UNIVERSIDAD LATINOAMERICANA DE CIENCIA Y TECNOLOGÍA

Facultad de Ingeniería

Escuela de Ingeniería

Trabajo final para optar por el grado de Licenciatura en Informática en Gestión de Recursos Tecnológicos

Tema: Análisis de la seguridad física, aplicable a un Centro de Cómputo, de acuerdo a las buenas prácticas y normativa aplicada

Estudiante: Bernardo Fernández Ramírez

Cédula: 1-0810-0276

Profesor: Lic. Miguel Pérez Montero

I Cuatrimestre 2008

Indice

Centro de Cómputo: Espacio físico donde se albergan los servidores o computadores, equipo de comunicaciones, conocido comúnmente como el "CORE del negocioso".

Ing. Bernardo Fernández Ramírez[1]

Resumen

El desarrollo de las organizaciones, en el mundo globalizado, ha generado que los sistemas informáticos sean más complejos, lo cual contribuye a la especialización de una parte de la informática, enfocada en la gestión de las tecnologías de Información.

Existe una especialización en materia de seguridad física y lógica para administrar tanto la información, como las plataformas tecnológicas que soportan los sistemas informáticos modernos. La administración de los centros de cómputo, no es la excepción en complejidad de su gestión.

Un centro de cómputo debe conceptualizarse como un área de acceso restringido, en los que la interacción humana debe ser mínima, con el fin de mantener las condiciones idóneas en materia de seguridad ambiental y de acceso a la información. El control de acceso debe conceptualizarse como una bóveda, donde todo movimiento debe ser registrado por diversos métodos y sistemas de control, tales como: cámaras de circuito cerrado, llavines magnéticos, y registros escritos de las actividades que se desarrollan en dichos recintos.

En esta materia, se han desarrollado muchos y diversas normativas que se especializan en áreas específicas en materia de seguridad de centros de cómputo. Así, existen códigos en materia de comunicaciones, electricidad, infraestructura, ambiente, en los cuales se apoyan los códigos que desarrollan normativas de seguridad física para centros de cómputo.

La presente investigación, pretende visualizar las mejores prácticas que se puede aplicar en materia de seguridad física a un centro de cómputo, para una compañía autónoma del estado de Costa Rica, con la finalidad de facilitar y prevenir debilidades que atenten contra la continuidad de las operaciones, y a su vez, sirva como agente disparador en la adopción de sanas prácticas, según las normativas de punta.

Palabras clave: Seguridad Física, Centro de Cómputo, Normativa, Buenas Prácticas, Tecnologías de Información.

[1] Ing. Bernardo Fernández Ramírez, candidato a Licenciado en Informática con énfasis en Gestión en Recursos Tecnológicos, Correo electrónico: bfernandez@costarricense.cr

Abstract

The develop of the organizations, in the globalize World, has generated that all the computer systems be more complex, which contributes to the specialization in a part of the informatics, focus in the management of the information technologies.

There is a special study in the subject of physical security and logistics to administrate the information as much as the technological platforms that give support to the modern informatics systems. The administration of the Data centers, is not the exception in the complexity of it management.

A computer center must be conceptualized as a restricted access area, in which the human interaction must be minimum, with the purpose of maintaining the right conditions in the subject of environmental security and of access to the information. The access control must be conceptualized as a vault, where every movement has to be registered by several methods and control systems such as: close circuit cameras, magnetic locks, and written registers of the activities developing in the already mentioned precincts.

In this matter, have been developed a lot of norms specialize in specific areas related to Security of Data Centers. In fact, there are codes related to communications, electricity, infrastructure, environment; and those are the foundation of Physical Security Norms for Data Centers.

This research try to visualize the best practices for apply in matter of Phisical Security for Data Centers, for an self-support company of state of Costa Rica, with the purpose of make easier and prevent risks that attempt against the continuity of the business's operations; and at the same time it can be useful as a trigger in the adoption of best practices according to the last Norms of the Industry.

Key words: Physical Security, Data Center, Norm, Best Practices, Technologies of Information

I. Introducción

Esta investigación se ha llevado a cabo en una Institución autónoma del sector público nacional y dado que se incluyen detalles que podrían comprometer la seguridad de dicha entidad, se ha optado por mantenerla en el anonimato, no obstante, los resultados de este estudio serán utilizados por dicha institución para mejorar su condición actual.

En esta institución, se ha implementado un centro de cómputo que se ha quedado rezagado en cuanto a las exigencias de continuidad y seguridad, de acuerdo con el crecimiento y desarrollo del negocio, lo que ha redundado en no contar con un centro de cómputo que garantice la continuidad de las operaciones, y la seguridad física de la información y de los equipos que la soportan.

De cara a una inevitable apertura del mercado de los mercados, esta situación representa una amenaza real, que puede materializar riesgos tales como: pérdida y trasiego de información, daños en equipo vitales de negocio en telecomunicaciones y almacenamiento, pérdida de capacidad de respuesta ante las amenazas y oportunidades del mercado, inadecuado uso de los recursos tecnológicos, entre otros.

Por otro lado los estándares y normativas mundiales presionan por que cada organización que se considere competitiva, cuide y administre sus recursos en materia de TI, de manera organizada, orientada a la gestión por medio de procesos que garanticen la gobernabilidad de TI.

Localmente, a mediados del año pasado, la Contraloría General de la República, emitió el nuevo Manual de Normas técnicas para Control y la gestión de TI, el cual enmarca las buenas prácticas mínimas que debe implementar tanto la misma Contraloría General de la República, como las organizaciones sujetas a su fiscalización. Estas normas deben ser implementadas a más tardar a 31 de julio del 2009.

Dicho Manual está basado en normativas de punta en materia de gestión de TI; tales como COBIT, ITIL, ISO 27001, PMBOOK, que vienen impulsar la metodología de realizar las actividades por medio de procesos, los cuales deberán aplicarse para la gestión apropiada de las TI, con el único objetivo de garantizar la calidad de los servicios que brinda cada Institución.

La investigación se basa en la recolección de información a partir de fuentes bibliográficas e internet, así como de la obtención de los documentos generados a partir de previos diagnósticos.

Los aspectos a recopilar en la fase teórica serán: Seguridad Física como punto fundamental, Infraestructura, Comunicaciones, Instalación eléctrica y Aire Acondicionado. El artículo está enfocado en la seguridad física de los centros de cómputo, los capítulos en los que se describe seguridad, Infraestructura y comunicaciones son en los que eventualmente se basarán las conclusiones y recomendaciones. Los capítulos referentes a Instalación eléctrica y Aire acondicionado a pesar que conforman aspectos que se deben evaluar por separado en la implementación de centros de cómputo, se utilizarán como apoyo en la descripción, como complementos a la seguridad.

Con base en los aspectos teóricos anteriores, se procederá a establecer el nivel de cumplimiento de las medidas de seguridad del Centro de Cómputo de la institución sujeta de estudio, se propondrán las medidas en materia de seguridad física que se pueden aplicar en el corto plazo para ajustarse a un nivel aceptable, proponer las medidas necesarias para garantizar la continuidad de las operaciones, en materia de Hardware, respaldo eléctrico, ambiente, espacio físico.

II. **Normativa**

En materia de diseño será basado en la normativas internacionales tales como: COBIT, ITIL, ISO 27001 y adicionalmente apoyado tanto en el Manual de normas Técnicas para la Gestión y Control de la tecnologías de Información y El Manual de Control Interno; emitidos por la Contraloría General de la República. Cada recomendación será justificada y referenciada puntualmente por la normativa.

El marco de referencia Cobit (*Control Objectives for Information and related Technology)* del IT Governance Institute), se ha convertido en un estandar de aplicación en materia de Gobierno de Tecnologías de Información (TI), utilizada por las organizaciones que pretendan garantizar minimizar los riesgos asociados en la gestión de los recursos informáticos, según el Governance Institute (Cobit 4.0, 2006):

> COBIT es un marco de referencia y un juego de herramientas de soporte que permiten a la gerencia cerrar la brecha con respecto a los requerimientos de control, temas técnicos y riesgos de negocio, y

> comunicar ese nivel de control a los participantes. COBIT permite el desarrollo de políticas claras y de buenas prácticas para control de TI a través de las empresas. COBIT constantemente se actualiza y armoniza con otros estándares. Por lo tanto, COBIT se ha convertido en el integrador de las mejores prácticas de TI y el marco de referencia general para el gobierno de TI que ayuda a comprender y administrar los riesgos y beneficios asociados con TI. La estructura de procesos de COBIT y su enfoque de alto nivel orientado al negocio brindan una visión completa de TI y de las decisiones a tomar acerca de TI. (p.9)

Otra norma de uso obligatorio de referencia, es la norma en materia de seguridad ISO:27001, según lo como lo establece Corletti(2006):

> ISO (Organización Internacional de Estándares) e IEC (Comisión Internacional de Electrotecnia) conforman un sistema especializado para los estándares mundiales. Organismos nacionales (España) que son miembros de ISO o IEC participan en el desarrollo de Normas Internacionales a través de comités técnicos establecidos por la organización respectiva para tratar con los campos particulares de actividad técnica. Los comités técnicos de ISO e IEC colaboran en los campos de interés mutuo. Otras organizaciones internacionales, gubernamentales y no gubernamentales, en relación con ISO e IEC, también forman parte del trabajo. En el campo de tecnología de información, ISO e IEC han establecido unir un comité técnico, ISO/IEC JTC 1 (Join Technical Committee Nº1). Los borradores de estas Normas Internacionales adoptadas por la unión de este comité técnico son enviados a los organismos de las diferentes naciones para su votación. La publicación, ya como una Norma Internacional, requiere la aprobación de por lo menos el 75% de los organismos nacionales que emiten su voto. El Estándar Internacional ISO/IEC 17799 fue preparado inicialmente por el Instituto de Normas Británico (como BS 7799) y fue adoptado, bajo la supervisión del grupo de trabajo “Tecnologías de la Información”, del Comité Técnico de esta unión entre ISO/IEC JTC 1, en paralelo con su aprobación por los organismos nacionales de ISO e IEC.

De la mano del la Normativa Cobit, que establece qué se debe adoptar en materia de gestión de recursos informáticos, tenemos a la normativa ITIL en su Version 3, la cual establece el cómo se pude implementar las acciones. Así lo establece la enciclopedia electrónica Wikipedia (2008):

> La ***Information Technology Infrastructure Library*** (‘Biblioteca de Infraestructura de Tecnologías de Información’), frecuentemente abreviada

ITIL, es un marco de trabajo de las mejores prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información (TI) de alta calidad. ITIL resume un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI. Estos procedimientos son independientes del proveedor y han sido desarrollados para servir de guía para que abarque toda infraestructura, desarrollo y operaciones de TI.

ITIL se considera a menudo junto con otros marcos de trabajo de mejores prácticas como la *Information Services Procurement Library* (ISPL, 'Biblioteca de adquisición de servicios de información'), la *Application Services Library* (ASL, 'Biblioteca de servicios de aplicativos'), el método de desarrollo de sistemas dinámicos (DSDM, *Dynamic Systems Development Method*), el Modelo de Capacidad y Madurez (CMM/CMMI) y a menudo se relaciona con la gobernanza de tecnologías de la información mediante COBIT (*Control Objectives for Information and related Technology*).

Por otro lado, tenemos el Manual de Normas Técnicas para la Gestión y Control de TI, emitida el año anterior por la Contraloría General de la República, la cual está basada en materia de seguridad e infraestructura en los estándares anteriores, y otros, en donde se establece qué debe implementar las organizaciones en ésta materia. Lo anterior se puede sustentar en la norma 1.4.3, según Contraloría General de la República (2007), de la siguiente manera:

1.4.3 Seguridad física y ambiental

La organización debe proteger los recursos de TI estableciendo un ambiente físico seguro y controlado, con medidas de protección suficientemente fundamentadas en políticas vigentes y análisis de riesgos. Como parte de esa protección debe considerar:

a. Los controles de acceso a las instalaciones: seguridad perimetral, mecanismos de control de acceso a recintos o áreas de trabajo, protección de oficinas, separación adecuada de áreas.
b. La ubicación física segura de los recursos de TI.
c. El ingreso y salida de equipos de la organización.
d. El debido control de los servicios de mantenimiento.
e. Los controles para el desecho y reutilización de recursos de TI.
f. La continuidad, seguridad y control del suministro de energía eléctrica, del cableado de datos y de las comunicaciones inalámbricas.
g. El acceso de terceros.
h. Los riesgos asociados con el ambiente. (p.3)

Adicionalmente las instalaciones y la infraestructura que soporta la plataforma tecnológica debe ser mantenida por las organizaciones en condiciones que garanticen la continuidad y confiabilidad de las operaciones, tal como lo exige la Contraloría General de la República (2007), según la norma 4.2:

> ***4.2 Administración y operación de la plataforma tecnológica***
> La organización debe mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas. Para ello debe:
> a. Establecer y documentar los procedimientos y las responsabilidades asociados con la operación de la plataforma.
> b. Vigilar de manera constante la disponibilidad, capacidad, desempeño y uso de la plataforma, asegurar su correcta operación y mantener un registro de sus eventuales fallas.
> c. Identificar eventuales requerimientos presentes y futuros, establecer planes para su satisfacción y garantizar la oportuna adquisición de recursos de TI requeridos tomando en cuenta la obsolescencia de la plataforma, contingencias, cargas de trabajo y tendencias tecnológicas. d. Controlar la composición y cambios de la plataforma y mantener un registro actualizado de sus componentes (hardware y software), custodiar adecuadamente las licencias de software y realizar verificaciones físicas periódicas.
> e. Controlar la ejecución de los trabajos mediante su programación, supervisión y registro.
> f. Mantener separados y controlados los ambientes de desarrollo y producción.
> g. Brindar el soporte requerido a los equipos principales y periféricos.
> h. Definir formalmente y efectuar rutinas de respaldo, custodiar los medios de respaldo en ambientes adecuados, controlar el acceso a dichos medios y establecer procedimientos de control para los procesos de restauración.
> i. Controlar los servicios e instalaciones externos. (p.9)

De este modo, se enmarca de manera general, el sustento para la aplicación de las medidas correctivas necesarias para que la infraestructura de un centro de cómputo, que debe estar en constante monitoreo y actualización, con lo cual se pretende que las condiciones en materia de seguridad, garanticen las operaciones, la confiablidad y confidencialidad que vengan a apoyar a la organización en la gestión de las Tecnologías de Información de manera fluida y eficiente.

En los siguientes capítulos se hará referencia específica a la normativa descrita hasta ahora y se incluirán aportes de otras organizaciones con fines de lucro que se dedican a desarrollar o normalizar la implementación de Centros de Cómputo.

Adicionalmente la estructura de los capítulos por desarrollar, está basado en la estructura de investigación del Instituto ICREA, la cual es una empresa que certifica centros de cómputo, la cual se determina que para este trabajo, es la más adecuada en el desarrollo del tema.

III. **Seguridad**

De la mano del diseño de un centro de cómputo apropiado con base en los requerimientos de la organización, se debe plantear toda una política en materia de seguridad, tanto en aspectos físicos ambientales como de control de accesos a los centros de cómputo, que permitan controlar y diagnosticar debilidades que atenten contra el acceso y menoscabo de la infraestructura y equipos que soportan la información del negocio, elemento considerado por muchos, como uno de los activos más importantes de la organizaciones.

Al respecto la norma de seguridad IRAM ISO/IEC 17799:2002 (2002) define la seguridad de la siguiente manera:

> La seguridad de la información se define aquí como la preservación de las siguientes características:
> a) confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a ella.
> b) integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
> c) disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con ella toda vez que se requiera. (p.9)

Esto por cuanto las organizaciones se enfrentan a diversas amenazas, según ISO/IEC 17799:2002 (2002):

> Relativas a la seguridad, de diversos orígenes, incluyendo el fraude asistido por computadora, espionaje, sabotaje, vandalismo, incendio o inundación. Daños tales como los ataques mediante virus informáticos,

> *hacking* y denegación de servicio se han vuelto más comunes, ambiciosos y crecientemente sofisticados. (p.9)

En primera instancia se deben establecer los requerimientos de seguridad en la organización mediante la evaluación de tres recursos principales, según IRAM ISO/IEC 17799:2002 (2002):

> - El primer paso consiste en evaluar los riesgos que enfrenta la organización. Mediante la evaluación de riesgos se identifican las amenazas a los activos, se evalúan las vulnerabilidades y probabilidades de ocurrencia, y se estima el impacto potencial.
> - El segundo recurso está constituido por los requisitos legales, normativos, reglamentarios y contractuales que deben cumplir la organización, sus socios comerciales, los contratistas y los prestadores de servicios.
> - El tercer recurso es el conjunto específico de principios, objetivos y requisitos para el procesamiento de la información, que ha desarrollado la organización para respaldar sus operaciones.(p.10)

Las instalaciones de procesamiento de información crítica o sensible de la empresa deben estar ubicadas en áreas protegidas y resguardadas por un perímetro de seguridad definido, con vallas de seguridad y controles de acceso apropiados. Deben estar físicamente protegidas contra accesos no autorizados, daños e intrusiones. (IRAM ISO/IEC 17799:2002, 2002)

Por otro lado, se deben considerar e implementar los siguientes lineamientos y controles, según corresponda según, (IRAM ISO/IEC 17799:2002, 2002):

- El perímetro de seguridad debe estar claramente definido.
- El perímetro de un edificio o área que contenga instalaciones de procesamiento de información debe ser físicamente sólido (por ejemplo, no deben existir claros [o aberturas] en el perímetro o áreas donde pueda producirse fácilmente una irrupción). Las paredes externas del área deben ser de construcción sólida y todas las puertas que comunican con el exterior deben ser adecuadamente protegidas contra accesos no autorizados, por ejemplo, mediante mecanismos de control, vallas, alarmas, cerraduras u otros.
- Debe existir un área de recepción atendida por personal u otros medios de control de acceso físico al área o edificio. El acceso a las distintas áreas y edificios debe estar restringido exclusivamente al personal autorizado.

- Las barreras físicas deben, si es necesario, extenderse desde el piso (real) hasta el techo (real), a fin de impedir el ingreso no autorizado y la contaminación ambiental, por ejemplo, la ocasionada por incendio e inundación.
- Todas las puertas de incendio de un perímetro de seguridad deben tener alarma y cerrarse automáticamente.(p.27)

Una base de la estructura de los aspectos en materia de seguridad de ambiental, según el Comité de Informática del Colegio de Postgrados de México. (2000) es la que considera aspectos tales como:

> ***Seguridad de las instalaciones***
>
> La seguridad del centro y de los laboratorios de cómputo, está basada en el control de todos los puntos de entrada y salida no solo del propio laboratorio o centro de cómputo, sino de las instalaciones en donde se ubican, por lo que deben estar siempre debidamente controlados para evitar el acceso de personas no autorizadas o en caso de una eventualidad facilitar la evacuación del personal.
>
> El área donde se guarda el software, respaldos, papelería u otros, se consideran como áreas de acceso restringido y preferentemente se controlaran por un sistema automático de control de acceso.

Por tanto las organizaciones deben utilizar perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información. Según IRAM ISO/IEC 17799:2002, (2002):

> Un perímetro de seguridad es algo delimitado por una barrera, por ejemplo, una pared, una puerta de acceso controlado por tarjeta o un escritorio u oficina de recepción atendidos por personas. El emplazamiento y la fortaleza de cada barrera dependerán de los resultados de una evaluación de riesgos. (p.27)

En cuanto al control de acceso según el Comité de Informática del Colegio de Postgrados de México. (2000):

> ***Control de acceso a las instalaciones***
>
> El personal del laboratorio y/o del centro de cómputo es responsable del control y acceso de proveedores, contratistas, personal de servicio y visitantes, así como de los recursos (equipo de cómputo, suministros, documentos, medios de cómputo y demás.) que entren o salgan. Los empleados tienen la autoridad de ejercer los procedimientos de seguridad y control de acceso al centro y/o laboratorio en cualquier momento durante su turno.
>
> ***Control de acceso del personal***
>
> El personal del centro de cómputo y/o del laboratorio debe cumplir con el horario de trabajo que se le ha indicado y no se le permitirá el acceso fuera de las horas que labora, los empleados deberán llegar a tiempo al iniciar su turno. El empleado registrará en su tarjeta de control la hora de entrada, así como la de salida. Con este procedimiento se llevara un mejor control de los empleados que se encuentran en el centro y/o laboratorio.

Al respecto la norma IRAM ISO/IEC 17799:2002, (2002), establece que:

> Las áreas protegidas deben ser resguardadas por adecuados controles de acceso que permitan garantizar que sólo se permite el acceso de personal autorizado. Deben tenerse en cuenta los siguientes controles:
>
> - Los visitantes de áreas protegidas deben ser supervisados o inspeccionados y la fecha y horario de su ingreso y egreso deben ser registrados. Sólo se debe permitir el acceso a los mismos con propósitos específicos y autorizados, instruyéndose en dicho momento al visitante sobre los requerimientos de seguridad del área y los procedimientos de emergencia.
> - El acceso a la información sensible, y a las instalaciones de procesamiento de información, debe ser controlado y limitado exclusivamente a las personas autorizadas. Se deben utilizar controles de autenticación, por ejemplo, tarjeta y número de identificación personal (PIN), para autorizar y validar todos los accesos. Debe mantenerse una pista protegida que permita auditar todos los accesos.

- Se debe requerir que todo el personal exhiba alguna forma de identificación visible y se lo debe alentar a cuestionar la presencia de desconocidos no acompañados y a cualquier persona que no exhiba una identificación visible.(p.27)

La seguridad física, la cual, según Comité de Informática del Colegio de Postgrados de México. (2000), pretende prevenir riesgos de accidentes del personal del laboratorio y/o del centro de cómputo y prevenir daños al equipo e instalaciones y adicionalmente es responsabilidad de todos los miembros de la organización.

Se debe limitar e implementar controles adicionales sobre personal que tenga contacto sobre áreas protegidas, como lo son los centros de cómputo, según la norma IRAM ISO/IEC 17799:2002, (2002):

- El personal sólo debe tener conocimiento de la existencia de un área protegida, o de las actividades que se llevan a cabo dentro de la misma, según el criterio de necesidad de conocer.
- Se debe evitar el trabajo no controlado en las áreas protegidas tanto por razones de seguridad como para evitar la posibilidad de que se lleven a cabo actividades maliciosas.
- Las áreas protegidas desocupadas deben ser físicamente bloqueadas y periódicamente inspeccionadas.
- El personal del servicio de soporte externo debe tener acceso limitado a las áreas protegidas o a las instalaciones de procesamiento de información sensible. Este acceso debe ser otorgado solamente cuando sea necesario y debe ser autorizado y monitoreado. Pueden requerirse barreras y perímetros adicionales para controlar el acceso físico entre áreas con diferentes requerimientos de seguridad, y que están ubicadas dentro del mismo perímetro de seguridad.
- A menos que se autorice expresamente, no debe permitirse el ingreso de equipos fotográficos, de vídeo, audio u otro tipo de equipamiento que registre información.(p.29)

Algunas medidas adoptadas por el Colegio de Posgrados de México (2000) son:

Pisos. Las superficies destinadas al tránsito de empleados y al manejo de paquetes de documentación y equipo deben ser suficientemente llanas para circular con seguridad.

En los pisos de las aéreas de trabajo del centro o laboratorio de cómputo debe evitarse el almacenamiento de líquidos, para evitar derrames.

Las aéreas de los pisos destinados al tránsito, manejo de paquetes y equipo, deben ser exclusivas para el uso a que se destinen, se delimitaran mediante marcas, avisos o señalamientos, de ser posible, con franjas de color amarillo; cuando estas áreas sean utilizadas simultáneamente para el tránsito de empleados, se debe destinar una zona específicamente para tal efecto.

Seguridad de iluminación. Se aseguraran que haya iluminación adecuada para prevenir esfuerzo innecesario de la vista de los empleados, que haya iluminación exterior adecuada para prevenir vandalismo y asaltos y que provea iluminación de emergencia para cada cuarto ocupado luego de la puesta del sol.

Se aseguraran que todo el equipo de iluminación de emergencia se cheque periódicamente.

La ups (nobreak o fuente de energía ininterrumpible) este ventilado apropiadamente, sin materiales u objetos que lo obstruyan.

En los lugares o locales de trabajo en los que existen condiciones térmicas ambientales elevadas, los vocales y/o coordinador deben disponer de las medidas preventivas para proteger a los trabajadores de dichas condiciones y mantener estas dentro de los límites de exposición procurando un mantenimiento efectivo y constante al aire acondicionado.

Equipo de seguridad. Se debe asegurar que se instalen protecciones en las aspas de los abanicos de ventilación, que se instalen seguros en las mesas de trabajo, 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.

La ubicación de los centros de cómputo debe obedecer a un análisis de los riesgos asociados a vulnerabilidad en acceso de terceros y exposición a factores ambientales, según la norma IRAM ISO/IEC 17799:2002, (2002):

Para la selección y el diseño de un área protegida debe tenerse en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre. También deben tomarse en cuenta las disposiciones y normas en

materia de sanidad y seguridad. Asimismo, se deberán considerar las amenazas a la seguridad que representan los edificios y zonas aledañas, por ejemplo, filtración de agua desde otras áreas. (p.28)

Para el cumplimiento de tales efectos, se deben considerar los siguientes controles, según la norma IRAM ISO/IEC 17799:2002, (2002):

- Las instalaciones clave deben ubicarse en lugares a los cuales no pueda acceder el público.
- Los edificios deben ser discretos y ofrecer un señalamiento mínimo de su propósito, sin signos obvios, exteriores o interiores, que identifiquen la presencia de actividades de procesamiento de información.
- Las funciones y el equipamiento de soporte, por ejemplo, fotocopiadoras, máquinas de fax, deben estar ubicados adecuadamente dentro del área protegida para evitar solicitudes de acceso, el cual podría comprometer la información.
- Las puertas y ventanas deben estar bloqueadas cuando no hay vigilancia **y** debe considerarse la posibilidad de agregar protección externa a las ventanas, en particular las que se encuentran al nivel del suelo.
- Se deben implementar adecuados sistemas de detección de intrusos. Los mismos deben ser instalados según estándares profesionales y probados periódicamente. Estos sistemas comprenderán todas las puertas exteriores y ventanas accesibles. Las áreas vacías deben tener alarmas activadas en todo momento. También deben protegerse otras áreas, como la sala de cómputos o las salas de comunicaciones.
- Las instalaciones de procesamiento de información administradas por la organización deben estar físicamente separadas de aquellas administradas por terceros.
- Las guías telefónicos y listados de teléfonos internos que identifican las ubicaciones de las instalaciones de procesamiento de información sensible no deben ser fácilmente accesibles al público.
- Los materiales peligrosos o combustibles deben ser almacenados en lugares seguros a una distancia prudencial del área protegida. Los suministros a granel, como los útiles de escritorio, no deben ser almacenados en el área protegida hasta que sean requeridos.
- El equipamiento de sistemas de soporte UPC (usage parameter control) de reposición de información pérdida ("fallback") y los medios informáticos de resguardo deben estar situados a una distancia prudencial para evitar daños ocasionados por eventuales desastres en el sitio principal.(p.28)

Las áreas de entrega y carga deben ser controladas y, si es posible, estar aisladas de las instalaciones de procesamiento de información, a fin de impedir accesos no autorizados. Los requerimientos de seguridad de dichas áreas deben ser determinados mediante una evaluación de riesgos.

Se deben tener en cuenta los siguientes lineamientos, según la norma IRAM ISO/IEC 17799:2002, (2002):

- El acceso a las áreas de depósito, desde el exterior de la sede de la organización, debe estar limitado a personal que sea previamente identificado y autorizado.
- El área de depósito debe ser diseñada de manera tal que los suministros puedan ser descargados sin que el personal que realiza la entrega acceda a otros sectores del edificio.
- Todas las puertas exteriores de un área de depósito deben ser aseguradas cuando se abre la puerta interna.
- El material entrante debe ser inspeccionado para descartar peligros potenciales antes de ser trasladado desde el área de depósito hasta el lugar de uso.
- El material entrante debe ser registrado, si corresponde, al ingresar al sitio pertinente.(p.29)

Se deben adoptar medidas de seguridad para prevenir daños en los equipos que están ubicados en las aéreas protegidas en los centros de compto. Los requerimientos de seguridad de dichas áreas deben ser determinados mediante una evaluación de riesgos. Se deben tener en cuenta los siguientes lineamientos según la norma IRAM ISO/IEC 17799:2002(2002):

El equipamiento debe ser ubicado o protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y oportunidades de acceso no autorizado. Se deben tener en cuenta los siguientes puntos:

- El equipamiento debe ser ubicado en un sitio que permita minimizar el acceso innecesario a las áreas de trabajo.
- Las instalaciones de procesamiento y almacenamiento de información, que manejan datos sensibles, deben ubicarse en un sitio que permita reducir el riesgo de falta de supervisión de las mismas durante su uso.

- Los ítems que requieren protección especial deben ser aislados para reducir el nivel general de protección requerida.
- Se deben adoptar controles para minimizar el riesgo de amenazas potenciales, por ejemplo: robo, incendio, explosivos, humo, agua (o falta de suministro), polvo, vibraciones, efectos químicos, interferencia en el suministro de energía eléctrica, radiación electromagnética.
- La organización debe analizar su política respecto de comer, beber y fumar cerca de las instalaciones de procesamiento de información,
- Se deben monitorear las condiciones ambientales para verificar que las mismas no afecten de manera adversa el funcionamiento de las instalaciones de procesamiento de la información.
- Se debe tener en cuenta el uso de métodos de protección especial, como las cubiertas de teclado, para los equipos ubicados en ambientes industriales.
- Se debe considerar el impacto de un eventual desastre que tenga lugar en zonas próximas a la sede de la organización, por ejemplo, un incendio en un edificio cercano, la filtración de agua desde el cielo raso o en pisos por debajo del nivel del suelo o una explosión en la calle.(pag.30)

Los trabajos que se deben realizar en los centros de cómputo, deben ser controlados y supervisados, con el fin que no interfieran o dañen equipos que provoquen que la pérdida de información o amenacen la continuidad de las operaciones normales. Según la norma la norma IRAM ISO/IEC 17799:2002(2002):

- El personal sólo debe tener conocimiento de la existencia de un área protegida, o de las actividades que se llevan a cabo dentro de la misma, según el criterio de necesidad de conocer.
- Se debe evitar el trabajo no controlado en las áreas protegidas tanto por razones de seguridad como para evitar la posibilidad de que se lleven a cabo actividades maliciosas.
- Las áreas protegidas desocupadas deben ser físicamente bloqueadas y periódicamente inspeccionadas.
- El personal del servicio de soporte externo debe tener acceso limitado a las áreas protegidas o a las instalaciones de procesamiento de información sensible. Este acceso debe ser otorgado solamente cuando sea necesario y debe ser autorizado y monitoreado. Pueden requerirse

barreras y perímetros adicionales para controlar el acceso físico entre áreas con diferentes requerimientos de seguridad, y que están ubicadas dentro del mismo perímetro de seguridad.

- A menos que se autorice expresamente, no debe permitirse el ingreso de equipos fotográficos, de vídeo, audio u otro tipo de equipamiento que registre información.(p.29)

Los equipos deben estar protegidos con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. Se debe contar con un adecuado suministro de energía que esté de acuerdo con las especificaciones del fabricante o proveedor de los equipos.

Entre las alternativas para asegurar la continuidad del suministro según la norma IRAM ISO/IEC 17799:2002(2002):

- Se recomienda una UPS para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas de la organización. Los planes de contingencia deben contemplar las acciones que han de emprenderse ante una falla de la UPS. Los equipos de UPS deben inspeccionarse periódicamente para asegurar que tienen la capacidad requerida y se deben probar de conformidad con las recomendaciones del fabricante o proveedor.
- Se debe tener en cuenta el empleo de un generador de respaldo si el procesamiento ha de continuar en caso de una falla prolongada en el suministro de energía. De instalarse, los generadores deben ser probados periódicamente de acuerdo con las instrucciones del fabricante o proveedor. Se debe disponer de un adecuado suministro de combustible para garantizar que el generador pueda funcionar por un período prolongado.
- Asimismo, los interruptores de emergencia deben ubicarse cerca de las salidas de emergencia de las salas donde se encuentra el equipamiento, a fin de facilitar un corte rápido de la energía en caso de producirse una situación crítica. Se debe proveer de iluminación de emergencia en caso de producirse una falla en el suministro principal de energía. Se debe implementar protección contra rayos en todos los edificios y se deben adaptar filtros de protección contra rayos en todas las líneas de comunicaciones externas.(p.31)

Los cableados eléctricos y de transmisión de datos debe estar protegidos contra daños exposición al medio que podían provocar intercepciones maliciosas o accidentales, según la norma IRAM ISO/IEC 17799:2002(2002):

- Las líneas de energía eléctrica y telecomunicaciones que se conectan con las instalaciones de procesamiento de información deben ser subterráneas, siempre que sea posible, o sujetas a una adecuada protección alternativa.
- El cableado de red debe estar protegido contra interceptación no autorizada o daño, por ejemplo, mediante el uso de conductos o evitando trayectos que atraviesen áreas públicas.
- Los cables de energía deben estar separados de los cables de comunicaciones para evitar interferencias.
- Entre los controles adicionales a considerar para los sistemas sensibles o críticos se encuentran los siguientes:
    - instalación de conductos blindados y recintos o cajas con cerradura en los puntos terminales y de inspección.
    - uso de rutas o medios de transmisión alternativos
    - uso de cableado de fibra óptica
    - iniciar barridos para eliminar dispositivos no autorizados conectados a los cables.(p.31)

De manera ilustrativa, algunas medidas adoptadas por el Colegio de Posgrados de México (2000) son:

> ***Seguridad sobre energía eléctrica.*** Se debe asegurar 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 empleados; se asegurara que todos los circuitos estén conectados a una tierra común; y de que haya suficientes circuitos y estén instaladas distribuidamente 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 o laboratorio de cómputo y de las salidas del edificio.(p.21)

Los aspectos de seguridad analizados hasta anteriormente, aplican también para los equipos destinados al procesamiento de la información cuyo utilización externa debe estar normada por la organización y debidamente autorizado su uso y gestión.

Según la norma IRAM ISO/IEC 17799:2002(2002):

> El uso de los equipos destinado al procesamiento de información, fuera del ámbito de la organización, debe ser autorizado por el nivel gerencial, sin importar quién es el propietario del mismo. La seguridad provista debe ser equivalente a la suministrada dentro del ámbito de la organización, para un propósito similar, teniendo en cuenta los riesgos de trabajar fuera de la misma. El equipamiento de procesamiento de la información incluye todo tipo de computadoras personales, organizadores, teléfonos móviles, papel u otros formularios, necesarios para el trabajo en el domiciliario o que es transportado fuera del lugar habitual de trabajo. Una adecuada cobertura de seguro debe estar en orden para proteger el equipamiento fuera del ámbito de la organización.

Cuando por alguna razón especial, se requiera retirar equipo de las áreas protegidas es importante considerar, según la norma IRAM ISO/IEC 17799:2002(2002) que: "El equipamiento, la información o el software no deben ser retirados de la sede de la organización sin autorización." Se deben llevar a cabo comprobaciones puntuales para detectar el retiro no autorizado de activos de la organización y el personal debe conocer la posibilidad de realización de dichas comprobaciones".

De esta manera se recopila la información mas relevante con respecto a la seguridad física con respecto a la normativa mas adoptada para cubrir aspectos de seguridad, y sobre la cual se harán las recomendaciones y conclusiones.

Los siguientes capítulos pretenden reforzar algunos conceptos destacados por la normativa de la seguridad para ampliar la aplicación de controles que facilítenla gestión de la seguridad física en áreas protegidas de Ti, común lo es un centro de cómputo.

IV. **Infraestructura**

Los aspectos de seguridad física tales que permitan reforzar dichos normativa contemplada en la normativa abarcada en el capitulo anterior.

Piso elevado y cámara plena: en la actualidad la tecnología de vanguardia tiende a no utilizar pisos falsos ya que se ha demostrado a través del tiempo que el rendimiento y el aprovechamiento del aire frio generado por los equipos especializados de aire acondicionado.

Según la compañía Editel (2008) en su página Web, establece las características de acuerdo a normas internacionales

- Resistencia Eléctrica.- No menos de 5 x 105 ohms y no más de 2 x 1010 ohms (norma NFPA99), medida desde la cubierta de la placa a un pedestal de la estructura. Esta especificación es para plástico laminado, incluyendo el empaque de tierra. Variará con otros materiales y acabados.
- El piso está construido con la capacidad de Disipación Estática, ofreciendo un efectivo contacto para descargas estáticas que son críticas en áreas en donde se tiene equipo electrónico altamente sensible.
- Resistencia al Fuego.- De acuerdo a normas ASTM, E85-61 y NFPA 255 con factor "0" de aportación de combustible, obtienen una clasificación de "20". Estas normas son de aceptación internacional para pisos elevados en cualquier aplicación.
- Propiedades Térmicas.- Excelente comportamiento cuando se usa como cámara plena para aire acondicionado sin que se transmita el frío a la superficie del piso y sin que cambie de dimensiones. Esto permite un ajuste permanente y exacto de las placas, un ambiente muy confortable para quienes trabajan en el área cubierta por piso elevado, evitando así las molestias y enfermedades ortopédicas provocadas por el piso elevado totalmente metálico o con cemento.
- Propiedades Acústicas.- Dada su construcción, el piso amortigua los ruidos del lugar de trabajo, como los emitidos por impresoras electromecánicas de alta velocidad (hasta 90 dcb), pisadas, ruido exterior u otras más.

Ubicación del Centro de Cómputo y materiales de construcción.

En la construcción de un edificio para instalar un sistema informático, lo primero que se debe elegir es su emplazamiento. La elección del emplazamiento, aparte de las consideraciones de tipo estratégico o de tipo económico para la entidad, precisa ser seguro frente a los riesgos de naturaleza física.

Tanto el centro de cómputo como las áreas y recintos aledaños, deben estar construidas con materiales no inflamables y de retardo en la propagación del

fuego no menor a una hora, según la Norma NFPA 75 (2003). Esto incluye pisos, techos y paredes.

Toda área que contenga equipo de cómputo debe poseer un sistema extintor de incendio de acuerdo a la norma de NFPA 13 y no debe ser emplazado sobre debajo ni contiguo a otros recintos que no cuenten con la medidas de seguridad anteriormente citadas.

Según Instituto Nacional de Estadística e Informática de Perú (1997):

- Es recomendable que el Centro de Cómputo no esté ubicado en las áreas de alto tráfico de personas o con un alto número de invitados.
- 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 terrorismo y sabotaje.
- 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.

Complementando los requerimientos en la ubicación del los centros de cómputo se deben garantizar los siguientes aspectos, según el Instituto Tecnológico de Sonora (1997):
Cercanía de usuario.

- Cercanía de configuración de respaldo.
- Corriente eléctrica confiable.
- Comunicación confiable.
- Vía rápida de acceso.
- Evitar zonas con incidencia de desastres naturales.
- Evitar zonas propensas a disturbios sociales.
- Cercanía de Policía y Bomberos.
- Rentas atractivas.
- Sistema escolar y servicios comunitarios.

- Elevado.
- Minimizar el efecto de lluvias.
- Evitar la proximidad de aeropuertos.
- Evitar Interferencia electromagnética.
- Separación de vía rápida.
- Transporte comercial cercano Estacionamiento Espacio adecuado.
- Para planta eléctrica de respaldo para UPS.
- Para sistema de aire acondicionado.
- Puertas y pasillos amplios.
- Lejanía de inflamables y explosivos.
- Control de acceso.
- Área para visitas.
- Área de comida y Sanitarios.
- No más allá de un sexto piso.

V. **Comunicaciones**

En este aspecto se la norma que se debe adoptar es la TIA – 942 de Telecomminication Industry Association. La misma establece aspectos mínimos en materia de diseño e implementación de cableado para cetros de cómputo.

Si bien en propósito es proponer e valuar aspectos de seguridad física en materia de centros de cómputo, al utilizar y observar buenas prácticas en materia de seguridad de cableado establecen controles que permiten adoptar medidas de protección de los datos que son transmitidos por la redes de cómputo.

Los elementos básicos de una red de cableado para centro de datos, según El Comité de Normalización de Petróleos Mexicanos. (2007), son:

- Cableado Horizontal.
- Cableado Principal.

- Distribuidor de cableado en el cuarto de entrada o área de distribución principal
- Distribuidor Principal (DP) en el área de distribución principal.
- Distribuidor Horizontal (DH) en el cuarto de telecomunicaciones, área de distribución horizontal o área
- de distribución principal.
- Zona de salida o punto de consolidación en el área de distribución de zona.
- Salida en el área de distribución de equipo.(p.157)

En los centros de datos deben existir espacios dedicados para la instalación de equipos y cableados de telecomunicaciones, según El Comité de Normalización de Petróleos Mexicanos. (2007),

> Los espacios típicos dentro de un centro de datos, generalmente incluyen el cuarto de entrada (CENT), el área de distribución principal (ADP), área de distribución horizontal (ADH), área de distribución de zona (ADZ) y área de distribución de equipo (ADE). La cantidad y tipo de espacios en un centro de datos dependerá primordialmente del tamaño de éste. Estos espacios se deben planear para permitir el crecimiento y la transición a las tecnologías emergentes. Estos espacios pueden o no estar separados de los espacios para equipo de cómputo, a través de paredes u otro elemento de separación.(p.158)

Los cuartos de comunicaciones principales que se deben distribuir adecuadamente referentes al centro de cómputo, según El Comité de Normalización de Petróleos Mexicanos. (2007),

- **Cuarto de Telecomunicaciones;** en los centros de datos, el cuarto de telecomunicaciones (CT) es un espacio que distribuye el cableado hacia las áreas exteriores al cuarto de cómputo. El cuarto de telecomunicaciones se localiza normalmente fuera del cuarto de cómputo, pero si fuera necesario puede combinarse con el área de distribución principal o con las áreas de distribución horizontal. El centro de datos puede tener más de un cuarto de telecomunicaciones, en caso de que las áreas que serán atendidas no puedan ser soportadas por un sólo cuarto de telecomunicaciones.

- **Cuarto de Entrada:** el cuarto de entrada es el espacio utilizado para la interfaz entre la red de cableado del centro de datos y el cableado entre

edificios, tanto para el proveedor de acceso, como para el propietario del cableado. En este espacio generalmente se instala el equipo de acceso y de demarcación del proveedor de servicios. El cuarto de entrada puede estar localizado fuera del cuarto de cómputo, si el centro de datos está en un edificio que contiene oficinas de propósito general u otros tipos de espacios diferentes al centro de datos. El cuarto de entrada también puede estar fuera del cuarto de cómputo por razones de seguridad, ya que esto evitaría la necesidad de que el personal técnico del proveedor de servicio entre al cuarto de cómputo.

Los centros de datos pueden tener múltiples cuartos de entrada para proporcionar esquemas de redundancia adicional o para evitar que se excedan las longitudes máximas del cableado permitidas por los circuitos de los equipos del proveedor de servicios. El cuarto de entrada se interconecta con el cuarto de cómputo a través del área de distribución principal. El cuarto de entrada puede estar colocado en una posición adyacente o contenido en el área de distribución principal.

- **Áreas de soporte del Centro de Datos:** las áreas de soporte del centro de datos son espacios exteriores al cuarto de cómputo destinadas al alojamiento de los equipos auxiliares del centro de datos. Estas áreas de soporte pueden incluir los centros de operación, oficinas para el personal de soporte, cuartos de seguridad, cuartos eléctricos, cuartos mecánicos y cuartos de almacenamiento.

  Los cuartos eléctricos, cuartos mecánicos y cuartos de almacenamiento deben tener por lo menos una salida de telecomunicaciones para la conexión de un teléfono. Asimismo, los cuartos eléctricos y mecánicos deben tener también por lo menos una conexión a la red de datos para el acceso a sus sistemas administración.(p.163-164)

VI. **Instalación eléctrica**

Uno de los aspectos por considerar seriamente a la hora de diseñar un centro de cómputo es la carga eléctrica que debe soportar así como la prevención en materia de crecimiento que debe ser considerada.

La normativa aplicada para los aspectos de infraestructura eléctrica esta contenida principalmente por Norma IEEE 1100-1999 Recommended Practice for Powering and Grounding Electronic Equipment.

Los principales aspectos técnicos, que se deben evaluar según el Departamento de Control de Calidad y Auditoría Informática del Ministerio de Obras Públicas y transportes de Ecuador, (2000), son:

- Se cuenta con instalación con tierra física para todos los equipos
- La instalación eléctrica se realizó específicamente para el centro de cómputo
- Se cuenta con otra Instalación dentro el centro de cómputo, diferente de la que alimenta a los equipos de cómputo
- La acometida llega a un tablero de distribución
- El tablero de distribución está en la sala, visible y accesible
- El tablero considera espacio para futuras ampliaciones de hasta de un 30 % (Considerando que se dispone de espacio físico para la instalación de más equipos)

  La Instalación es independiente para el centro de cómputo. La misma instalación con tierra física se ocupa en otras partes del Edificio.

- La iluminación está alimentada de la misma acometida que los equipos
- Las reactancias (balastros de las lámparas) están ubicadas dentro de la sala.
- Los ventiladores y aire acondicionado están conectados en la misma instalación de los equipos a la planta de emergencia.
- Los ventiladores y aire acondicionado están conectados en la misma instalación de los equipos cómputo.
- Se cuenta con interruptores generales.
- Se cuenta con interruptores de emergencia en serie al interruptor general.
- Se cuenta con interruptores por secciones o aulas.
- Se tienen los interruptores rotulados adecuadamente.
- Se tienen protecciones contra corto circuito.
- Se tiene implementado algún tipo de equipo de energía auxiliar.
- Se cuenta con Planta de emergencia.
- Se tienen conectadas algunas lámparas del centro de cómputo a la planta de emergencia.
- Qué porcentaje de lámparas: % están conectadas a la planta de emergencia (recomendable el 25 %).
- Voltaje de Salida regulado.
- Tensión nominal especificada en los equipos: Volts.
- Potencia consumida por los equipos: Watts.
- Tolerancia máxima en tensión de 10% sobre tensión nominal.

- Tolerancia mínima en tensión de 8% sobre tensión nominal.
  Tolerancia máxima en frecuencia de 1/2 Hz. Variación de voltaje entre fases máxima de 2.5% de la media aritmética de las tres fases. Contenido de armónicas máximo inferior al 5% con equipo desconectado.
- La Sección de los conductores eléctricos están calculados sobre la potencia consumida por el equipo de cómputo más el 75% adicional de margen de seguridad.
- El tablero de distribución cuenta con un interruptor principal, voltímetro de tres fases, indicadores luminosos e interruptores termos magnéticos para cada uno de los circuitos derivados.
- Los circuitos derivados terminan abajo del piso falso en una caja de conexiones cerca de la máquina que va a alimentar.
- Las cajas de conexiones bajo el piso falso están ancladas y aisladas o
- plastificadas exteriormente.
- Se cuenta con toma de tierra física independiente, con resistencia total de 3 Ohms, que incluye conductor más electrodo.

VII. **Aire Acondicionado**

El tipo de equipos de aire acondicionado que se utilizan en los centros de cómputo, juegan un papel fundamental en la prolongación de la vida útil de los equipos ya que permiten un adecuado regulación de la temperatura, la cual debe ser recibida a 21 ± 1℃ por los equipos, para evitar sobrecalentamientos que provoquen caídas y acorten la vida útil de los equipos, ya que los computadores como equipos eléctrico, es una fuente generadora de energía calórica por definición.

Los estándares establecen que los equipos de enfriamiento deben ser de tipo de denominado de precisión ya adicionalmente deben regular el control de humedad relativa de 50% ± 5%, otro aspecto fundamental en a la conservación de los equipos, y que haya en el recinto un flujo de aire 15 ft3/min por persona en ocupación constante.

La tendencial actual es utilizar sistemas modulares para inyectar el aire acondicionado a los equipos bajo la filosofía de pasillos calientes y pasillos fríos en combinación con idea en la utilización de pisos falsos que han resultado ser menos eficientes, ya que crean puntos de aire caliente que desperdicia el aire enfriado que es inyectado al los pisos.

En su lugar se utiliza la tecnología de dos tipos desarrollados `por la compañía APC Legendary Reability:

Uno se basa en colocar los bastidores de los computadores con racks de aires acondicionados mediante la técnica de pasillos fríos y calientes de manera que el aire frio es empujado hacia delante y lo vuelve a tomar de atrás para completar el ciclo. Este método es mucho más eficiente que el de piso falso ya que el aire frío fluye a lo largo de los bastidores y no desde debajo como con lo hace el método de piso falso.

La otra combinación se basa en encapsular lo parte de atrás de los bastidores espalda con espalda, para evitar que el aire caliente se escape a otros punto del cuarto de cómputo y el aire frio se distribuye directamente a la parte de absorción de los equipos. Este método es el más eficiente en la actualidad.

VIII. **Conclusiones y Recomendaciones**

A través de este estudio, se ha podido dimensionar la labor tan intrincada que resulta la conformación de un centro de cómputo o sala de computadores, o *data center*, como se le quiere llamar, debido a que el desarrollo adecuado de esta labor, implica la participación de un grupo interdisciplinario en materia de aspectos eléctricos, infraestructura, comunicaciones, entre otros.

La normativa a aplicar para la conformación de un centro de cómputo, es basta y variada, lo cual hace complejo la aplicación de la misma para la construcción de un centro de cómputo. En este sentido, sólo para la aplicación de la normativa en materia de seguridad física, se requiere la participación de un equipo de trabajo, que lidere un proyecto de aplicación de la normativa.

Algunas de las normativas que se pudo determinar aplicable en materia de seguridad e implementación de centros de cómputo son:

- NFPA 99 y ANSI/ESD Normas de resistencia eléctrica y Control de estática.
- NFPA 255 y ASTM E84 Normas de resistencia al fuego.
- NFPA 75 Normas para la construcción de Cuartos de Proceso de Datos.
- ISO 27001 y IRAM ISO/IEC 17799:2002 en seguridad.
- TIA-942 en comunicaciones

La complejidad de la conformación y gestión de un centro de cómputo, es proporcional a la diversidad y cantidad de equipamiento que pretende hospedar, de ahí la importancia de establecer políticas en materia de TI, que estandaricen las plataformas en las que van a soportar las aplicaciones de la organización. Claro, la planificación empieza desde la definición clara de políticas, por parte de la organización, de cómo quiere que la TI apoyen su gestión

Existe a nivel internacional una conciencia por parte de los gobiernos de la necesidad de controlar la gestión de la TI, por lo que cada uno ha realizado esfuerzos en para de adoptar y adaptar normativa internacional que aplique a su realidad nacional; Costa Rica no es la excepción y de ahí que la Contraloría General de la República, ha actualizado el Manual de Normas Técnicas de TI, que abarcan controles y disposiciones mínimas que garanticen que una

organización logre gestionar sus TI, de manera eficiente, lo que incluye la infraestructura.

Para una institución, como la analizada en este trabajo, dada la complejidad de sistemas que contiene, lo primero que se debe hacer es homogenizar las plataformas en las que han sido desarrollado sus sistemas, esto con la finalidad de disminuir la complejidad de la implementación de medidas de seguridad física, lo cual podría permitir encapsular con en bastidores los servidores, cuya administración de acceso es más puntual.

Por otro lado, este tipo de tecnología permitiría adoptar sistemas de enfriamiento y de redundancia eléctrica de vanguardia, reduciendo los costos por metro cuadrado ya que se aprovecha el espacio de forma horizontal y al distribuirse mejor el suministro de aire se incrementa la vida útil de los equipos y elimina la utilización de piso falso, cuyo deterioro es más acelerado y no aprovecha adecuadamente la distribución del suministro de aire.

El emplazamiento del centro de cómputo, es un punto muy complejo para el caso en estudio, ya que se debe adaptar al edificio que actualmente lo hospeda. En todo caso, debería alejarse de los ventanales ya que está expuesto a la radiación solar, lo cual eleva la temperatura del recinto y también atenta contra la seguridad, ya que es un foco de acceso a la información y equipos.

A este respecto, debería reubicarse como máximo en el sexto piso, esto por facilitar el acceso en caso de emergencia y evacuaciones, alejado de las paredes exteriores del edificio para evitar que se vea afectado por la radiación solar. Todo los recintos aledaños deben estar constituidos al igual que el centro de cómputo, por materiales que retarden la acción del fuego por al menos una hora.

Por otro lado, se debe adoptar controles de acceso como puertas con magnetos, para restringir y registrar apropiadamente los ingresos al centro de cómputo, lo cual elimina el acceso a llaves que podrían duplicarse o perderse. Se garantiza que sólo ingrese el personal debidamente autorizado.

Otra medida inmediata que se debe adoptar, es un procedimiento o política que restrinja el acceso al centro de cómputo de manera que sólo se ingrese si es estrictamente necesario, y autorizado por sus superiores; con el propósito de que se registre qué hace cada funcionario en el centro de cómputo y se limite la cantidad de personas, para que no alteren el ambiente.

Se podrían mencionar y analizar otros aspectos en materia de seguridad, pero se convertiría en un manual técnico, lo cual no es el propósito del documento.

La recomendación más importante, es que se debe adoptar una política de seguridad integral que involucre otras áreas de la organización, para que visualicen la seguridad del centro de cómputo, como un todo en materia de seguridad de la información, y que las políticas que se vayan a aplicar, obedezcan a una clara conciencia de la importancia de mantener la confidencialidad e integridad de la información, que en la actualidad se ha convertido en uno de los activos más importantes de las organizaciones.

IX. **Bibliografía y Referencias**

Colegio de Postgrados de Mexico. Comité de Informática.(2000). Seguridad Física y Ambientación de los Laboratorios y Centros de Cómputo. Referenciado el 31 de Marzo de 2008. http://www.colpos.mx/cominf/mmsegurid.htm

Comité de Normalización de Petróleos Mexicanos y Organismos Subsidiarios. (2007). Redes de Cableado Estructurado de Telecomunicaciones para Edificios Administrativos y Areas Industriales. Referenciado el 6 de abril de 2008, de http://www.pemex.com/files/content/PROY-NRF-022-PEMEX-2007.pdf

Contraloría General de la República (2007). Manual de Normas Técnicas para la Gestión y Control de TI. San José.

Corletti Estrada, Alejandro (2006). ISO-27001: Los Controles Partel. Tomado el 30 de Marzo de 2008. http://www.belt.es/expertos/HOME2_index2.asp?id=821

Departamento de Control de Calidad y Auditoría Informática del Ministerio de Obras Publica y Transportes (2000). Guía para pruebas en Áreas de Cómputo. Referenciado el 30 de Marzo de 2008. http://www.mtop.gov.ec/uploads/archivos/centro%20de%20cómputo.pdf

Editel (2008). Catalogo de Piso falso. Referenciado el 6 de Abril de 2008. http://www.editel.com.mx/pages/PagsProductos/pisoFalso.html

Instituto Argentino de Normalización (2002). IRAM-ISO/IEC 17799:2002. Argentina: Documento Digital.

IT Governance Institute (2006). Cobit 4.0. EE.UU

INTERNATIONAL COMPUTER ROOM EXPERTS ASSOCIATION A.C (2008). Referenciado el 25 de febrero de 2008. http://www.icrea-international.com/internationalWeb/mx/index.html

Instituto Nacional de Estadística e Informática de Perú (1997). Plan de contingencias y seguridad de la información. Referenciado el 6 de Abril de 2008. http://www.inei.gob.pe/biblioineipub/bancopub/inf/lib5007/0300.HTM

Instituto Tecnológico de Sonora (2008). Administración de Recursos de Cómputo. Referenciado el 6 de Abril de 2008, de http://www.itson.mx/dii/jgaxiola/admon_tecnologia/capitulo2.html

National Fire Protection Association. (2003). Norma NFPA 75. Referenciado el 6 de Abril de 2008. http://www.nfpa.org/freecodes/free_access_document.asp

Wikipedia, La Enciclopedia Libre (2008). Concepto de ITIL. Tomado el 30 de marzo de 2008. http://es.wikipedia.org/wiki/ITIL