UNIVERSIDAD DE SOTAVENTO A.C.

ESTUDIOS INCORPORADOS A LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INFORMÁTICA

"SEGURIDAD FÍSICA EN LOS CENTROS DE COMPUTO DE LA UNIVERSIDAD DE SOTAVENTO"

TESIS PROFESIONAL

QUE PARA OBTENER EL TÍTULO DE

LICENCIADO EN INFORMÁTICA

PRESENTA:

ERICK CHAN LUNA

ASESOR DE TESIS:

LIC. RAÚL DE JESUS OCAMPO COLIN

COATZACOALCOS, VERACRUZ JULIO 2008

Dedicatoria

Dios te agradezco por haberme dado la vida, y la fuerza necesaria para poder alcanzar mis objetivos y por guiar cada uno de mis pasos, por darme la oportunidad de pensar y la inteligencia para aprender y así poder alcanzar este sueño.

A mis padres, y mis hermanas que han sido el ejemplo más grandioso, por su extraordinario apoyo que me brindaron a lo largo de toda mi vida como estudiante y por la confianza y el cariño que siempre me han demostrado, por haber sido la motivación y apoyo para lograr una meta más en mi vida.

También doy las gracias a mis amigos que en momentos difíciles estuvieron conmigo y demostraron su apoyo incondicional.

A mis maestros, por ayudarme en mi formación profesional y por guiarme en realización de este trabajo.

Índice

Índice de tablas y figuras

Problema

Conocer aquellos riesgos físicos potenciales en un centro de cómputo, y qué medidas se deben tomar para que la población estudiantil este en un área segura.

Hipótesis

La seguridad física puede convertirse en el eslabón más débil de la cadena en un centro de cómputo, es necesario tener en cuenta diversas medidas de seguridad para evitar riegos o accidentes que afecten la integridad de las Personas y a los Sistemas de Información.

Objetivo general

Establecer los procedimientos y recursos para lograr un sistema de Seguridad Física de alto rendimiento en un Centro de Cómputo.

Objetivos específicos

- Dar las adecuadas recomendaciones sobre cómo tratar los equipos de cómputo y de facilidad de comunicación de datos.
- Hacer tomar conciencia a los usuarios del centro de cómputo la importancia de la seguridad.
- Contribuir a generar conciencia en muchos de los especialistas en seguridad física e informática que pueden ser una de las causas principales de la perdida de información y riesgo al personal.
- Dar a conocer diversas tecnologías que existen actualmente para combatir la inseguridad en los centros de cómputo e incluso que pueden ayudar a la Universidad en su totalidad.

Justificación

El tema de seguridad física en centros de cómputo es un tema que muchas veces se deja de lado dando prioridades a la seguridad lógica, siendo que la seguridad física es de suma importancia. Con una buena previsión y teniendo instalaciones adecuadas, se pueden prevenir muchos accidentes o en caso de que algo suceda, minimizar el impacto sobre las mismas.

Al ser un tema muy complejo se darán a conocer diversos conceptos y referencias sobre cuales pueden ser los puntos débiles en un centro de cómputo para así poder tomar todas las medidas necesarias para evitar daños a las instalaciones, al personal y al equipo con el que se trabaja.

Actualmente tanto los sistemas de información como las bases de datos son de gran relevancia para cualquier institución y en el caso de la Universidad de Sotavento es fundamental salvaguardar estos activos.

Introducción

Hoy[1] en día, se tiene como punto de referencia a la seguridad como la protección contra las amenazas virtuales, sin embargo existen otros niveles de vulnerabilidad en los que es necesario prepararnos para evitar pérdidas de información o paros en el funcionamiento de la compañía como los peligros y amenazas físicas. En ese sentido, es importante contar con sistemas de seguridad física, divida en dos segmentos: la externa (cercados, sistemas de alarma antirrobos, tecnología de CCTV) y la interna (detectores de humo, sistema de supresión, cajas fuertes y bóvedas) para garantizar una protección basada en niveles de protección.

Del mismo modo es importante "no poner todos los huevos en la misma canasta", pues ante la posibilidad de catástrofes naturales es importante contar con respaldos resguardados en otras áreas o locaciones. "Hay que tomar en cuenta que la pérdida de información no sólo se da por la falta de protecciones de antivirus y la generación de respaldos, hay cientos de factores externos que pueden detener o hasta estropear nuestro funcionamiento como accidentes, robos, desastres naturales, por mencionar algunos. La seguridad física se debe considerar como un complemento de la seguridad informática".

Para poder evitar estas amenazas o sus efectos más devastadores (ya que es imposible evitar un terremoto) para esto es necesario saber que hacer en casos de una emergencia.

En la protección y salvaguarda de los centros de computo una planeación de las instalaciones físicas requiere de un análisis y diseño detallado el cual se hace con anticipación para prevenir riesgos y posibles fallas, esta se lleva acabo tomando en cuenta importantes factores como son el área y la ubicación del centro de computo al igual que la ubicación de las áreas donde van a estar los diferentes departamentos de informática, considerando factores importantes como seguridad, instalaciones eléctricas y ruido, lo cual es primordial para la seguridad y el buen uso del centro de computo y sus diversas áreas de soporte, análisis,

[1] *Seminario "Seguridad en Redes 2006"/ InfoWorld México/ Jaime Oliva Garduño*

captura de datos entre otras, al igual que los principales requisitos como la conexión a tierra física, reguladores de voltaje, aire acondicionado y todo lo que tenga que ver con seguridad para el mismo.

En estos capítulos se dará gran énfasis a los diferentes aspectos relacionados a la seguridad, se tocara el tema de los tipos de desastres que podrían afectar a nuestro entorno y se hace referencia a que elementos pueden ocasionar diversos accidentes como un incendio, tener las herramientas necesarias para combatirlo y el tipo de personal capacitado.

En general en caso de querer poner un centro de cómputo sirve como orientación para ver cuales son los puntos más débiles que se tienen y que pueden ocasionar daños.

En el caso de la Universidad de Sotavento, al ya tener una estructura para los centros de computo únicamente se reforzara lo que ya se tiene para que exista una mejor rendimiento, también se tocan otros temas que pueden afectar como pueden ser el robo o sabotaje y cómo podemos prevenirlo, de igual forma si se tiene un mayor presupuesto se pueden integrar a un centro de computo diversos tipos de protecciones adicionales que pueden ser, vigilancia con perros guardianes, cámaras de video para monitorear las entradas y salidas de personal para verificar tanto los accesos autorizados y los no autorizados, esto con el fin de garantizar el desarrollo de las actividades humanas ofreciendo seguridad informática.

La estructura de la tesis básicamente se compone de siete capítulos, cuyo contenido se resume en los siguientes párrafos:

El Primer capítulo, Resumen Ejecutivo contiene una introducción sobre la Universidad de Sotavento, su misión, visión, organigramas, objetivos del centro de cómputo y su problemática.

El Segundo capítulo, Generalidades trata el tema de que tan importante es que la Universidad cuente con un centro de cómputo seguro, para esto se tiene que hacer un análisis de riesgos haciendo varios cuestionamientos sobre la situación actual del centro de cómputo.

El Tercer capítulo, Tipos de amenazas o Riesgos en este se mencionan las principales amenazas a las que está expuesto un centro de cómputo como: Incendios, inundaciones y condiciones climatológicas además de otros riesgos como son: robo, fraude y sabotaje.

El Cuarto capítulo, Infraestructura tiene que ver con las instalaciones físicas de la Universidad de Sotavento y otros conceptos como son: Instalación eléctrica, cableado, aire acondicionado y emisiones electromagnéticas.

En el Quinto capítulo, Prevención y Salvaguarda se menciona la importancia de tener un control de las personas que entran y salen de las instituciones, para esto son necesarios diversos elementos como: emplear servicio de vigilancia (guardias), control de acceso a vehículos, detectores de metales, sistemas biométricos, seguridad con animales, circuitos cerrados de televisión, etcétera.

El Sexto capítulo, Alternativas para mejorar la seguridad física en los centros de cómputo de la Universidad de Sotavento aquí se mencionan tres alternativas explicando cada una de ellas además de sus ventajas y desventajas al final se elegirá a una como la más adecuada.

El Séptimo capítulo, Recomendaciones para la seguridad física en los centros de cómputo de la Universidad de Sotavento. Se harán recomendaciones básicas de seguridad, control de accesos, primeros auxilios y mantenimiento de los equipos de cómputo para evitar futuros riesgos.

También se establecerá como actuar ante algunos tipos de desastres como el fuego, inundaciones, sismos. Otros puntos Importantes serán como tratar de evitar los robos, sabotajes y como actuar en caso de que sucedan acciones hostiles.

Marco Teórico

En los últimos años, las tecnologías de la información y la comunicación han revolucionado la vida social en numerosos aspectos: científicos, comerciales, laborales, profesionales, escolares, etcétera.

La tecnología avanza a una velocidad vertiginosa y las leyes, en especial el Derecho Mexicano, se ha quedado muy rezagado en la regulación de una materia que lo ha rebasado totalmente.

En el Artículo 231 del Código Penal para el Distrito Federal se menciona “Que individuo que obtenga algún beneficio para sí o para un tercero, por cualquier medio acceda, entre o se introduzca a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores, independientemente de que los recursos no salgan de la Institución.” Código Penal Federal, artículos 211 bis 1 a 211 bis 7

A pesar de que existen algunas leyes el abuso y fraudes quedan impunes. Los avances no son suficientes, todavía no existe una verdadera protección contra ataques maliciosos

Hace dos años, en México se acusó a un empleado de una maquiladora, de enviar por correo electrónico información secreta a la competencia. La firma confiscó la computadora del afectado y la llevó ante un juez, casi 40 días después del supuesto fraude.

La compañía tenía dos factores principales en su contra: no cancelaron inmediatamente la cuenta de correo electrónico del empleado y había transcurrido mucho tiempo entre que se cometió la acción y se presentaron las pruebas, así que no se pudo demostrar que la evidencia no se había modificado.

Además, al evaluar las políticas de seguridad de la empresa se encontró que no había privacidad en el uso de los equipos y, lo peor, la gente compartía sus claves de acceso (passwords).

Al juez se le entregó un expediente de 60 páginas, de las cuales 10 eran la descripción del incidente y le resto un curso de tecnologías de la información, así como de seguridad informática. La intención es que las personas que trataran el caso, a nivel federal aprendieran un poco sobre el tema.

El empleado resultó inocente y ganó bajo la premisa de despido injustificado, gracias a que su abogado estaba asesorado por un perito en delitos digitales.

"En materia legal, para casos de delitos informáticos, estamos en pañales", [2]dijo Jorge Garibay, director de servicios profesionales de Xertix y miembro de ISACA, Information Systems Audit and Control Association. Por eso es recomendable una protección lógica (software) y física (hardware) de los sistemas de información.

- En Estados Unidos, Francia y Japón hay leyes para operaciones financieras, así como el manejo y tratamiento de información en medios magnéticos.
- En Canadá existe una sección del código criminal que culpa a cualquiera, sin autorización, que modifique datos o cause la acción.
- Los países del G8 firmaron un acuerdo el año pasado para establecer principios internacionales para el manejo de la evidencia computacional.
- La evidencia digital no puede ser modificada, cualquier persona que accese a ella debe estar certificado y cualquier movimiento de la misma debe ser documentada

[2] *"ISACA"/ http://www.isaca.org*

Capitulo 1. Resumen ejecutivo.

1.1. Introducción.

La Universidad de Sotavento A.C. es una institución privada de Educación Superior y de interés social.

El principal objetivo de la Universidad es impartir educación superior para formar profesionistas, investigadores, profesores universitarios, así como el conservar, crear y transmitir la cultura, en beneficio y para el desarrollo económico y social, con el más alto nivel de calidad académica.

La Universidad de Sotavento esta vinculada permanentemente con la sociedad, para incidir en la solución de sus problemas, en el planteamiento de alternativas para el desarrollo, sustentadas en el avance de la ciencia y la tecnología, proporcionándole los beneficios de la cultura y obteniendo de ella la reciprocidad y los apoyos necesarios para su fortalecimiento.

La educación que imparte la Universidad de Sotavento, está sustentada por bases acordes con las nuevas tendencias y condiciones del desarrollo, y con el proceso de modernización del país; siendo formal y no formal. Para el caso de la educación formal, que implica un reconocimiento académico, se podrán adoptar las modalidades de escolarizada y/o no escolarizada teniendo en cuenta que la Universidad de Sotavento cuenta con dos afiliaciones que son la Universidad Nacional Autónoma de México (UNAM) y la Secretaría de Educación Pública (SEP). Siendo la primera del orden escolarizado y la segunda del orden no escolarizado.

Con estas dos modalidades se tiene la misión de formar profesionistas de excelencia académica, de conservar, generar ó transmitir el conocimiento científico, humanístico, artístico y tecnológico, mediante la docencia, la investigación, las actividades deportistas y la difusión de la cultura.

1.2. Visión.

La visión de la Universidad de Sotavento es formar profesionistas de una excelencia académica, capaces de asumir el compromiso que tienen con la sociedad, de conservar, generar y transmitir el conocimiento científico, humanístico, artístico y tecnológico, mediante la docencia, la investigación y la difusión de la cultura.

1.3. Misión.

Asegurar la generación de licenciados preparados en el área con los lineamientos de calidad, preparación, creatividad y competencia, garantizando:

- Estudiantes preparados.
- Nivel competitivo.
- Capacitación continúa.
- Creatividad y calidad en el desarrollo de proyectos.

La Universidad de Sotavento, A.C. cuenta con diferentes carreras tales como: Licenciatura en Arquitectura, Licenciatura en Informática, Licenciatura en Administración, Licenciatura en Contaduría, Licenciatura en Psicología, Licenciatura en Educación Física, Licenciatura en Derecho, Ingeniería Industrial e Ingeniería en Sistemas Computacionales, actualmente cuenta con aproximadamente 1500 alumnos inscritos en las diferentes carreras.

1.4. Organigrama general de la Universidad de Sotavento.

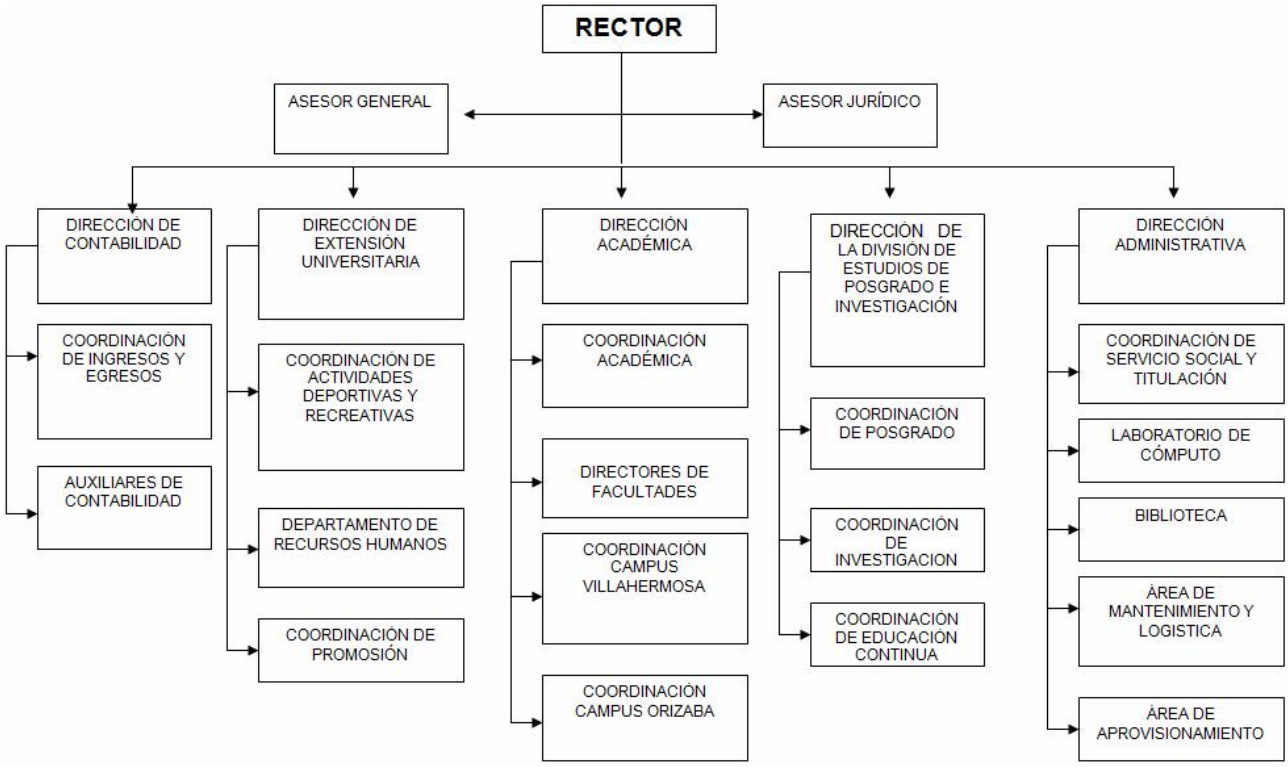


Figura 1.4. Organigrama general de la Universidad de Sotavento

1.5. Coordinación del centro de cómputo.

Debido a la prioridad que tiene la computadora hoy en día, los sistemas educativos necesitan proporcionar las herramientas al alcance de los docentes para el aprovechamiento y uso de los sistemas y software aplicados a sus perfiles educativos.

Es por esto que la Universidad de Sotavento, A.C. (U.S.) cuenta con un centro de cómputo (C.C.) que permite abastecer este servicio a más de 1,500 estudiantes de las diez diferentes carreras que la conforman tales como: Arquitectura, Pedagogía, Informática, Derecho, Ingeniería en Sistemas Computacionales, Educación Física, por mencionar algunas.

Para esto se necesita y requiere de una administración y control absoluto sobre los equipos que pertenecen a este departamento además de que el grupo universitario se encuentra conformado por dos Instituciones Universidad de Sotavento y la Universidad Istmo-Americana dando un equivalente de dos centros de computo y un aproximado de 116 equipos a administrar, con los cuales se proporcionan los diferentes servicios que los docentes requieran.

El centro de computo de la Universidad de Sotavento, es un departamento que permite dentro de la estructura organizacional el control y la administración del equipo de computo, siendo que provee los servicios necesarios de preparación de clases, obtención de Internet, servicio de impresión, coordinación de practicas docentes a el alumnado, recopilación de información de investigación, es un departamento independiente en el registro, control, mantenimiento y proporción de servicios propios, mencionando que provee el soporte técnico apropiado a los diferentes departamentos tales como: Dirección Administrativa, Dirección Académica, Coordinación de Directores, Prefectura, Control de Pagos y el propio Centro de computo.

Con lo anterior el Centro de Cómputo requiere el control absoluto sobre el inventario de equipos y piezas de mantenimiento preventivo así como las de soporte técnico, obteniendo un control eficiente sobre las piezas faltantes, en reparación, obsoletas ó en garantía, creando un registro de cada una de ellas, así como de una bitácora que permite el registro de las fallas de cada equipo, se necesita la coordinación de los horarios de los profesores que acceden al Centro de Cómputo para la impartición de sus cátedras, el control de licencias y del software necesario en cada semestre que se necesite implementar en los equipos retirando el que no se ocupe con la intención de mantener al 100% el uso adecuado de los ordenadores.

Tomando a consideración lo anterior se menciona que la Universidad de Sotavento no solo cuenta con un campus en Tesoro, sino que además posee campus en la Ciudad de Villahermosa, Orizaba y mantiene un grupo universitario con la Universidad Istmo Americana por lo que el campus de Román Marín pertenece a la Universidad de Sotavento, por esto la Coordinación del Centro de Computo tiene la obligación de satisfacer las necesidades que se presenten en cualquier departamento cuando exista una falla, se necesite reemplazarlo de manera temporal o definitiva mientras se realiza un diagnostico que requiera un mantenimiento correctivo o preventivo y en caso de no tener compostura y haber expirado su garantía se requerirá el reemplazo de ese ordenador.

De esto que exista un control adecuado y eficiente por cada campus de la Universidad de Sotavento, así como llevar diversos registros para poder obtener información en el momento que rectoría lo requiera.

Para poder controlar y registrar todas estas actividades realizadas en el control del alumnado y la administración de la Institución Educativa, Universidad de Sotavento cuenta con una Coordinación del Centro de Computo (CCC), la cual proporciona el soporte necesario a los requerimientos de todas las áreas de la

Institución Educativa. Los departamentos en que se divide la Coordinación, son los siguientes:

- Atención a usuarios.
- Soporte Técnico
- Redes
- Analistas
- Programadores
- Administradores de Bases de Datos.

Además de las actividades que abarca la Coordinación del Centro de Computo en el campus generado en la colonia Tesoro de la Ciudad de Coatzacoalcos, la Universidad de Sotavento cuenta con diferentes campus en otras ciudades como: Coatzacoalcos-Istmo, Villahermosa, y Orizaba, debido a esto el campus Tesoro proporciona el soporte necesario a los diferentes campus en base a las políticas establecidas en la Centro de Cómputo.

Analizando la situación actual del mercado, se necesita reafirmar nuestro compromiso con los cambios, a fin de mejorar y elevar los niveles de productividad y calidad en forma continúa, manteniendo un servicio de excelentes niveles competitivos.

De esto surge la importancia que representa para nuestra Institución la planificación de sistemas de información y la aplicación de la tecnología necesaria para lograr los objetivos de la Institución, ya que el principal reto es mejorar la calidad, reduciendo el costo de las soluciones basadas en la computadora utilizando los medios proporcionados por nuestra Institución para la mejora continua.

Objetivo general.

Administrar, controlar y organizar la coordinación del Centro de Cómputo, además de tener a su cargo el desarrollo de proyectos y servicios para la propia institución como para clientes externos de la misma.

Objetivos específicos.

- Mantener actualizado el Inventario del Centro de Cómputo.
- Actualizar nuestros equipos para el abastecimiento de las necesidades de los estudiantes.
- Actualizar al personal del Centro de Cómputo, para el cumplimiento de sus funciones.
- Mantener los equipos del personal administrativo en óptimas funciones y condiciones.
- Administrar el equipo de computo con el que cuenta la Universidad de Sotavento, A.C.
- Proporcionar un buen servicio al estudiantado y profesorado de la Institución.
- Analizar las necesidades del profesorado en relación al software a utilizar.
- Lograr una administración adecuada y completa de los diversos servicios otorgados por la Universidad de Sotavento
- Mantener a la vanguardia con proyectos de crecimiento a la Universidad y la Coordinación en particular.
- Permitir un trabajo colectivo y coordinado con la Dirección Administrativa.
- Impulsar y dirigir al personal de la coordinación del Centro de cómputo.

Misión

Ofrecer servicios de vanguardia, todo ello con la finalidad de permitir mejor control y calidad en el servicio otorgado por la Universidad de Sotavento, A.C. de la Ciudad de Coatzacoalcos, Veracruz.

Visión

Lograr ser el mejor centro de computo de los campus de la Universidad de Sotavento, A.C. además de permitir tener alcance y trascendencia en todo el estado.

1.6. Organigrama del centro de cómputo.

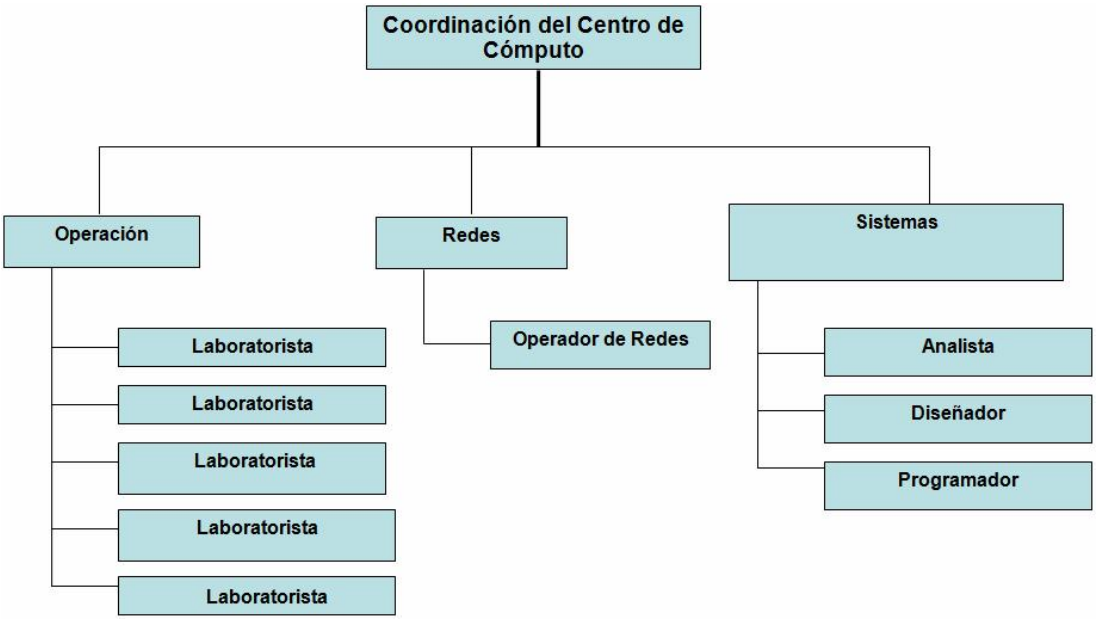


Figura 1.6. Organigrama del centro de cómputo.

1.7. Problemas más comunes en el centro de cómputo:

En el Centro de Cómputo de la Universidad de Sotavento se han detectan diversos problemas de los cuales los más importantes son:

- Robos de memorias RAM, discos duros, mouse, teclados etcétera.

En el caso de los robos o extravió de objetos, es porque los alumnos entran con mochilas haciendo demasiado fácil que puedan ocultar o esconder los artículos del centro de computo y así llevárselo sin que nadie se de cuenta.

- Horarios

A los horarios muchas veces hay conflictos entre dos grupos que tienen asignado el mismo horario para el centro de computo, esto pasa debido a que al profesor en el inicio del semestre se le asignan un rol semanal posteriormente

quedan inconformes y logran cambiarlo, esto hace que coincida con el horario asignado de otro profesor.

- Inmobiliario

Respecto al inmobiliario, no es el mas adecuado los equipos únicamente están sobre mesas y están demasiado juntos ocasionando el deterioro acelerado de las mesas. Se observa que las mesas están dobladas o pandeadas. Y el hecho de ser de plástico generan mucha estática que un tiempo prolongado afecta a los equipos de cómputo. En cuanto a las sillas no son ergonómicas ocasionado cansancio y malestar a los usuarios.

- Virus

En cuanto a los virus se tiene una infinidad de estos. Donde dañan la información y equipos de almacenamiento; además de ocasionar trastornos al sistema operativo.

- Falta de Software

Escasez de software y licencias. Los centros de computo no cuentan con licencias propias, por lo regular son versiones FREE, TRIAL o en el peor de lo casos software pirata. Y aun así con esto, no se cuenta con todo el software necesario para que los alumno pueden realizar sus trabajos y cubrir los programas académicos. Es conveniente mencionar que normalmente se instalan los programas conforme se vayan a usar lo que ocasiona mucha pérdida de tiempo.

- Falla de Internet

La mayoría de las veces no está disponible la conexión a Internet, afectando a todo los alumnos. Y teniendo una gran población de equipos portátiles tanto de alumnos como de docentes es muy común que estos estén inconformes con el servicio. Además que se restringen los accesos a algunos sitios de ocio.

- Cambio de equipo sin autorización:

Es muy común que los equipos asignados a los dichos centros no se encuentran completos, siendo los principales faltantes mouse, teclado, etc. como consecuencia se tiene que quitar el mouse o teclado de otro equipo.

- Vandalismo

Se ha detectado que en ocasiones el alumno destroza equipos de cómputo, por ejemplo quita las bolitas de los mouse o bien cambia las teclas en diferente lugar en un teclado.

- Accesos no autorizados

Debido a que no existe ningún tipo de restricción tanto del acceso al centro de cómputo (física) como a los equipos de cómputo (lógica), cualquier persona puede utilizar las computadoras y dispositivos disponibles.

- No se usa el equipo para fines académicos.

Al no tener un control sobre las actividades que se realizan, el alumnado tiende a jugar en horas de clases y/o a “chatear” o visitar páginas WEB de ocio.

- Fallas Eléctricas

En la actualidad no se tiene un buen equilibro de las cargas y además se tiene sobre cargados los circuito eléctricos. La forma en que son conectadas los equipos es en serie entre los mismo reguladores, ocasionado la sobrecarga del circuito. No se cuenta con tierras físicas adecuadas. Es muy frecuente que los equipos se quemen o tengan fallas irreparables debido a estos.

1.8. Factores de riesgos en el centro de cómputo:

Para cada riesgo, se determina la probabilidad del factor de riesgo. Se mencionan algunos factores de riesgo en el centro de cómputo de la Universidad de Sotavento.

- Factor de riesgo bajo
- Factor de riesgo muy bajo
- Factor de riesgo alto
- Factor de riesgo muy alto
- Factor de riesgo medio

Tipo de Riegos	Factor de Riesgo
Robo	Alto
Vandalismo	Medio
Fallas en los equipos	Alto
Acción de Virus	Alto
Terremotos	Bajo
Accesos no Autorizados	Alto
Robo de datos	Bajo
Fuego	Bajo
Fraude	Muy Bajo

Tabla 1.8. Factores de riesgos en el centro de cómputo.

Capitulo 2. Generalidades.

2.1. Seguridad física.

"Un experto es aquel que sabe cada vez más sobre menos cosas, hasta que sabe absolutamente todo sobre nada. Es la persona que evita los errores pequeños mientras sigue su avance inexorable hacia la gran falacia"[3]

Es muy importante ser consciente que por más que nuestra empresa sea la más segura desde el punto de vista de ataques externos, piratas informáticos(Hackers), virus, etcétera, la seguridad de la misma será nula si no se ha previsto como combatir un incendio o como evitar robos.

La seguridad física es una rama de la seguridad informática que se preocupa de establecer distintos tipos de controles sobre activos físicos. Dentro de una organización podemos ubicar la seguridad física entre los niveles estratégicos y operativos.

Dentro de los factores a proteger están:

-Humanos:

Corresponde a todos los administradores, usuarios y personal en general que pertenecen a una organización.

- Tecnológicos:

Recursos tecnológicos necesarios para el funcionamiento de los servicios como Hardware, software, servidores, Internet, equipos de red y datos, etcétera.

- Estructurales:

Edificios, centro de datos (datacenters), oficinas, bodegas, etcétera.

Sobre estos factores siempre existirán sucesos que amenacen la seguridad (integridad, confidencialidad, disponibilidad) de los mismos. Estos sucesos se conocen como amenazas y dentro de las más inminentes podemos distinguir:

[3] *Webwer/ Corolario de Weinberger/ (Leyes de Murphy).*

- Desastres naturales

Tormentas eléctricas, terremotos, inundaciones y otros problemas ligados principalmente a situaciones ambientales.

- Desastres del entorno

Incendios, temperaturas extremas, cortes de energía.

La seguridad física “es uno de los aspectos más olvidados a la hora del diseño de un sistema informático. Si bien algunos de los aspectos tratados a continuación se prevén, otros, como la detección de un atacante interno a la empresa que intenta a acceder físicamente a una sala de operaciones de la misma, no”[4]. Esto puede derivar en que para un atacante sea más fácil lograr tomar y copiar una cinta de la sala, que intentar acceder vía lógica a la misma.

Así, la Seguridad Física consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial". Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

2.2. Cómo implementar una política de seguridad.[5]

Generalmente, la seguridad de los sistemas informáticos se concentra en garantizar el derecho a acceder a datos y recursos del sistema configurando los mecanismos de autentificación y control que aseguran que los usuarios de estos recursos sólo posean los derechos que se les han otorgado.

Los mecanismos de seguridad pueden sin embargo, causar inconvenientes a los usuarios. Con frecuencia, las instrucciones y las reglas se vuelven cada vez más complicadas a medida que la red crece. Por consiguiente, la seguridad informática debe estudiarse de modo que no evite que los usuarios desarrollen

4 "Seguridad en Unix y Redes"/ HUERTA, Antonio Villalón/ Open Publication License
5 Seguridad-Introducción al seguridad informática/Kioskea

usos necesarios y así puedan utilizar los sistemas de información en forma segura.

Por esta razón, uno de los primeros pasos que debe dar una compañía es definir una política de seguridad que pueda implementar en función a las siguientes cuatro etapas:

- Identificar las necesidades de seguridad y los riesgos informáticos que enfrenta la compañía así como sus posibles consecuencias
- Establecer niveles de prioridad e importancia sobre esta información Proporcionar una perspectiva general de las reglas y los procedimientos que deben implementarse para afrontar los riesgos identificados en los diferentes departamentos de la organización
- Controlar y detectar las vulnerabilidades del sistema de información, y mantenerse informado acerca de las debilidades en las aplicaciones y en los materiales que se usan
- Definir las acciones a realizar y las personas a contactar en caso de detectar una amenaza

La política de seguridad comprende todas las reglas de seguridad que sigue una organización (en el sentido general de la palabra). Por lo tanto, la administración de la organización en cuestión debe encargarse de definirla, ya que afecta a todos los usuarios del sistema.

En este sentido, no son sólo los administradores de informática los encargados de definir los derechos de acceso sino sus superiores. El rol de un administrador de informática es el de asegurar que los recursos de informática y los derechos de acceso a estos recursos coincidan con la política de seguridad definida por la organización.

Es más, dado que el/la administrador/a es la única persona que conoce perfectamente el sistema, deberá proporcionar información acerca de la seguridad a sus superiores, eventualmente aconsejar a quienes toman las decisiones con respecto a las estrategias que deben implementarse, y constituir el punto de

entrada de las comunicaciones destinadas a los usuarios en relación con los problemas y las recomendaciones de seguridad.

La seguridad informática de una compañía depende de que los empleados (usuarios) aprendan las reglas a través de sesiones de capacitación y de concientización.

2.3. Etapas para implementar un sistema de seguridad.

Para dotar de medios necesarios para elaborar un sistema de seguridad se debe considerar los siguientes puntos:

- Sensibilizar a los ejecutivos de la organización en torno al tema de seguridad.
- Se debe realizar un diagnóstico de la situación de riesgo y seguridad de la información en la organización a nivel software, hardware, recursos humanos, y ambientales.
- Elaborar un plan para un programa de seguridad.

2.4. Análisis de riesgos.

En el manual de la Tecnología de la Información ISO/IEC 17799[6], se describe el análisis de riesgos como el proceso mediante el cual se identifican las amenazas y las vulnerabilidades en una organización, se valora su impacto y la probabilidad de que ocurran con el fin de generar controles que minimicen los efectos de los riesgos

El objetivo del análisis de riesgo es tener la capacidad para:

- Evaluar y manejar los riesgos de seguridad
- Tomar las mejores decisiones en seguridad informática
- Enfocar los esfuerzos en la protección de los activos

[6] *Code of practice for information security management*

El análisis de riesgos supone más que el hecho de calcular la posibilidad de que ocurran cosas negativas. Se ha de poder obtener una evaluación económica

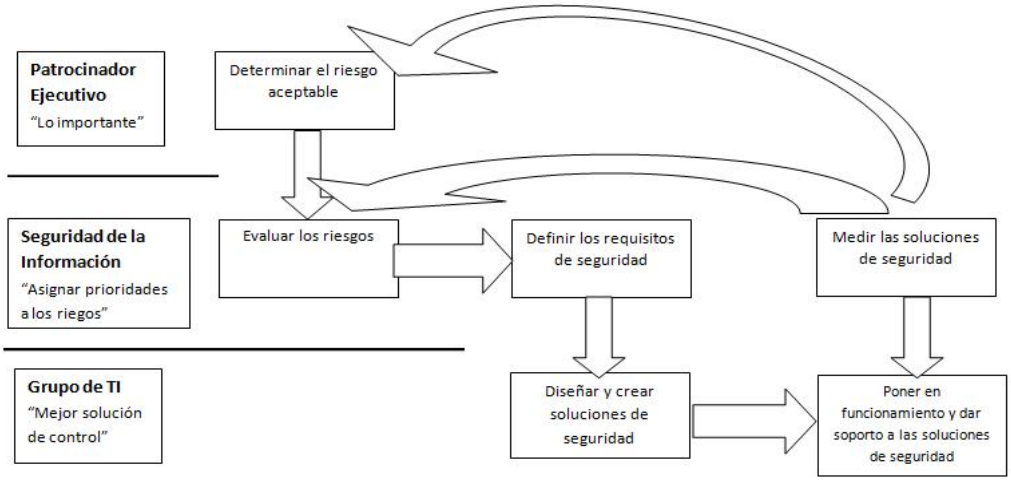


Figura 2.4.- El ciclo del análisis de riesgo

del impacto de estos sucesos negativos. La evaluación de riesgos y presentación de respuestas debe prepararse de forma personalizada para cada organización.

Algunos de los beneficios del análisis de riesgo son:

- Asegurar la continuidad operacional de la organización
- Aprender a manejar las amenazas y riesgos críticos
- Mantener una estrategia de protección y de reducción de riesgos
- Justificar una mejora continua de la seguridad informática
- Permite que la seguridad se convierta en parte de la cultura de la organización, incrementando la conciencia de seguridad en todos los niveles
- Brinda criterios para el diseño y evaluación de planes de contingencia

La evaluación de riesgos supone imaginarse lo que puede ir mal y a continuación estimar el coste o las pérdidas en caso de que así sea. Se ha de tener en cuenta la probabilidad de que sucedan cada uno de los problemas

posibles. De esta forma se pueden priorizar los problemas y su coste potencial desarrollando un plan de acción adecuado.

El análisis de riesgos supone responder a preguntas del tipo:

- ¿Qué puede ir mal?
- ¿Con qué frecuencia puede ocurrir?
- ¿Cuáles serían sus consecuencias?
- ¿Qué fiabilidad tienen las respuestas a las tres primeras preguntas?

En lo fundamental la evaluación de riesgos que se ha de llevar a cabo ha de contestar, con la mayor fiabilidad posible, a las siguientes preguntas:

- ¿Qué se intenta proteger?
- ¿Cuál es su valor para uno o para la organización?
- ¿Frente a qué se intenta proteger?
- ¿Cuál es la probabilidad de un ataque?

El o los responsables de la oficina de informática se sentarán con los responsables de las áreas y realizarán el siguiente conjunto de puntualizaciones.

Riesgos en la seguridad informática a los que se enfrenta la Institución:

- Al fuego, que puede destruir los equipos y archivos.
- Al robo común, llevándose los equipos y archivos.
- Al vandalismo, que dañen los equipos y archivos.
- A fallas en los equipos, que dañen los archivos.
- A equivocaciones, que dañen los archivos.
- A la acción de virus, que dañen los equipos y archivos.
- A terremotos, que destruyen el equipo y los archivos.
- A accesos no autorizados, filtrándose datos no autorizados.
- Al robo de datos, difundiéndose los datos sin cobrarlos.

Luego de elaborar esta lista, el personal de la Institución estará listo para responder a los efectos que estos riesgos tendrán para su Institución.

¿Qué probabilidad hay de que tenga efecto alguno de los riesgos mencionados?

- Al fuego, que puede destruir los equipos y los archivos
- ¿La Institución cuenta con protección contra incendios?
- ¿Se cuenta con sistemas de aspersión automática?
- ¿Diversos extintores?
- ¿Detectores de humo?
- ¿Los empleados están preparados para enfrentar un posible incendio?
- ¿En que tipo de vecindario se encuentra la Institución?
- ¿Hay venta de drogas?
- ¿Las computadoras se ven desde la calle?
- ¿Hay personal de seguridad en la Institución?
- ¿Cuántos vigilantes hay?
- ¿Los vigilantes, están ubicados en zonas estratégicas?
- Al vandalismo, que dañen los equipos y archivos
- ¿Existe la posibilidad que un ladrón desilusionado o frustrado cause daños?
- ¿Hay la probabilidad que causen algún otro tipo de daño intencionado?
- A fallas en los equipos, que dañen los archivos
- ¿Los equipos tienen un mantenimiento continuo por parte de personal calificado?
- ¿Cuáles son las condiciones actuales del hardware?
- ¿Es posible predecir las fallas a que están expuestos los equipos?
- A equivocaciones que dañen los archivos
- ¿Cuánto saben los empleados de computadoras o redes?
- Los que no conocen del manejo de la computadora, ¿saben a quién pedir ayuda?

- Durante el tiempo de vacaciones de los empleados, ¿qué tipo de personal los sustituye y qué tanto saben del manejo de computadoras?
- A la acción de virus, que dañen los archivos
- ¿Se prueba software en la oficina sin hacerle un examen previo?
- ¿Está permitido el uso de disquetes en la oficina?
- ¿Todas las máquinas tienen unidades de disquetes?
- ¿Se cuentan con procedimientos contra los virus?
- A terremotos, que destruyen los equipos y archivos
- ¿La Institución se encuentra en una zona sísmica?
- ¿El edificio cumple con las normas antisísmicas?
- Un terremoto, ¿cuánto daño podría causar?
- ¿Cuánta competencia hay para la Institución?
- ¿Qué probabilidad hay que un competidor intente hacer un acceso no autorizado?
- ¿Contamos con Sistemas de Seguridad en el Correo Electrónico o Internet?
- Al robo de datos; difundiéndose los datos.
- ¿Cuánto valor tienen actualmente las Bases de Datos?
- ¿Se ha elaborado una lista de los posibles sospechosos que pudieran efectuar el robo?
- La lista de sospechosos, ¿es amplia o corta?
- ¿Cuántas personas se ocupan de la contabilidad de la Institución?
- ¿El sistema de contabilidad es confiable?
- Las personas que trabajan en el departamento de contabilidad, ¿qué tipo de antecedentes laborales tienen?
- ¿Existe acceso al Sistema Contable desde otros Sistemas o Personas?

2.5. Protecciones actuales en la Universidad.

- Generales, Se hacen copias periódicas de los archivos que son vitales para la Institución.
- Robo común, se cierran las puertas de entrada y ventanas, además de tener un control de llaves.
- Falla de los equipos, se tratan con cuidado, se realiza el mantenimiento de forma regular, no se permite fumar, está previsto el préstamo de otros equipos.
- Daño por virus, no todo el software que llega se analiza en un sistema utilizando software antivirus. Los programas de dominio público y de uso compartido (Shareware), pueden ser descargados por cualquier usuario.
- Equivocaciones, los empleados tienen buena formación.
- Acceso no autorizado, se cierra la puerta de entrada. Los computadores no disponen de llave de bloqueo del teclado.
- Fuego, en la actualidad no se encuentran instalados sistemas contra incendios, solo cuenta con algunos extinguidores, en sitios estratégicos y no se brinda entrenamiento en el manejo de los extinguidores al personal, en forma periódica.

Capitulo 3. Tipos de amenazas o riesgos.

Cada sistema es diferente y por lo tanto la política de seguridad a implementar no será única. Este concepto vale, también, para el edificio en el que nos encontramos. Es por ello que siempre se recomendarán pautas de aplicación general y no procedimientos específicos.

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

3.1. Principales amenazas que se prevén en la seguridad física.

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

No hace falta recurrir a películas de espionaje para sacar ideas de cómo obtener la máxima seguridad en un sistema informático, además de que la solución sería extremadamente cara.

A veces basta recurrir al sentido común para darse cuenta que cerrar una puerta con llave o cortar la electricidad en ciertas áreas siguen siendo técnicas válidas en cualquier entorno.

A continuación se analizan los peligros más importantes que se corren en un centro de procesamiento; con el objetivo de mantener una serie de acciones a seguir en forma eficaz y oportuna para la prevención, reducción, recuperación y corrección de los diferentes tipos de riesgos.

3.2. Incendios.

Los incendios son causados por el uso inadecuado de combustibles, fallas de instalaciones eléctricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas.

El fuego es una de las principales amenazas contra la seguridad. Es considerado el enemigo número uno de las computadoras ya que puede destruir fácilmente los archivos de información y programas.

Desgraciadamente los sistemas antifuego dejan mucho que desear, causando casi igual daño que el propio fuego, sobre todo a los elementos electrónicos. El dióxido de carbono, actual alternativa del agua, resulta peligroso para los propios empleados si quedan atrapados en la sala de cómputos.

Los diversos factores a contemplar para reducir los riesgos de incendio a los que se encuentra sometido un centro de cómputos son:

- El área en la que se encuentran las computadoras debe estar en un local que no sea combustible o inflamable.
- El local no debe situarse encima, debajo o adyacente a áreas donde se procesen, fabriquen o almacenen materiales inflamables, explosivos, gases tóxicos o sustancias radioactivas.
- Las paredes deben hacerse de materiales incombustibles y extenderse desde el suelo al techo.
- Debe construirse un "piso falso" instalado sobre el piso real, con materiales incombustibles y resistentes al fuego.
- No debe estar permitido fumar en el área de proceso.
- Deben emplearse muebles incombustibles, y cestos metálicos para papeles. Deben evitarse los materiales plásticos e inflamables.

- El piso y el techo en el recinto del centro de cómputo y de almacenamiento de los medios magnéticos deben ser impermeables.

Seguridad del Equipamiento.

Es necesario proteger los equipos de cómputo instalándolos en áreas en las cuales el acceso a los mismos sólo sea para personal autorizado. Además, es necesario que estas áreas cuenten con los mecanismos de ventilación y detección de incendios adecuados.

Para protegerlos se debe tener en cuenta que:

- La temperatura no debe sobrepasar los 18º C y el límite de humedad no debe superar el 65% para evitar el deterioro.
- Los centros de cómputos deben estar provistos de equipo para la extinción de incendios en relación al grado de riesgo y la clase de fuego que sea posible en ese ámbito.
- Deben instalarse extintores manuales (portátiles) o automáticos (rociadores).

Recomendaciones.

El personal designado para usar extinguidores de fuego debe ser entrenado en su uso.

Si hay sistemas de detección de fuego que activan el sistema de extinción, todo el personal de esa área debe estar entrenado para no interferir con este proceso automático.

Implementar paredes protectoras de fuego alrededor de las áreas que se desea proteger del incendio que podría originarse en las áreas adyacentes.

Proteger el sistema contra daños causados por el humo. Este, en particular la clase que es principalmente espeso, negro y de materiales especiales, puede ser muy dañino y requiere una lenta y costosa operación de limpieza.

Mantener procedimientos planeados para recibir y almacenar abastecimientos de papel.

Suministrar información del centro de cómputo, al departamento local de bomberos, antes de que ellos sean llamados en una emergencia. Hacer que este departamento esté consciente de las particularidades y vulnerabilidades del sistema, por excesivas cantidades de agua y la conveniencia de una salida para el humo, es importante. Además, ellos pueden ofrecer excelentes consejos como precauciones para prevenir incendios.

3.3. Condiciones climatológicas.

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

La frecuencia y severidad de su ocurrencia deben tenerse en cuenta al decidir la construcción de un edificio. La comprobación de los informes climatológicos o la existencia de un servicio que notifique la proximidad de una tormenta severa, permite que se tomen precauciones adicionales, tales como la retirada de objetos móviles, la provisión de calor, iluminación o combustible para la emergencia.

Inundaciones.

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

Además de las causas naturales de inundaciones, puede existir la posibilidad de una inundación provocada por la necesidad de apagar un incendio en un piso superior.

Para evitar este inconveniente se pueden tomar las siguientes medidas: construir un techo impermeable para evitar el paso de agua desde un nivel superior y acondicionar las puertas para contener el agua que bajase por las escaleras.

Terremotos.

Estos fenómenos sísmicos pueden ser tan poco intensos que solamente instrumentos muy sensibles los detectan o tan intensos que causan la destrucción de edificios y hasta la pérdida de vidas humanas. El problema es que en la actualidad, estos fenómenos están ocurriendo en lugares donde no se los asociaba. Por fortuna los daños en las zonas improbables suelen ser a veces más ligeros.

3.4. Acciones hostiles.

Robo.

Las computadoras son posesiones valiosas de las empresas y están expuestas, de la misma forma que lo están las piezas de stock e incluso el dinero. Es frecuente que los operadores utilicen la computadora de la empresa para realizar trabajos privados o para otras organizaciones y, de esta manera, robar tiempo de máquina.

"La información importante o confidencial puede ser fácilmente copiada. Muchas empresas invierten millones de dólares en programas y archivos de información, a los que dan menor protección que la que otorgan a una máquina de escribir o una calculadora". [7]

[7] *"Seguridad Informática" / ALDEGANI, Gustavo. Miguel/1° Edición. Argentina*

El software, es una propiedad muy fácilmente de sustraerse y las cintas y discos son fácilmente copiados sin dejar ningún rastro.

Fraude.

Cada año, millones de dólares son sustraídos de empresas y, en muchas ocasiones, las computadoras han sido utilizadas como instrumento para dichos fines.

Sin embargo, debido a que ninguna de las partes implicadas (compañía, empleados, fabricantes, auditores, etc.), tienen algo que ganar, sino que más bien pierden en imagen, no se da ninguna publicidad a este tipo de situaciones.

Sabotaje.

El peligro más temido en los centros de procesamiento de datos, es el sabotaje. Empresas que han intentado implementar programas de seguridad de alto nivel, han encontrado que la protección contra el saboteador es uno de los retos más duros. Este puede ser un empleado o un sujeto ajeno a la propia empresa.

Físicamente, los imanes son las herramientas a las que se recurre, ya que con una ligera pasada la información desaparece, aunque las cintas estén almacenadas en el interior de su funda de protección. Una habitación llena de cintas puede ser destruida en pocos minutos y los centros de procesamiento de datos pueden ser destruidos sin entrar en ellos.

Además, suciedad, partículas de metal o gasolina pueden ser introducidos por los conductos de aire acondicionado. Las líneas de comunicaciones y eléctricas pueden ser cortadas, etc.

Capitulo 4. Infraestructura.

4.1. Instalaciones físicas de la Universidad.

Figura 4. 1. Panorámica de la Universidad de Sotavento

La Universidad de Sotavento tiene 3 edificios principales, que son:

Edificio A1.

En la planta baja se encuentran ubicadas las oficinas de las áreas administrativas; Supervisión de actividades académicas, Dirección Académica, Archivo General, Control Escolar y Titulación, Dirección Administrativa y el Departamento de Promoción.

En las plantas altas de este mismo edificio se encuentran Aulas de clases de diversas carreras.

Edificio B1.

En la planta baja se encuentra un Salón de Usos Múltiples, Biblioteca, Servicios Médicos, Departamento de Deportes y Aulas del Centro de Cómputo.

En las plantas altas están Aulas de clases de diversas carreras

Figura 4.1.1. Edificio A

Edificio C1.

Este cuenta con algunos talleres y el Aula Clavijero un centro de computo donde se da educación a distancia y al contar este con computadoras más modernas a los de otros Centros de computo de la misma Universidad también es utilizado por el Alumnado que necesita usar software que requieren más capacidad de memoria.

La universidad también cuenta con instalaciones deportivas básicamente un campo de futbol soccer, cafetería, cancha de basquetbol, áreas verdes, actualmente se están construyendo nuevos salones en el Edificio C1.

4.2. Personal del centro cómputo.

El centro de cómputo de la Universidad de Sotavento básicamente dispone de un encargado principal el cual verifica que se estén satisfaciendo todas las necesidades que debe brindar el área de informática, también hay un auxiliar el cual se encarga de que se instalen nuevos equipos, este el software necesario y también funciona como apoyo a los profesores.

El demás personal del centro de cómputo está conformado por los becarios los cuales están en dos turnos de 8:00 a.m. a 2:00 p.m. y de 3:00 p.m. a 8:00 p.m.

Figura 4.2 Edificio B

4.3. Aulas.

Aula biblioteca.

En esta Aula se cuentan con libros para satisfacer a toda la población estudiantil de diversas carreras, también cuenta con servicio de Internet para que el alumno realice investigaciones, los equipos de computo son muy limitados básicamente cuentan con la paquetería office y no hay restricción a software de mensajería instantánea.

En caso de necesitar un libro hay que presentar tú credencial de la Universidad al encargado de la biblioteca, esto con el fin de que te lo presten para sacarle copias.

Sin embargo cualquier persona incluso que no sea de la Universidad puede acceder al área de los libros sin ninguna restricción.

La biblioteca cuenta con un sensor en la entrada principal esto en caso de que alguien intente sacar un libro sin autorización se activaría la alarma.

La biblioteca cuenta con un circuito cerrado de televisión el cual no está en funcionamiento.

Reglamento interno.

- Al ingresar al Centro de Cómputo, en el módulo de la entrada, el alumno entregará la credencial actualizada, misma que le será devuelta al salir.
- Cuando el usuario ingrese al Centro de Cómputo el encargado le asignará el equipo que va ocupar.
- Los usuarios no podrán cambiar de computadora sin autorización del encargado.
- Únicamente dos personas podrán trabajar, al mismo tiempo en una computadora.
- Se prohíbe instalar cualquier tipo de software en las computadoras del Centro de Cómputo.
- Se prohíbe modificar la configuración de la computadora o introducir contraseñas de cualquier tipo.
- Los disquetes a utilizar, deberán ser revisados para comprobar la ausencia de virus.
- Se prohíbe fumar e introducir alimentos y bebidas de cualquier tipo.
- El usuario sólo va a emplear el equipo para elaborar actividades estrictamente académicas.
- También se prestarán los siguientes servicios: chatear. Escuchar o bajar música y consultar páginas de contenido educativo.

- Se suspenderá el servicio al usuario que no cumpla con el presente reglamento y dependiendo de la falta cometida se aplicará una sanción.

Aula 1.

Esta aula se utiliza para fomentar la investigación académica las materias que abarca son según la carrera.

Cuenta con equipos de cómputo, servicio de Internet y el software es básico, funciona de lunes a viernes de 8 a 21 Hrs. y la asignación del centro de computo al alumnado va de acuerdo a la programación que se haya convenido con los profesores, sin embargo en momentos que no hay clases cualquier persona puede acceder al aula sin ninguna objeción.

Reglamento interno.

- El alumno deberá presentar la credencial que lo acredite como estudiante de la facultad.
- Queda prohibida la introducción de alimentos y bebidas.
- El alumno deberá de mantener orden y limpieza de las instalaciones.
- Al inicio de cualquier sesión de trabajo deberá revisar que sus discos estén libres de virus.
- Reportar cualquier falla encontrada en el equipo al encargado del laboratorio con el fin de mantenerlo en óptimas condiciones de uso.
- Al término de cada sesión de trabajo el alumno deberá apagar el equipo que haya utilizado.
- Respetar la estructura de los directorios, paquetes, lenguajes y programas que se tienen instalados en las computadoras.
- El alumno podrá guardar sus archivos solo en la carpeta "mis documentos", el contenido de dicha carpeta será borrado periódicamente y el alumno será responsable de mantener respaldados sus archivos.
- Queda prohibida la instalación de programas en el disco duro de las computadoras sin previa autorización del encargado del centro de cómputo.

- Queda prohibido utilizar el equipo para recreación toda persona que sea sorprendida con juegos, chat o pornografía será suspendida.
- Todo lo no previsto en estos lineamientos quedará a consideración de la Dirección de la facultad.

Figura 4.3. Centro de cómputo

Aula 2.

Es muy similar al Aula 1, se encuentran instalados equipos de cómputo con servicio a Internet y paquetería básica tanto para alumnos como profesores, se apoya a la investigación académica.

Esta aula fue únicamente diseñada para fines académicos sin embargo la mayoría de las veces se puede acceder para chatear, bajar música, jugar en línea y otras actividades de ocio.

Aula clavijero.

El aula Clavijero funciona de acuerdo a los lineamientos del "Consorcio Clavijero" el cual es un esfuerzo colectivo de instituciones públicas y privadas de educación superior de Veracruz que ofrece opciones educativas de calidad y pertinencia, en la modalidad de educación a distancia en línea, considerada como el proyecto innovador nacional más importante para llevar educación a distancia

en línea, aprovechando las ventajas que ofrecen las nuevas tecnologías como la Internet.

En este sentido, contribuye a incrementar la cobertura educativa en México y acrecentar la capacidad del sistema educativo veracruzano, mediante la oferta de programas académicos orientados a las áreas estratégicas del conocimiento no atendidas por las instituciones de educación superior, además de acciones de educación continua y capacitación.

4.4. Instalación eléctrica.

Trabajar con computadoras implica trabajar con electricidad. Por lo tanto esta una de las principales áreas a considerar en la seguridad física. Además, es una problemática que abarca desde el usuario hogareño hasta la gran empresa.

En la medida que los sistemas se vuelven más complicados se hace más necesaria la presencia de un especialista para evaluar riesgos particulares y aplicar soluciones que estén de acuerdo con una norma de seguridad industrial.

Para que funcionen adecuadamente, las computadoras personales necesitan de una fuente de alimentación eléctrica fiable, es decir, una que se mantenga dentro de parámetros específicos. Si se interrumpe inesperadamente la alimentación eléctrica o varía en forma significativa, fuera de los valores normales, las consecuencias pueden ser serias. Pueden perderse o dañarse los datos que hay en memoria, se puede dañar el hardware, interrumpirse las operaciones activas y la información podría quedar temporal o definitivamente inaccesible.

Por lo general las computadoras personales toman la electricidad de los circuitos eléctricos domésticos normales, a los que se llama tomas de corriente. Esta corriente es bastante fuerte, siendo una corriente alterna (ac), ya que alterna el positivo con el negativo.

La mayor parte de las computadoras personales incluyen un elemento denominado fuente de alimentación, la cual recibe corriente alterna de las tomas

de corriente y la convierte o transforma en la corriente continua de baja potencia que utilizan los componentes de la computadora.

La fuente de alimentación es un componente vital de cualquier computadora personal, y es la que ha de soportar la mayor parte de las anomalías del suministro eléctrico. Actualmente existe el concepto de fuente de alimentación redundante, la cual entrará en operación si se detecta una falla en la fuente de alimentación principal.

En nuestro medio se han podido identificar siete problemas de energía más frecuente:

- Fallas de energía.
- Transistores y pulsos.
- Bajo voltaje.
- Ruido electromagnético.
- Distorsión.
- Alto voltaje.
- Variación de frecuencia.

Picos y ruidos electromagnéticos.

Las subidas (picos) y caídas de tensión no son el único problema eléctrico al que se han de enfrentar los usuarios. También está el tema del ruido que interfiere en el funcionamiento de los componentes electrónicos. El ruido interfiere en los datos, además de favorecer la escucha electrónica.

Cableado.

Los cables que se suelen utilizar para construir las redes locales van del cable telefónico normal al cable coaxial o la fibra óptica. Algunos edificios de oficinas ya se construyen con los cables instalados para evitar el tiempo y el gasto posterior, y de forma que se minimice el riesgo de un corte, rozadura u otro daño accidental.

Los riesgos más comunes para el cableado se pueden resumir en los siguientes:

- Interferencia: Estas modificaciones pueden estar generadas por cables de alimentación de maquinaria pesada o por equipos de radio o microondas. Los cables de fibra óptica no sufren el problema de alteración (de los datos que viajan a través de él) por acción de campos eléctricos, que si sufren los cables metálicos.
- Corte del cable: La conexión establecida se rompe, lo que impide que el flujo de datos circule por el cable.
- Daños en el cable: Los daños normales con el uso pueden dañar el apantallamiento que preserva la integridad de los datos transmitidos o dañar al propio cable, lo que hace que las comunicaciones dejen de ser fiables.

En la mayor parte de las organizaciones, estos problemas entran dentro de la categoría de daños naturales. Sin embargo también se pueden ver como un medio para atacar la red si el objetivo es únicamente interferir en su funcionamiento.

El cable de red ofrece también un nuevo frente de ataque para un determinado intruso que intentase acceder a los datos. Esto se puede hacer:

- Desviando o estableciendo una conexión no autorizada en la red: un sistema de administración y procedimiento de identificación de acceso adecuado hará difícil que se puedan obtener privilegios de usuarios en la red, pero los datos que fluyen a través del cable pueden estar en peligro.
- Haciendo una escucha sin establecer conexión, los datos se pueden seguir y pueden verse comprometidos.

Luego, no hace falta penetrar en los cables físicamente para obtener los datos que transportan.

Cableado de alto nivel de seguridad.

Son cableados de redes que se recomiendan para instalaciones con grado de seguridad militar. El objetivo es impedir la posibilidad de infiltraciones y monitoreos de la información que circula por el cable. Consta de un sistema de tubos (herméticamente cerrados) por cuyo interior circula aire a presión y el cable. A lo largo de la tubería hay sensores conectados a una computadora. Si se detecta algún tipo de variación de presión se dispara un sistema de alarma.

Sistema de aire acondicionado.

Se debe proveer un sistema de calefacción, ventilación y aire acondicionado separado, que se dedique al cuarto de computadoras y equipos de proceso de datos en forma exclusiva.

Teniendo en cuenta que los aparatos de aire acondicionado son causa potencial de incendios e inundaciones, es recomendable instalar redes de protección en todo el sistema de cañería al interior y al exterior, detectores y extinguidores de incendio, monitores y alarmas efectivas.

Emisiones electromagnéticas.

Desde hace tiempo se sospecha que las emisiones, de muy baja frecuencia que generan algunos periféricos, son dañinas para el ser humano.

Según recomendaciones científicas estas emisiones podrían reducirse mediante filtros adecuados al rango de las radiofrecuencias, siendo estas totalmente seguras para las personas.

Capitulo 5. Prevención y Salvaguarda.

Si hay un problema que compartimos todos, desde los gobiernos, las grandes corporaciones y hasta el último usuario final, es la falta de prevención. Asumimos, erróneamente, que nunca sucederá un hecho que comprometa nuestros activos y que, si el mismo sucede, no los comprometerá de forma irreversible.

Otro error común es pensar que un hecho desgraciado "puede" ocurrir. El pensamiento correcto y sobre el cual debemos actuar es que el infortunio "ya ha ocurrido". Este cambio de visión involucra un crecimiento que envuelve la forma en que se protegen los activos y las medidas preventivas tomadas para que no ocurran.

Es común encontrar bibliografía que trate sobre las formas de recuperación de un sistema o sobre las posibilidades de derribar y construir luego de ocurrido un ataque, pero no es sencillo encontrar información sobre la capacidad para mitigar una amenaza, minimizar los riesgos y prevenir un desastre.

En el capítulo 2 se definió ampliamente el concepto de seguridad física que es una de las herramientas de la prevención y en este capítulo presentaremos las más importantes medidas de seguridad física que actualmente existen:

5.1. Servicio de vigilancia.

El Servicio de Vigilancia es el encargado del control de acceso de personas y vehículos a la instalación y edificios. Este servicio es el encargado de colocar los guardias en lugares estratégicos para cumplir con sus objetivos y controlar los accesos.

Control de personas.

El control de acceso no sólo requiere la capacidad de identificación, sino también asociarla a la apertura o cierre de puertas, permitir o negar acceso basado en restricciones de tiempo, área o sector dentro de una empresa o institución. A cualquier personal ajeno a la planta se le solicitará completar un

formulario de datos personales, los motivos de la visita, hora de ingreso y de egreso, etc.

El uso de credenciales de identificación es uno de los puntos más importantes del sistema de seguridad, a fin de poder efectuar un control eficaz del ingreso y egreso del personal a los distintos sectores de la empresa.

En este caso la persona se identifica por algo que posee, por ejemplo una tarjeta de identificación. Cada una de ellas tiene un PIN (Personal Identification Number) único, siendo este el que se almacena en una base de datos para su posterior seguimiento, si fuera necesario.

Su mayor desventaja es que estas tarjetas pueden ser copiadas, robadas, etc., permitiendo ingresar a cualquier persona que la posea. Estas credenciales se pueden clasificar de la siguiente manera:

- Normal o definitiva: para el personal permanente de planta.
- Temporaria: para personal recién ingresado.
- Contratistas: personas ajenas a la empresa, que por razones de servicio deben ingresar a la misma.
- Visitas.

Las personas también pueden acceder mediante algo que saben (por ejemplo un número de identificación o un password) que se solicitará a su ingreso. Al igual que el caso de las tarjetas de identificación los datos ingresados se contrastarán contra una base donde se almacena los datos de las personas autorizadas. Este sistema tiene la desventaja que generalmente se eligen identificaciones sencillas, bien se olvidan dichas identificaciones o incluso las bases de datos pueden verse alteradas o robadas por personas no autorizadas.

Control de vehículos.

Para controlar el ingreso y egreso de vehículos, el personal de vigilancia debe asentar en una planilla los datos personales de los ocupantes del vehículo, la marca y patente del mismo, y la hora de ingreso y egreso de la empresa.

Desventajas de utilizar guardias.

La principal desventaja de la aplicación de personal de guardia es que éste puede llegar a ser sobornado por un tercero para lograr el acceso a sectores donde no esté habilitado, como así también para poder ingresar o egresar de la planta con materiales no autorizados.

Esta situación de soborno es muy frecuente, por lo que es recomendable la utilización de sistemas biométricos para el control de accesos.

5.2. Utilización de detectores de metales.

El detector de metales es un elemento sumamente práctico para la revisión de personas, ofreciendo grandes ventajas sobre el sistema de palpación manual.

La sensibilidad del detector es regulable, permitiendo de esta manera establecer un volumen metálico mínimo, a partir del cual se activará la alarma.

La utilización de este tipo de detectores debe hacerse conocer a todo el personal. De este modo, actuará como elemento disuasivo.

5.3. Sistemas biométricos.

Definimos a la Biometría como "la parte de la biología que estudia en forma cuantitativa la variabilidad individual de los seres vivos utilizando métodos estadísticos".

La Biometría es una tecnología que realiza mediciones en forma electrónica, guarda y compara características únicas para la identificación de personas.

La forma de identificación consiste en la comparación de características físicas de cada persona con un patrón conocido y almacenado en una base de

datos. Los lectores biométricos identifican a la persona por lo que es (manos, ojos, huellas digitales y voz).

Emisión de calor.

Se mide la emisión de calor del cuerpo (termograma), realizando un mapa de valores sobre la forma de cada persona.

Huella digital.

Basado en el principio de que no existen dos huellas dactilares iguales, este sistema viene siendo utilizado desde el siglo pasado con excelentes resultados.

Cada huella digital posee pequeños arcos, ángulos, bucles, remolinos, etc. (llamados minucias) características y la posición relativa de cada una de ellas es lo analizado para establecer la identificación de una persona. Esta aceptado que dos personas no tienen más de ocho minucias iguales y cada una posee más de 30, lo que hace al método sumamente confiable.

Verificación de voz.

La dicción de una (o más) frase es grabada y en el acceso se compara la vos (entonación, diptongos, agudeza, etc.).

Este sistema es muy sensible a factores externos como el ruido, el estado de ánimo y enfermedades de la persona, el envejecimiento, etc.

Verificación de patrones oculares.

Estos modelos pueden estar basados en los patrones del iris o de la retina y hasta el momento son los considerados más efectivos (en 200 millones de personas la probabilidad de coincidencia es casi 0).

Su principal desventaja reside en la resistencia por parte de las personas a que les analicen los ojos, por revelarse en las mismas enfermedades que en ocasiones se prefiere mantener en secreto.

Verificación automática de firmas (VAF).

En este caso lo que se considera es lo que el usuario es capaz de hacer, aunque también podría encuadrarse dentro de las verificaciones biométricas.

Mientras es posible para un falsificador producir una buena copia visual o facsímil, es extremadamente difícil reproducir las dinámicas de una persona: por ejemplo la firma genuina con exactitud.

La VAF, usando emisiones acústicas toma datos del proceso dinámico de firmar o de escribir.

La secuencia sonora de emisión acústica generada por el proceso de escribir constituye un patrón que es único en cada individuo. El patrón contiene información extensa sobre la manera en que la escritura es ejecutada.

El equipamiento de colección de firmas es inherentemente de bajo costo y robusto. Esencialmente, consta de un bloque de metal (o algún otro material con propiedades acústicas similares) y una computadora barata.

Los beneficios de una tecnología biométrica.

Pueden eliminar la necesidad de poseer una tarjeta para acceder. Aunque las reducciones de precios han disminuido el costo inicial de las tarjetas en los últimos años, el verdadero beneficio de eliminarlas consiste en la reducción del trabajo concerniente a su administración.

Utilizando un dispositivo biométrico los costos de administración son más pequeños, se realiza el mantenimiento del lector, y una persona se encarga de mantener la base de datos actualizada. Sumado a esto, las características biométricas de una persona son intransferibles a otra.

5.4. Seguridad con animales.

Sirven para grandes extensiones de terreno, y además tienen órganos sensitivos mucho más sensibles que los de cualquier dispositivo y, generalmente, el costo de cuidado y mantenimiento se disminuyen considerablemente utilizando este tipo de sistema.

Así mismo, este sistema posee la desventaja de que los animales pueden ser engañados para lograr el acceso deseado.

Figura 5.4. Seguridad con Animales

5.5. Protección electrónica.

Se llama así a la detección de robo, intrusión, asalto e incendios mediante la utilización de sensores conectados a centrales de alarmas. Estas centrales tienen conectadas los elementos de señalización que son los encargados de hacerles saber al personal de una situación de emergencia.

Cuando uno de los elementos sensores detectan una situación de riesgo, éstos transmiten inmediatamente el aviso a la central; ésta procesa la información recibida y ordena en respuesta la emisión de señales sonoras o luminosas alertando de la situación.

Barreras infrarrojas y de micro-ondas.

Transmiten y reciben haces de luces infrarrojas y de micro-ondas respectivamente. Se codifican por medio de pulsos con el fin de evadir los intentos

de sabotaje. Estas barreras están compuestas por un transmisor y un receptor de igual tamaño y apariencia externa.

Cuando el haz es interrumpido, se activa el sistema de alarma, y luego vuelve al estado de alerta. Estas barreras son inmunes a fenómenos aleatorios como calefacción, luz ambiental, vibraciones, movimientos de masas de aire, etc.

Las invisibles barreras fotoeléctricas pueden llegar a cubrir áreas de hasta 150 metros de longitud (distancias exteriores). Pueden reflejar sus rayos por medio de espejos infrarrojos con el fin de cubrir con una misma barrera diferentes sectores.

Las microondas son ondas de radio de frecuencia muy elevada. Esto permite que el sensor opere con señales de muy bajo nivel sin ser afectado por otras emisiones de radio, ya que están muy alejadas en frecuencia. Debido a que estos detectores no utilizan aire como medio de propagación, poseen la ventaja de no ser afectados por turbulencias de aire o sonidos muy fuertes.

Otra ventaja importante es la capacidad de atravesar ciertos materiales como son el vidrio, lana de vidrio, plástico, tabiques de madera, revoques sobre madera, mampostería y hormigón.

Detector ultrasónico.

Este equipo utiliza ultrasonidos para crear un campo de ondas.

De esta manera, cualquier movimiento que realice un cuerpo dentro del espacio protegido, generará una perturbación en dicho campo que accionará la alarma. Este sistema posee un circuito refinado que elimina las falsas alarmas. La cobertura de este sistema puede llegar a un máximo de 40 metros cuadrados.

Detectores pasivos sin alimentación.

Estos elementos no requieren alimentación extra de ningún tipo, sólo van conectados a la central de control de alarmas para mandar la información de control. Los siguientes están incluidos dentro de este tipo de detectores:

- **Detector de aberturas:** Contactos magnéticos externos o de embutir.

- **Detector de roturas de vidrios:** Inmune a falsas alarmas provocadas por sonidos de baja frecuencia; sensibilidad regulable.
- **Detector de vibraciones:** Detecta golpes o manipulaciones extrañas sobre la superficie controlada.

Sonorización y dispositivos luminosos.

Dentro de los elementos de sonorización se encuentran las sirenas, campanas, timbres, etc. Algunos dispositivos luminosos son los faros rotativos, las balizas, las luces intermitentes, etc.

Estos deben estar colocados de modo que sean efectivamente oídos o vistos por aquellos a quienes están dirigidos. Los elementos de sonorización deben estar bien identificados para poder determinar rápidamente si el estado de alarma es de robo, intrusión, asalto o aviso de incendio.

Se pueden usar transmisores de radio a corto alcance para las instalaciones de alarmas locales. Los sensores se conectan a un transmisor que envía la señal de radio a un receptor conectado a la central de control de alarmas encargada de procesar la información recibida.

Circuitos cerrados de televisión.

Permiten el control de todo lo que sucede en la planta según lo captado por las cámaras estratégicamente colocadas. Los monitores de estos circuitos deben estar ubicados en un sector de alta seguridad. Las cámaras pueden estar a la vista (para ser utilizada como medida disuasiva) u ocultas (para evitar que el intruso sepa que está siendo captado por el personal de seguridad).

Figura 5.5. Circuitos Cerrados de Televisión.

Todos los elementos anteriormente descriptos poseen un control contra sabotaje, de manera que si en algún momento se corta la alimentación o se produce la rotura de alguno de sus componentes, se enviará una señal a la central de alarma para que ésta accione los elementos de señalización correspondientes.

Edificios inteligentes.

La infraestructura inmobiliaria no podía quedarse rezagada en lo que se refiere a avances tecnológicos el Edificio Inteligente (surgido hace unos 10 años) "se define como una estructura que facilita a usuarios y administradores, herramientas y servicios integrados a la administración y comunicación".[8]

Este concepto propone la integración de todos los sistemas existentes dentro del edificio, tales como teléfonos, comunicaciones por computadora, seguridad, control de todos los subsistemas del edificio (gas, calefacción, ventilación y aire acondicionado, etc.) y todas las formas de administración de energía.

[8] *MANUNTA, Giovanni/ "Presentación del libro Seguridad: una introducción. Consultor y Profesor de Seguridad de Cranfield University. Revista Virtual Seguridad Corporativa/ http://www.seguridadcorporativa.org*

Una característica común de los Edificios Inteligentes es la flexibilidad que deben tener para asumir modificaciones de manera conveniente y económica.

Capitulo 6. Alternativas para mejorar la seguridad física en los centros de cómputo de la Universidad de Sotavento.

Garantizar que los recursos informáticos de una compañía estén disponibles para cumplir sus propósitos, es decir, que no estén dañados o alterados por circunstancias o factores externos, es una definición útil para conocer lo que implica el concepto de seguridad física informática.

En términos generales, la seguridad puede entenderse como aquellas reglas técnicas y/o actividades destinadas a prevenir, proteger y resguardar lo que es considerado como susceptible de robo, pérdida o daño, ya sea de manera personal, grupal o empresarial.

Es por la existencia de un número importante de amenazas y riesgos, que la infraestructura de red y recursos informáticos de una organización deben estar protegidos bajo un esquema de seguridad que reduzca los niveles de vulnerabilidad y permita una eficiente administración del riesgo.

En este trabajo se analizan tres alternativas de solución para el mejoramiento de la seguridad física, al final de capítulo exponemos lo que a nuestro juicio es la mejor alternativa.

6.1. Alternativa 1.- Invertir únicamente en seguridad.

Como primera alternativa se propone adquirir dispositivos de seguridad física, y contratar servicios externos de vigilancia. Algunas compañías consultoras en seguridad informática recomiendan los siguientes elementos de seguridad:

- Protección exterior.(Barreras)
- Monitoreo y alarma (Dispositivos mecánicos, eléctricos, electrónicos y equipo)
- Iluminación de protección
- Seguridad de cierre (Cajas fuertes y bóvedas)

- Sistemas de cerradura y llave
- Identificación y control (Control de tráfico)
- Sistema de vigilancia (Guardias)
- Programa de sensibilización (Encuestas de seguridad)

	Ventajas	**Desventajas**
Invertir únicamente en Seguridad.	• Mejora el ambiente laboral. • Ataca puntos débiles de seguridad. • Mejora la productividad. • Se contara con los elementos necesarios en caso de algún incidente.	• Costos elevados debido a la adquisición de tecnología • Rechazo por alguna parte del personal a usar nuevas tecnologías • Adaptación o cursos para la nueva tecnología • Posible falla en la inversión, que no de los resultados esperados.

Tabla 6.1 Alternativa 1.- Invertir únicamente en seguridad.

6.2. Alternativa 2.- Contratar a un Proveedor de Servicio(Outsourcing)

En la actualidad existen en el mercado muchas compañías que ofrecen servicios de seguridad física informática englobados en paquetes que ellos llaman con el término de "soluciones integrales", en los cuales se contemplan la planeación, el análisis de riesgos, definición de normas y políticas, hasta la implementación de los controles de acceso físico y lógico con aplicaciones tecnológicas, que pueden incluir desde productos y dispositivos con tecnología de punta hasta metodologías y estándares de seguridad y mejores prácticas.

	Ventajas	**Desventajas**
Contratar un proveedor de servicio (Outsourcing).	• Mejorara la seguridad en el centro de cómputo. • Ayuda a redefinir el centro de cómputo. • Construye una larga ventaja competitiva sostenida mediante un cambio de reglas y un mayor alcance de la organización. • Permite a la empresa poseer lo mejor de la tecnología sin la necesidad de entrenar personal de la organización para manejarla. • Permite disponer de servicios de información en forma rápida considerando las presiones competitivas. • Disposición de personal altamente capacitado.	• La empresa pierde contacto con las nuevas tecnologías que ofrecen oportunidades para innovar los productos y procesos. • La empresa pierde contacto con las nuevas tecnologías que ofrecen oportunidades para innovar los productos y procesos • El costo ahorrado con el uso de Outsourcing puede que no sea el esperado. • Despido de empleados quienes actualmente manejan el centro de cómputo.

Tabla 6.2 Alternativa 2.- Contratar a un Proveedor de Servicio (Outsourcing).

6.3. Alternativa 3.- Crear manual de procedimientos.

Es por la existencia de un número importante de amenazas y riesgos, que la infraestructura de red y recursos informáticos de una organización deben estar protegidos bajo un esquema de seguridad que reduzca los niveles de vulnerabilidad y permita una eficiente administración del riesgo.

Para ello, resulta importante establecer políticas de seguridad, las cuales van desde el monitoreo de la infraestructura de red, los enlaces de telecomunicaciones, la realización del respaldo de datos y hasta el reconocimiento de las propias necesidades de seguridad, para establecer los niveles de protección de los recursos.

Las políticas deberán basarse en los siguientes pasos:

- Identificar y seleccionar lo que se debe proteger (información sensible)
- Establecer niveles de prioridad e importancia sobre esta información
- Conocer las consecuencias que traería a la compañía, en lo que se refiere a costos y productividad, la pérdida de datos sensibles
- Identificar las amenazas, así como los niveles de vulnerabilidad de la red
- Realizar un análisis de costos en la prevención y recuperación de la información, en caso de sufrir un ataque y perderla
- Implementar un plan de respuesta a incidentes y recuperación para disminuir el impacto

Esta última debe ser proactiva, integrar una serie de iniciativas para actuar en forma rápida y eficaz ante incidentes y recuperación de información, así como elementos para generar una cultura de seguridad dentro de la organización.

Este tipo de políticas permitirá desplegar una arquitectura de seguridad basada en soluciones tecnológicas, así como el desarrollo de un plan de acción para el manejo de incidentes y recuperación para disminuir el impacto, ya que previamente habremos identificado y definido los sistemas y datos a proteger.

Es importante tomar en consideración, que las amenazas no disminuirán y las vulnerabilidades no desaparecerán en su totalidad, por lo que los niveles de inversión en el área de seguridad en cualquier empresa, deberán ir acordes a la importancia de la información en riesgo.

Desarrollar un manual de procedimientos significa: "planear, organizar coordinar dirigir y controlar las actividades relacionadas a mantener y garantizar la integridad física de los recursos implicados en la función informática, así como el resguardo de los activos de una empresa."[9]

Un manual de procedimientos para un sistema de seguridad integral debe contemplar:

- El manual de procedimientos debe asegurar la integridad y exactitud de los datos
- Debe permitir identificar la información que es confidencial
- Debe contemplar áreas de uso exclusivo
- Debe proteger y conservar los activos de desastres provocados por la mano del hombre y los actos abiertamente hostiles
- Debe asegurar la capacidad de la organización para sobrevivir accidentes
- Debe proteger a los empleados contra tentaciones o sospechas innecesarias
- Debe contemplar la administración contra acusaciones por imprudencia

[9] *"Evaluación de Seguridad de un Sistema de Información"/José Alfredo Jiménez*

	Ventajas	Desventajas
Crear manual de procedimientos.	• Incrementa la motivación del empleado, ya que permite la detección de los objetivos de la organización mediante el aporte de sus tareas. • Permite normalizar la ejecución de tareas estándar y facilita la toma de decisiones programadas. • Permitirte saber como actuar en caso de riesgo o indisciplina de un usurario. • Evita improvisaciones y decisiones apresuradas, a veces incongruentes con las tomadas por otro sector. • Facilita el control de gestión y la detección de deficiencias en los procedimientos administrativos. • Se contara con el mismo personal, únicamente se asignaran o deslindaran responsabilidades.	• La ejecución de tareas que cuando no están normalizadas resultan confusas, voluminosas y, por lógica consecuencia, costosas. • Muchas veces los manuales no son en la práctica utilizados por el personal para el aprendizaje y guía de las tareas que deben realizar. • Necesita actualizarse constantemente ya que en una organización siempre habrá cambios.

Figura 6.3 Alternativa 3.- Crear manual de procedimientos.

6.4. ¿Qué alternativa conviene más a la Universidad de Sotavento?

Se elige la alternativa 3 ya que al ser un centro de cómputo de una universidad existen elementos adecuados para implementar un manual de procedimientos y que tenga éxito, para esto es necesario corregir errores y actuar de manera adecuada en diversos casos que se puedan presentar, en relación a la alternativa 2 los gastos se reducirán considerablemente.

Respecto a la alternativa 1 es importante invertir en seguridad, pero este no debe ser el único paso a seguir si en verdad se quiere mejorar, se recomienda un equilibrio e invertir en algunos puntos débiles del centro de computo pero siempre tomando en cuenta las Políticas de Seguridad Informática y que este sea la base para hacer tomar conciencia a los usuarios de cómo minimizar los riesgos físicos potenciales en la institución.

- En la ejecución de tareas se tendrá un mejor control de las actividades del personal y que no interfieran con otra actividad.
- En caso de alguna indisciplina por parte de los usuarios se sabrá cómo proceder de acuerdo al reglamento el cual deberá ser acatado, de lo contrario se tomaran las sanciones que así convengan a la institución.
- Cada empleado tendrá que realizar únicamente sus actividades asignadas, lo cual evitara improvisar en alguna toma de decisiones, para esto es necesario que exista coordinación con otros sectores, esto permitirá llegar tanto a objetivos personales como organizacionales deslindando responsabilidad en las tareas que se realicen.
- Al poner en práctica este manual veremos como resultado un agradable ambiente estudiantil, se tendrá en cuenta la importancia de una buena seguridad física que haga sentir al alumno cómodo, y creara un sentimiento de corresponsabilidad de las instalaciones.
- Otro de los objetivos será poner gran énfasis para hacer tomar conciencia tanto al personal como a los usuarios de lo importante que es para todos respetar las normas establecidas y hacer caso a las recomendaciones.

Capitulo 7. Recomendaciones para la seguridad física en los centros de cómputo de la Universidad de Sotavento.

7.1. Recomendaciones Básicas

Hasta hace algunos años la exposición de los Equipos de Cómputo a través de grandes ventanales, constituían el orgullo de la organización, considerándose necesario que estuviesen a la vista del público, siendo constantemente visitados. Esto ha cambiado de modo radical, principalmente por el riesgo de robo y vandalismo.

- Se deben evitar, en lo posible, los grandes ventanales, los cuales además de que permiten la entrada del sol y calor (inconvenientes para el equipo de cómputo), puede ser un riesgo para la seguridad del Centro de Cómputo, en caso de la Universidad de Sotavento usa grandes cortinas que tapan la entrada de los rayos solares.
- El acceso al Centro de Cómputo debe estar restringido al personal autorizado. El personal de la Institución deberá tener su identificación siempre en un lugar visible.
- Se debe establecer un medio de control de entrada y salida de visitas al centro de cómputo. Si fuera posible, acondicionar un ambiente o área de visitas.
- Se recomienda que al momento de reclutar al personal se deben tener muy en cuenta sus antecedentes de trabajo, ya que un Centro de Cómputo depende en gran medida, de la integridad, estabilidad y lealtad del personal.
- Deben establecerse controles para una efectiva disuasión y detección, a tiempo, de los intentos no autorizados de acceder a los sistemas y a los archivos de información que contienen.
- Se recomienda establecer políticas para la creación de los passwords y establecer periodicidad de cambios de los mismos.

- Establecer políticas de autorizaciones de acceso físico al ambiente y de revisiones periódicas de dichas autorizaciones.
- Establecer políticas de control de entrada y salida del personal, así como de los paquetes u objetos que portan.
- Los controles de acceso, el acceso en sí y los vigilantes deben estar ubicados de tal manera que no sea fácil el ingreso de una persona extraña. En caso que ingresara algún extraño al centro de Cómputo, que no pase desapercibido y que no le sea fácil a dicha persona llevarse un archivo.
- Las cámaras fotográficas no se permitirán en ninguna sala de cómputo, sin permiso por escrito de la Dirección.
- Asignar a una sola persona la responsabilidad de la protección de los equipos en cada área.

7.2 Recomendaciones para el equipo de cómputo

- **Teclado:** Mantener fuera del teclado grapas y clips ya que pueden insertarse entre las teclas, puede causar un cruce de función. También se recomienda una alarma de sistema de movimientos este también puede aplicar a los demás periféricos.
- **CPU:** Mantener la parte posterior del CPU liberado en por lo menos 10cm. Para asegurar así una ventilación mínima adecuada.
- **Mouse:** Se recomienda un mouse óptico y ponerle de bajo una superficie plana y limpia, de tal manera que sea mas cómodo para el usuario.
- **Protectores de pantalla:** Estos sirven para evitar la radiación de las pantallas a color que causan irritación a los ojos.

Recomendaciones para el mantenimiento de los discos duros.

- Aunque el conjunto de cabezales y discos viene de fábrica sellado herméticamente, debe evitarse que los circuitos electrónicos que se encuentran alrededor se llenen de partículas de polvo y suciedad que pudieran ser causa de errores.
- La computadora debe colocarse en un lugar donde no pueda ser golpeado, de preferencia sobre un escritorio resistente y amplio.
- Se debe evitar que la microcomputadora se coloque en zonas donde haya acumulación de calor. Esta es una de las causas más frecuentes de las fallas de los discos duros, sobre todo cuando algunas piezas se dilatan más que otras.
- No se debe mover el CPU conteniendo al disco duro cuando esté encendido, porque los cabezales de lectura-escritura pueden dañar al disco.
- Una de las medidas más importantes en este aspecto, es hacer que la gente tome conciencia de lo importante que es cuidar un microcomputador.
- Se recomienda tener en buen estado los discos donde se resguarda la información, así como que esta sea respaldada en servidores cada 2 meses, para que en caso de que exista alguna pérdida se pueda recuperar.

Recomendaciones para el mantenimiento de memorias USB.

- Desconecte de manera adecuada el dispositivo de almacenamiento USB de su sistema.
- Es importante no desconectar el dispositivo USB hasta que todas las operaciones hayan finalizado. Si desconecta el dispositivo de almacenamiento mientras está grabando, puede dañar el dispositivo con la consecuente pérdida de datos.
- Es importante cerrar la conexión USB desde Windows (en Windows Vista use el icono “Quitar hardware con seguridad" de la bandeja del sistema).

- Guarde debidamente las tarjetas de memoria USB en su estuche de plástico.
- No inserte los dispositivos de almacenamiento haciendo fuerza en los contactos.
- Haga siempre copias de seguridad.
- Los dispositivos de almacenamiento no son infalibles, y pueden perder información por cualquiera de las causas mencionadas. Por ello es importante hacer siempre copias de seguridad o imprimir la información necesaria. No almacene su información únicamente en sus dispositivos USB.

Recomendaciones para el uso del monitor.

- La forma más fácil y común de reducir la fatiga en la visión que resulta de mirar a una pantalla todo el día, es el uso de medidas contra la refección.
- Generalmente éstos vienen en forma de una pantalla con un terminado áspero o algún tipo de capa contra brillo con una base de sílice, sobre la superficie de la pantalla del monitor.
- Se recomienda sentarse por lo menos a 60 cm. de la pantalla. No sólo esto reducirá su exposición a las emisiones (que se disipan a una razón proporcional al cuadrado de la distancia), sino que puede ayudar a reducir el esfuerzo visual.
- También manténgase por lo menos a 1 m. o 1.20 m. del monitor de su vecino, ya que la mayoría de los monitores producen más emisiones por detrás, que por delante. Finalmente apague su monitor cuando no lo esté usando.

Mantener las áreas operativas limpias y pulcras.

Limpieza interna: Se tendrá que realizar la limpieza 15min antes de la primer clases de cada modulo (7:00 AM y 3:00 PM), esta se realizara con trapeador, sin barrer.

Al finalizar cada clase el responsable del aula tendrá que acomodar la sillas, y equipos, en el caso de que se queden residuos de basura los tendrá que recoger.

Limpieza externa: Semestralmente se recomienda realizar una limpieza más detallada del Centro de Computo, esto incluye limpiar los equipos, cortinas, ventanas o en caso de ser necesario pintarlas, ya que la Universidad de Sotavento al estar ubicada en una zona arenosa se ensucia muy frecuentemente por el polvo.

7.3. Acceso a los servicios de los centros de cómputo

Para poder acceder a los servicios que proporciona el centro de cómputo, se recomienda que los usuarios cumplan con lo siguiente:

1. **Internos:**

   a) Si se trata de estudiantes:

   -La credencial de identificación vigente otorgada por la Universidad, o

   -El recibo de pago de la inscripción al período escolar corriente o de la última parcialidad vencida y una credencial de identificación con fotografía.

   b) Si se trata de personal académico o administrativo:

   -La credencial de identificación vigente otorgada por la Universidad, o

   -Último recibo de nómina y una credencial de identificación con fotografía.

   c) Si se trata de egresados:

   -La credencial de identificación vigente otorgada por la Universidad.

2. Externos:

a) Si se trata de participantes en cursos de formación profesional y/o educación continúa:

-Credencial de identificación con fotografía y/o el gafete de visitante que se les proporciona al ingresar al plantel, además deberán estar registrados en la lista de asistencia al curso en cuestión.

b) Si se trata de aspirantes a ingresar a la Universidad o candidatos para ocupar puestos administrativos:

-Credencial de identificación con fotografía y/o el gafete de visitante que se les proporciona cuando ingresan al plantel.

7.4. Precauciones ante los desastres naturales

Proteger los sistemas contra daños causados por el agua.

Un factor de riesgo grande en los centros de cómputo es el Agua, en el caso de Coatzacoalcos al ser considerada una zona costera las fuertes tormentas siempre arrojan grandes cantidades de agua que pueden ocasionar daño en el centro de cómputo.

Los daños por agua pueden ocurrir como resultado de goteos del techo de también goteo del aire acondicionado. Proteger el equipo, así como los muebles y cabinas contra agua y trazar un plan para la rápida eliminación de algo de agua que podría entrar en el área.

En caso de filtración de agua.

Poner particular atención en la instalación en el piso donde están instalados los sistemas de cables. Las cubiertas plásticas en canaletas son buenas para la protección del equipo contra el agua, procedente de filtraciones a través del techo. Los empleados que detecten agua en el piso, no deberán pisar el agua. Si hay cajas eléctricas inundadas, el jefe del área afectada debe localizar y bajar el

interruptor de energía eléctrica que controla la caja. En caso de que se detecte humedad en paredes o muros, los empleados no deberán tratar de investigar el problema. El encargado del centro computo o personal capacitado deberán bajar todos los interruptores de energía eléctrica y notificar al departamento de servicios generales para que investigue y en su caso corrija el problema.

Recomendaciones en caso sismos y movimientos del edificio.

En caso de sismos o movimientos del edificio, los empleados deben mantener la calma, si escuchan una alarma preventiva procederán de inmediato a desalojar las instalaciones y seguir las rutas de Evacuación para así ubicarse en una área abierta que previamente se haya definido (retirándose de edificios, bardas y cables de energía); si no se tiene tiempo de evacuar las instalaciones deberán resguardarse bajo los marcos de las puertas, escritorios, o mesas.

Una vez que el movimiento telúrico haya terminado, los empleados, sin esperar a que se les ordene, iniciaran la evacuación ordenada de las instalaciones.

Incendio.

Se recomienda que el encargado del Centro de cómputo haga un informe bimestral de los equipos contra incendio, esto con el fin de verificar que se tengan los elementos necesarios en condiciones para utilizarlo en caso de siniestro.

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

En la Universidad de Sotavento solo se cuenta con algunos extintores en algunos sitios estratégicos, para su uso se recomienda actuar con rapidez para poder sofocar el incendio.

Para ello, se debe tener en cuenta el material que está siendo consumido por el fuego, para esto es necesario que el personal haya recibido entrenamiento para su uso, ellos deben recibir algunas lecciones de instrucciones en el mecanismo de lucha contra el fuego y luego, estar enseñados de cómo operar el extintor de mano.

Es importante que existan sistemas de detección de fuego y todo el personal de esa área debe estar entrenado en la forma cómo usarlos.

Es muy importante que todo el personal reciba la instrucción de no interferir con este proceso automático y evitar su actuación en el sistema de extinción, a menos que estén seguros que no hay fuego.

Muchas veces la sensibilidad de comienzo de fuego en los aparatos de detección es muy alta. Esto genera falsas alarmas y el personal de operación se acostumbra a detener el sistema automático de extinción de fuego, sin observar realmente si hay incendio.

La Universidad no cuenta actualmente con Sistemas Automáticos Antifuego, el más común es el “Sprinklers” pero al ser un sistema “Tipo Ducha” el agua dañaría los centros de computo, por eso se recomienda el mencionado a continuación tomando en cuenta sus precauciones.

Inundación del área con gas.

Un método muy eficaz para combatir el fuego es la inundación del área con gas anti fuego. En una emergencia por fuego, el área se inunda con un determinado gas como:

- Dióxido de Carbono
- Halón.

Este sistema no causa daño al equipo, pero el personal tiene que abandonar el lugar con rapidez, porque este tipo de gas quita el oxígeno, por tanto las personas no pueden respirar y consecuentemente, causar la muerte por ahogamiento.

Mantener buenas relaciones con el departamento local de bomberos.

Otra recomendación es conseguir información con el Departamento local de Bomberos, antes de que ellos sean llamados en una emergencia.

Hacer que el Departamento esté consciente de las particularidades y vulnerabilidades del sistema por excesivas cantidades de agua que provienen de arriba y la conveniencia de una salida para el humo, tanto que minimice la cantidad de penetración al área de Procesamiento de Datos.

No es razonable anticipar que el Departamento de Bomberos puede estar completamente enterado de la situación peculiar presentada por su particular instalación. Ellos no podrían proporcionar intereses apropiados para la protección del sistema de Procesamiento de Datos, si no se les ha dado la oportunidad de revisarlo. Además, ellos pueden, usualmente, ofrecer excelentes consejos como precauciones, los cuales deben ser tomados para prevenir incendios.

Recomendaciones en caso de cortos eléctricos (Chispas).

Los empleados no deben investigar o tratar de corregir cortos circuitos o chispas asociadas con los tableros eléctricos, contactos o equipos. El encargado del Centro de computo o personal capacitado de informática bajaran los interruptores de suministro de energía eléctrica del área y notificar al departamento de servicios generales para que investigue y en su caso corrija el problema.

7.5. Que hacer en caso de acciones hostiles

Robo.

Los equipos de cómputo son posesiones muy valiosas de las empresas y están expuestas al robo.

Recomendaciones para Evitar el Robo.

- Que se creen sesiones (Passwords) para alumnos y profesores para restringir el manejo de información.
- Colocar plataformas de anclaje en los diferentes elementos del computador (Monitor, CPU e Impresora)
- Diseñar muebles para ordenadores de forma que se pueda asegurar fácilmente la máquina y los periféricos (Tapas con llave, puertas, etc.).
- Evitar que quiten la tapa del CPU y se lleven la unidad y tarjetas adaptadoras, se recomienda un sensor de movimiento.
- Colocar los proyectores (cañones) en una base fija de manera que estos no puedan ser removidos de su lugar.
- Tener un adecuado control de llaves.
- Cualquier persona puede ingresar a la Universidad ya que el Guardia de Seguridad nunca cuestiona la entrada de las personas. También existe otra entrada atrás de la cafetería la cual nunca es vigilada haciendo demasiado sencillo el acceso a la Institución de cualquier Individuo.

Sabotaje.

El peligro más temido por los centros de Procesamiento de Datos, es el sabotaje. Empresas que han intentado implementar programas de seguridad de alto nivel, han encontrado que la protección contra el saboteador es uno de los retos más duros. Este puede ser un empleado o un sujeto ajeno a la propia empresa.

La Universidad de Sotavento no tiene antecedentes de este tipo de acción hostil sin embargo se ha detectado que en este aspecto es demasiado vulnerable ya que únicamente de dispone de un guardia para toda la institución.

Requerimientos para la protección contra el sabotaje.

- Una selección rigurosa del personal.
- Buena administración de los recursos humanos.
- Buenos controles administrativos.
- Buena seguridad física en los ambientes donde están los principales componentes del equipo.
- Asignar a una sola persona la responsabilidad de la protección de los equipos en cada área.

Recomendaciones para tratar de evitar las acciones hostiles.

- No poner paredes de vidrios exteriores y ventanas en locales vulnerables
- Los Centros de Procesamiento de Datos que están localizados entre paredes de vidrio o grandes ventanas de vidrio en planta baja, son fácilmente visibles y vulnerables desde la acera o lugares altos. Estos centros de Procesamiento de Datos están expuestos a posibles tácticas destructivas por parte de grupos o individuos disidentes.
- En el caso de tener esta clase de instalación se debe considerar el uso de persianas o cubierta similar dentro de las ventanas, o uso de películas de plástico anti-impacto (suelen ser recomendadas para cubiertas exteriores donde existe vidrio). Un plástico grueso claro, como sustitución de vidrio, sería un buen empleo de desvío del arrojamiento de piedras o materiales incendiarios, y el costo de ello es suficientemente bajo para hacer una instalación económicamente factible en la mayoría de los centros.

Mantener una buena relación con el departamento de policía local.

La Administración del Centro de Cómputo o Personal de Servicio de Seguridad y el Abogado o Asesor jurídico, deberán reunirse con las autoridades del Departamento de Policía Local.

Debe asegurarse, en caso de emergencia, el llamar al departamento de Policía. El tiempo de la respuesta de un departamento puede variar ampliamente entre el día y la noche.

Es importante saber qué tipo de servicio ofrecen. Generalmente, se cree que la policía puede ser llamada para retirar a un intruso que se encuentre en la propiedad. Frecuentemente, ellos sólo darán este servicio en circunstancias especiales.

Estas circunstancias deben ser aclaradas, para que las personas responsables de llamar a la policía sepan qué servicio en particular deberá esperar que ella provea.

Amenazas telefónicas y amenazas de bombas.

Durante las operaciones normales del centro de cómputo administrativo y laboratorio de cómputo, cualquier persona que conteste un teléfono, está sujeta a recibir amenazas telefónicas dirigidas contra las instalaciones, al personal del centro de cómputo o al laboratorio de cómputo.

Que debe hacer la persona que recibe la llamada.

1. Tratar todas las amenazas como hechos reales.
2. No elaborar supuestos acerca de los motivos del que hace la amenaza telefónica.
3. Notificar únicamente al jefe inmediato, al encargado del centro de cómputo o comunicarse con la dirección general.
4. No ocasionar pánico comentando la amenaza con los demás empleados.

El coordinador de computo o la persona a cargo rápidamente evaluara la amenaza, después de analizar la situación puede determinar la evacuación del personal, antes de que la policía se presente a realizar la búsqueda y se encargue

de los objetos que resulten sospechosos, inmediatamente hará el reporte de la amenaza de bomba a la policía para que realice la búsqueda en el Centro de Computo o demás áreas. La búsqueda se efectuara en todas las áreas, dentro y fuera de las instalaciones, en el estacionamiento, en los patios, corredores, baños, áreas de almacenamiento, etc.

En caso de que se identifique un objeto sospechoso, se deberá notificar inmediatamente a la persona que esté a cargo de esta situación, es importante que bajo ninguna circunstancia ningún empleado deba tocar o mover el objeto.

Evacuación de las instalaciones.

Cuando se identifica y se investiga una situación de emergencia, el encargado del centro computo o quien esté a cargo ordenara una evacuación ya sea parcial o total. Si se ordena una evacuación parcial, el encargado monitoreara la situación personalmente y ordenara la evacuación total, una vez que esté justificada el proceso de evacuación se realizara conforme a los siguientes pasos:

- Notificar al personal informando a todo el personal del centro de cómputo y demás áreas que hay una evacuación en progreso.
- Mover al personal evacuar a los empleados del centro de cómputo y reunirlos en un área de recuperación seleccionada, alejada de las instalaciones.
- Hacer un paro del equipo para minimizar los riesgos de shock eléctrico y daños al equipo.
- Asegurar las instalaciones para proteger el centro de cómputo durante la situación de emergencia contra robo, vandalismo, etc.
- Notificar a las autoridades informando a la policía, los bomberos, los rescatistas y a otras dependencias de apoyo en caso de la eventualidad de que las instalaciones han sufrido una emergencia.

7.6. Primeros Auxilios

El objetivo de los primeros auxilios es tratar de salvar la vida y de evitar la aparición de secuelas o de incapacidades que puedan resultar como consecuencia del accidente que sufra el empleado o alumno del Centro de Cómputo.

Lineamientos:

- Cualquier persona que haya sufrido un accidente debe recibir los primeros auxilios inmediatamente, y ser trasladado a la brevedad posible a la unidad médica más cercana para que reciba la atención correspondiente, el caso de la Universidad de Sotavento cuenta con un área destinada a los primeros auxilios.
- Los responsables de prestar los primeros auxilios deben continuar el cuidado del empleado hasta que se pueda obtener la atención médica.
- Los primeros auxilios deben ser prestados por el personal que haya sido capacitado especialmente por personal médico en esas técnicas. es recomendable tener al menos a personas entrenadas en primeros auxilios en cada turno para que se dé respuesta rápidamente.
- Para prestar los primeros auxilios se requiere de un equipo compuesto por un conjunto de elementos básicos que deben mantenerse en disponibilidad permanente durante los turnos de trabajo.
- El centro y los laboratorios de cómputo deberán tener disponible el equipo apropiado para remover de la fuente de shock a una persona que ha recibido un shock eléctrico. El centro y los laboratorios de cómputo, deberán tener disponibles sabanas para mantener en calor al paciente.

- El personal del centro de trabajo designado para prestar los primeros auxilios es responsable de la conservación y el empleo del equipo destinado para ello.
- Los conocimientos de primeros auxilios deben incluir procedimientos para salvar vidas, prevención de heridas adicionales, y la colocación del paciente en el sistema apropiado de emergencia médica.
- En cualquier caso, todas las eventualidades que requieran primeros auxilios deberán ser notificadas a la unidad médica.

7.7. Recomendaciones para enfermedades diagnosticadas

Todo el personal con una enfermedad diagnosticada, como diabetes o epilepsia, deberá asegurarse que su superior de área este consciente de esta condición para facilitar la reacción en caso de posibles síntomas.

Para una persona inconsciente.

Al identificar a una persona inconsciente, se deberá notificar inmediatamente a la unidad médica y la persona capacitada en primeros auxilios, mientras esto ocurre, se deberá determinar la causa de la inconsciencia, el personal deberá tener la lista con los teléfonos para contactar al servicio médico necesario para su traslado si es necesario.

Para el transporte.

En caso de que el personal sufra algún accidente dentro de la institución y requiera ser trasladado de emergencia a cualquier unidad médica, se cuente con un medio de transporte propio del colegio para este tipo de eventualidades o cualquier otro.

7.8. Energía eléctrica

Unos de los puntos más vulnerables del Centro de Computo de la Universidad es su instalación eléctrica.

Se asegurara de que los cables eléctricos y las cajas de empalme estén levantados del piso. Los cables eléctricos, cajas de empalme, switches, toma de energía eléctrica y paneles estén localizados fuera del alcance de derrames potenciales de líquidos (ventanas, lavabos, maquinas de café, etc.); deberá proveer el drenaje adecuado y otros materiales para remover derrames de líquidos en las áreas de trabajo. Restringirán el uso de cables eléctricos sueltos en áreas de tráfico frecuente de usuarios; se asegurara que todos los circuitos estén conectados a una tierra común; y de que haya suficientes circuitos y estén instalados en forma distribuida para que ninguno se sobrecargue.

Los controles eléctricos serán guardados en paneles debidamente controlados. Se deberá procurar que las cajas de interruptores de energía eléctrica estén accesibles fácilmente e instalados cerca de la entrada al centro de computo y de las salidas del edificio.

7.9. Equipo de seguridad

El Coordinador del centro de computo debe asegurar de que se adhieran etiquetas de aviso a los cables eléctricos, cajas de empalme, paneles y equipo eléctrico, y que los extinguidores portátiles de incendio estén localizados cerca del alcance de la mayoría de los empleados del centro.

Para las Heridas menores el equipo de primeros auxilios deberá contar con suficientes vendas y otros materiales para heridas menores, incluyendo desinfectantes, vendas esterilizadas, etc.

En la mayoría de los casos los empleados que sufran heridas menores (ejemplo: cortadas por papel, heridas con vasos de vidrio rotos u otros objetos filosos) deberán ser capaces de manejarse ellos mismos usando el equipo de primeros auxilios.

Si no es así, una de las personas entrenadas para asistir en primeros auxilios será llamada para que colabore.

Todo el personal debe estar avisado sobre las emergencias médicas posibles que pueden suscitarse durante la jornada escolar y deben tomar

lineamientos propios para estar preparados en caso de emergencia y ayudarse ellos mismos y a sus compañeros de trabajo.

La administración del Centro de Cómputo, así como los distintos laboratorios de cómputo deben asistir a todos sus empleados en su esfuerzo y desempeño sobre estos lineamientos.

Conclusiones

Evaluar y controlar permanentemente la seguridad física del edificio es la base para o comenzar a integrar la seguridad como una función primordial dentro de cualquier organismo.

Antes de empezar por una seguridad lógica se recomienda empezar por lo físico ya que esto será la base de todos las implementaciones de seguridad que se quieran ir agregando en un futuro esto dependerá del tamaño y necesidad de la empresa, que tan importante y crucial sea mantener seguro los datos, sin embargo cualquier empresa tiene la obligación de dar seguridad a todo el personal que labore y hacerlo sentir cómodo ya que esto también influirá y se verá reflejado en gran medida en los objetivos ya planteados.

Tener controlado el ambiente y acceso físico permite:

- Disminuir siniestros
- Trabajar mejor manteniendo la sensación de seguridad
- Descartar falsas hipótesis si se produjeran incidentes
- Tener los medios para luchar contra accidentes

Las distintas alternativas estudiadas son suficientes para conocer en todo momento el estado del medio en el que nos desempeñamos; y así tomar decisiones sobre la base de la información brindada por los medios de control adecuados.

Estas decisiones pueden variar desde el conocimiento de la áreas que recorren ciertas personas hasta la extremo de evacuar el edificio en caso de accidentes.

"Cuando no ocurre nada, nos quejamos de lo mucho que gastamos en seguridad. Cuando algo sucede, nos lamentamos de no haber invertido más... Más vale dedicar recursos a la seguridad que convertirse en una estadística."[10]

[10]"*Seguridad de la información"/ Cristian Borghello*

Glosario

Biometría.- Parte de la biología que estudia en forma cuantitativa la variabilidad individual de los seres vivos utilizando métodos estadísticos.

Bucles.- En programación se entiende por bucle una secuencia de instrucciones que se repite varias veces. Pero las instrucciones sólo se introducen una vez en el código del programa. El número de repeticiones depende del valor de una variable que se llama contador.

CCTV.- Circuito cerrado de cámaras de TV: el uso de cámaras para tareas de vigilancia

Ergonomía.- Ciencia que se encarga de adaptar el cuerpo humano a las tareas y las herramientas de trabajo.

Hardware.- En contraposición al Software, es la "parte dura", es decir, los elementos físicos de la arquitectura de un ordenador, desde la CPU hasta el monitor, pasando por todos los periféricos que pueden ser acoplados al ordenador.

Outsourcing.- Proveedor de servicios. Modalidad de contratación en que una organización exterioriza determinadas actividades de la empresa, susceptibles de funcionar independiente, con el objetivo de reducir costes y mejorar servicios.

PIN.- Significa número de identificación personal y sirve para identificarse en un sistema de información.

Red.- Sistema de elementos interrelacionados que se conectan mediante un vínculo dedicado o conmutado para proporcionar una comunicación local o remota (de voz, vídeo, datos, etc.) y facilitar el intercambio de información entre usuarios con intereses comunes.

Sistemas de Información.- Son los flujos de información de una organización con medios electrónicos. Pueden ser aplicaciones de todo tipo de proceso de datos, automatización de oficinas y sistemas expertos. (Information systems)

Software.- Conjunto de componentes lógicos (instrucciones o datos) que hacen funcionar una computadora o posibilitan la operación de una red. Se considera software a todo aquello que se pueda almacenar electrónicamente en un sistema computacional.

Sprinklers.- El sistema de regaderas automáticas, conocido también como sistema sprinkler, es el más efectivo en la protección contra incendio.

Termograma.- Representación gráfica de una variación de temperatura.

Bibliografía

1. Seminario “Seguridad en Redes 2006”, InfoWorld México, Jaime Oliva Garduño

2. “ISACA”. http://www.isaca.org

3. “Corolario de Weinberge”, Leyes de Murphy

4. “Seguridad en Unix y Redes", HUERTA, Antonio Villalón, Open Publication License v.10 o Later. 2 de Octubre de 2000. http://www.kriptopolis.org

5. “Seguridad-Introducción a la seguridad informática”, Kioskea

6. Code of practice for information security management. http://www.iso.org/iso/support/faqs/

7. “Seguridad Informática”, ALDEGANI, Gustavo. Miguel, 1° Edición. Argentina

8. “Revista Virtual Seguridad Corporativa”, MANUNTA, Giovanni. http://www.seguridadcorporativa.org

9. “Evaluación de Seguridad de un Sistema de Información”, José Alfredo Jiménez

10. “Seguridad de la información”, Cristian Borghello

11. “Boletín” GÓMEZ, David José Manuel. Enero 1999 - Julio 2001. http://www.kriptopolis.org/boletin

12. “Firewalls Complete”, GONCALVES, Marcus. Editorial McGraw Hill. EE.UU, 1997. http://www.ods.com.ua/win/eng/security/firewall

13. Revista RED, “La comunidad de expertos en redes”, Noviembre, 2002.

Anexos

Ergonomía

La ergonomía es una disciplina que se ocupa de estudiar la forma en que interactúa el cuerpo humano con los artefactos y elementos que lo rodean, buscando que esa interacción sea lo menos agresiva y traumática posible.

El enfoque ergonómico plantea la adaptación de los métodos, los objetos, las maquinarias, herramientas e instrumentos o medios y las condiciones de trabajo a la anatomía, la fisiología y la psicología del operador. Entre los fines de su aplicación se encuentra, fundamentalmente, la protección de los trabajadores contra problemas tales como el agotamiento, las sobrecargas y el envejecimiento prematuro.

Trastornos Óseos y Musculares

Una de las maneras de provocar una lesión ósea o muscular es obligar al cuerpo a ejecutar movimientos repetitivos y rutinarios, y esta posibilidad se agrava enormemente si dichos movimientos se realizan en una posición incorrecta o antinatural.

En el ambiente informático, la operación del teclado es un movimiento repetitivo y continuo, si a esto le sumamos el hecho de trabajar con una distribución ineficiente de las teclas, el diseño antinatural del teclado y la ausencia (ahora atenuada por el uso del Mouse) de movimientos alternativos al de tecleado, tenemos un potencial riesgo de enfermedades o lesiones en los músculos, nervios y huesos de manos y brazos.

En resumen, el lugar de trabajo debe estar diseñado de manera que permita que el usuario se coloque en la posición más natural posible. Como esta posición variará de acuerdo a los distintos usuarios, lo fundamental en todo esto

es que el puesto de trabajo sea ajustable, para que pueda adaptarse a las medidas y posiciones naturales propias de cada operador.

Trastornos Visuales

Los ojos, sin duda, son las partes más afectadas por el trabajo con computadoras.

La pantalla es una fuente de luz que incide directamente sobre el ojo del operador, provocando, luego de exposiciones prolongadas el típico cansancio visual, irritación y lagrimeo, cefalea y visión borrosa.

Si a esto le sumamos un monitor cuya definición no sea la adecuada, se debe considerar la exigencia a la que se someterán los ojos del usuario al intentar descifrar el contenido de la pantalla.

Además de la fatiga del resto del cuerpo al tener que cambiar la posición de la cabeza y el cuello para acercar los ojos a la misma.

Para prevenir los trastornos visuales en los operadores podemos tomar recaudos como:

- Tener especial cuidado al elegir los monitores y placas de vídeo de las computadoras.
- Usar pantallas antirreflejo o anteojos con protección para el monitor, es una medida preventiva importante y de relativo bajo costo, que puede solucionar varios de los problemas antes mencionados.

La Salud Mental

La carga física del trabajo adopta modalidades diferentes en los puestos informatizados. De hecho, disminuye los desplazamientos de los trabajadores y las tareas requieren un menor esfuerzo muscular dinámico, pero aumenta, al mismo tiempo, la carga estática de acuerdo con las posturas inadecuadas asumidas.

Por su parte, la estandarización y racionalización que tiende a acompañar la aplicación de las PCs en las tareas de ingreso de datos, puede llevar a la transformación del trabajo en una rutina inflexible que inhibe la iniciativa personal, promueve sensaciones de hastío y monotonía y conduce a una pérdida de significado del trabajo.

Además, el estrés informático está convirtiéndose en una nueva enfermedad profesional relacionada con el trabajo, provocada por la carga mental y psíquica inherente a la operación con los nuevos equipos.

Los efectos del estrés pueden encuadrarse dentro de varias categorías:

- Los efectos fisiológicos inmediatos, caracterizados por el incremento de la presión arterial, el aumento de la frecuencia cardiaca, etc.
- Los efectos psicológicos inmediatos hacen referencia a la tensión, irritabilidad, cólera, agresividad, etc. Estos sentimientos pueden, a su vez, inducir ciertos efectos en el comportamiento tales como el consumo de alcohol y psicofármacos, el hábito de fumar, etc.
- También existen consecuencias médicas a largo plazo, tales como enfermedades coronarias, hipertensión arterial, úlceras pépticas, agotamiento; mientras que las consecuencias psicológicas a largo plazo pueden señalar neurosis, insomnio, estados crónicos de ansiedad o depresión, etc.
- La apatía, sensaciones generales de insatisfacción ante la vida, la pérdida de la propia estima, etc., alteran profundamente la vida personal, familiar y social del trabajador llevándolo, eventualmente, al aislamiento, al ausentismo laboral y la pérdida de la solidaridad social.

Ambiente Luminoso

Se parte de la base que las oficinas mal iluminadas son la principal causa de la pérdida de la productividad en las empresas y de un gasto energético

excesivo. Una iluminación deficiente provoca dolores de cabeza y perjudica a los ojos.

Ambiente Climático

En cuanto al ambiente climático, la temperatura de una oficina con computadoras debe estar comprendida entre 18 y 21 grados centígrados y la humedad relativa del aire debe estar comprendida entre el 45% y el 65%.

En todos los lugares hay que contar con sistemas que renueven el aire periódicamente. No menos importante es el ambiente sonoro por lo que se recomienda no adquirir equipos que superen los 55 decibeles, sobre todo cuando trabajan muchas personas en un mismo espacio.

Encuestas

Encuesta 1.- Factores de Riesgos en el Centro de Computo de la Universidad de Sotavento

Facultad_____ Semestre_____

¿Considera usted que el riesgo de que exista Robo en el Centro de Computo es?

*Bajo *Muy Bajo *Alto *Muy Alto *Medio

¿Considera usted que el riesgo de que exista Vandalismo en el Centro de Computo es?

*Bajo *Muy Bajo *Alto *Muy Alto *Medio

Las Fallas de los equipos del Centro de Cómputo se dan en frecuencias.

*Bajo *Muy Bajo *Alto *Muy Alto *Medio

¿Considera usted que el riesgo de que existan Virus en el Centro de Computo es?

*Bajo *Muy Bajo *Alto *Muy Alto *Medio

¿Para usted los Accesos no Autorizados en los Centros de Cómputo tienen un factor?

*Bajo *Muy Bajo *Alto *Muy Alto *Medio

¿Considera usted que el riesgo que se genere un incendio en los Centros de Computo es?

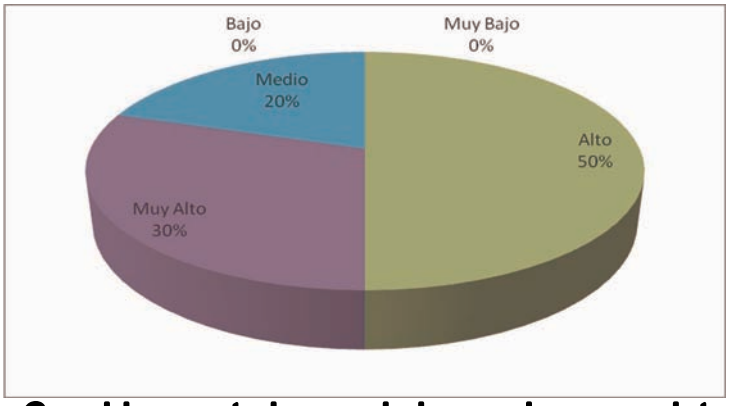
*Bajo *Muy Bajo *Alto *Muy Alto *Medio

¿Conoce usted el punto reunión de una de evacuación en caso de Siniestro?

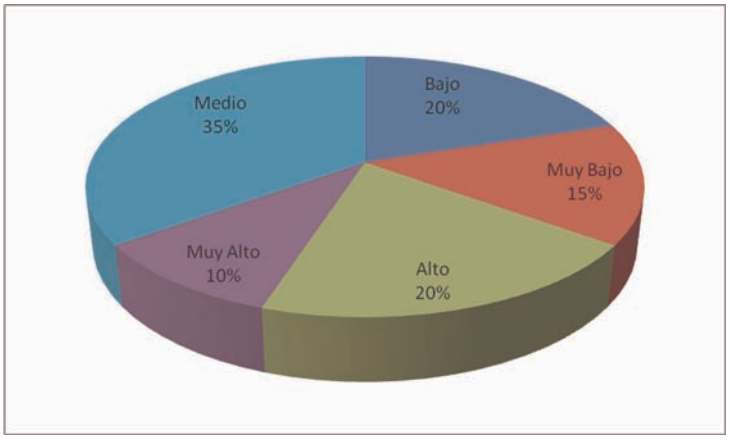
Si No

Resultados de la Encuesta 1, aplicada a 20 usuarios del Centro de Computo de la Universidad de Sotavento.

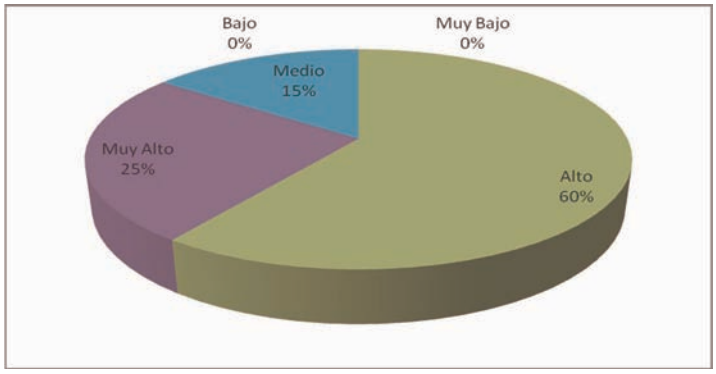
¿Considera usted que el riesgo de que exista Robo en el Centro de Computo es?



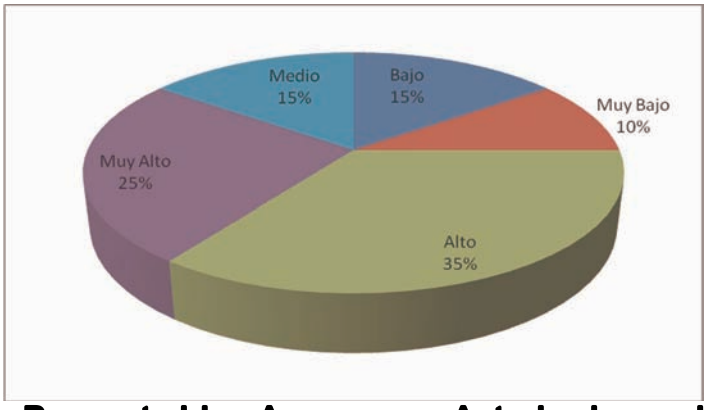
¿Considera usted que el riesgo de que exista Vandalismo en el Centro de Computo es?



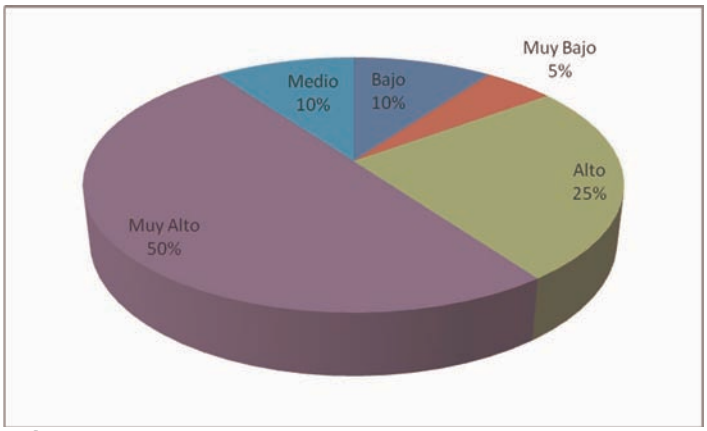
Las Fallas de los equipos del Centro de Cómputo se dan en frecuencias.



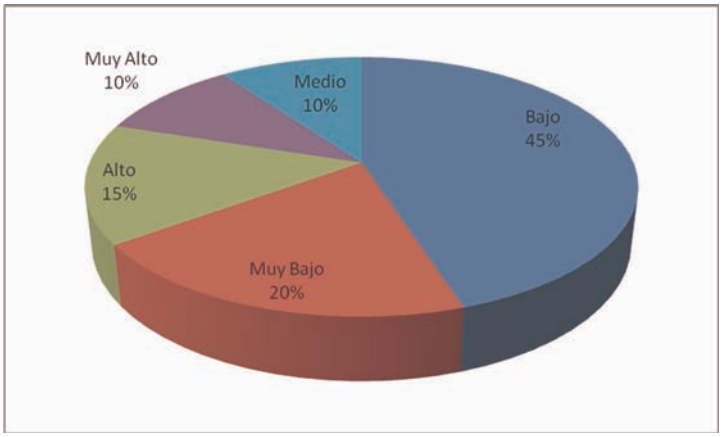
¿Considera usted que el riesgo de que existan Virus en el Centro de Computo es?



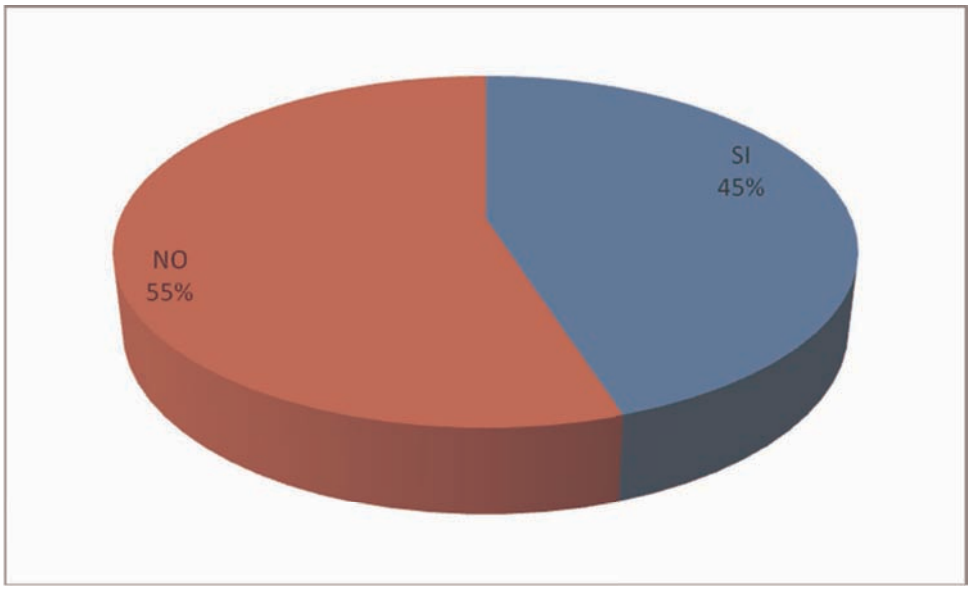
¿Para usted los Accesos no Autorizados en los Centros de Cómputo tienen un factor?



¿Considera usted que el riesgo que se genere un incendio en los Centros de Computo es?



¿Conoce usted el Punto Reunión de una de evacuación en caso de Siniestro?



Encuesta 2.- Protecciones Actuales en el Centro de Computo de la Universidad de Sotavento

Área_____ Responsable_____

¿Se realizan copias periódicas de los archivos que son vitales para la institución?

Siempre A veces Nunca

¿Qué acciones realizan para evitar el Robo Común en el Centro de Cómputo de la Universidad?

_____

_____

_____

_____

¿El software que de instala en los equipos todo el tiempo es verificado por un Antivirus?

Siempre A veces Nunca

¿Considera que la formación que tienen los Becarios es?

Buena Regular Mala Pésima

¿Considera que existe un Control de Llaves adecuado?

Si No

¿Y por qué?

_____

_____

_____

¿En la actualidad se cuenta con Sistemas contra Incendio?

Si No

¿Cuáles?

_____

_____

¿Existe el Robo en el Centro de Cómputo?

_____

_____

¿Qué factor de Robo existe?

*Bajo *Muy Bajo *Alto *Muy Alto *Medio

¿Cuáles son los Robos más habituales en el Centro de Cómputo?

_____

_____

En el último Semestre que equipo de Cómputo han robado

_____

_____

Resumen de los resultados de la Encuesta 2, aplicada a los responsables del centro de cómputo de la Universidad de Sotavento.

Aplicada a: Ing. Ángel Castillo y Misael Cruz Santiago

Copias periódicas de Archivos Vitales: Siempre

Acciones para Evitar el Robo Común: El uso de llaves y el Cierre de las aulas al terminar cada maestro, también se le cuenta el equipo total al final de la clase para verificar que este completo.

El software que se instala en los equipos de cómputo es siempre verificado por un Antivirus: A veces

La formación de los becarios es: Buena

El control de llaves es adecuado: Si, cada becario que entra y sale es el responsable de la llave, así como el uso adecuado de ello.

En la actualidad se cuenta con sistemas contra incendio: Si, Extinguidores

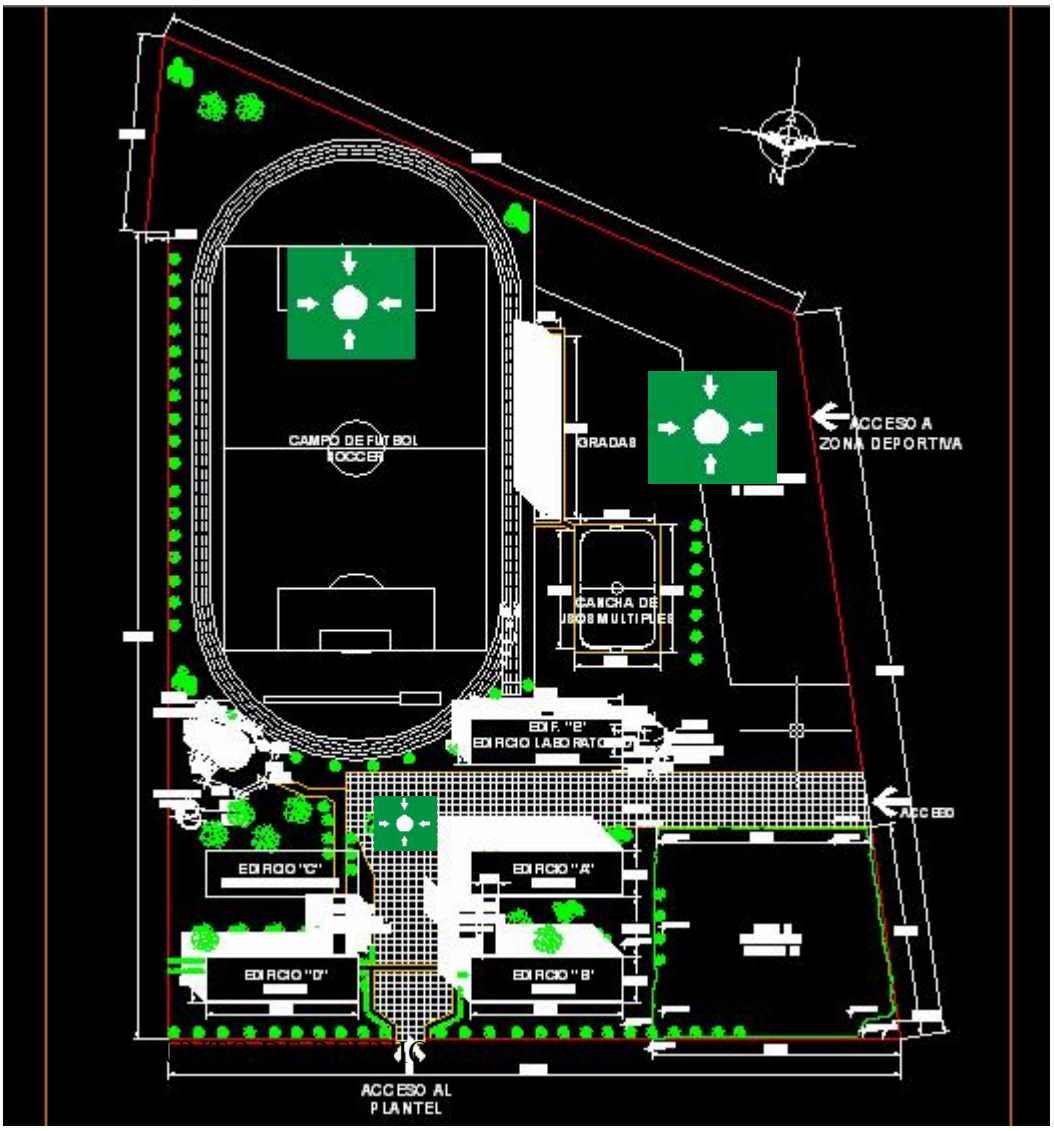
Existe el robo en el centro de cómputo: Si

Que factor de robo existe: Bajo

Cuáles son los robos más habituales: Mouse, Memorias.

En el último semestre que han robado: Mouse, Memorias, Teclados, Una Laptop, Un Proyector (Cañón) y el semestre anterior un Monitor Plano en el Aula clavijero.

Plano de Rutas de Evacuación



Lista de teléfonos de emergencia

Bomberos	212-5141, 213-0374
Cruz Roja	214-0405, 214-0434
Policía Municipal	214-1009, 214-1108
Policía Federal Preventiva	214-6405, 214-4822

Nota: Se recomienda tener el número del proveedor del host de la página de la Universidad, por políticas de la Institución no fue incluido en los anexos.