

Los siete requisitos a cumplir son los siguientes:

- ✓ Un entorno social favorable para la democracia.
- ✓ Una ley constitucional que regularice los sistemas de información.
- ✓ Una infraestructura técnica adecuada para su funcionamiento.
- ✓ Un financiamiento confiable y trasparente.
- ✓ Medios de producción adecuados.

- ✓ Colaboradores motivados y capacitados y
- ✓ Un programa aceptado por el espectador.

Si logramos poder hacer cumplir estos requisitos, podremos lograr una sociedad moral y éticamente fuerte en todos los sectores, una justicia independiente y un estado trasparente, ya sea en un manejo equitativo de los recursos financieros como en el buen comportamiento de sus funcionarios públicos.