Segundo trabajo de investigación:

Introducción norma TIA 942.

Introducción norma ISO 27001 y 27002.

Introducción norma ISO 20000.

Estudiante: Ariel Pérez Lobo.

Universidad Central.

Profesor: Roberto Quesada Vargas.

Curso: Administración de centros de cómputo.

I cuatrimestre 2021.

Tabla de contenido

1. Introducción.

En la actualidad las empresas consideran a la información como el activo más importante, es un recurso vital que puede significar el éxito o el fracaso de una organización; resguardar los datos de una institución se ha convertido en una labor muy importante. Los dispositivos o equipos digitales son los medios más usados para almacenar la información, por lo tanto, la tecnología se ha convertido en un aliado muy importante de las organizaciones.

Es así, que las organizaciones tienen la responsabilidad de crear políticas de seguridad de la información, establecidas en normas internacionales. Estas normas han sido reconocidas como los métodos más efectivos para el control de la información, ya que permiten establecer niveles de acceso a los procesos críticos de alto nivel.

La tecnología a su vez, está sujeta a continuos cambios, la evolución de este campo es muy acelerada, la infraestructura de los lugares donde la tecnología ha sido implementada debe tener la capacidad de adaptabilidad para brindar servicios que los sistemas consumen. Estas circunstancias, han sido los ejes principales a la horade decidir el sitio donde almacenar la información, pues se toman en cuenta muchos parámetros de seguridad y se evalúan de manera minuciosa el o los Centros de Datos con los que se dispondrá para este propósito.

Se considera de vital importancia el cumplimiento de conceptos de: seguridad, disponibilidad y redundancia dentro de los Centro de Datos. Estos conceptos se fundamentan en políticas y normas para la protección de la información, mismos que contribuyen al desarrollo fundamental de la empresa u organización. Es por ese motivo que se han establecido normas a nivel internacional para manejar estándares y lograr un crecimiento organizado de los Data center centros de datos.

La infraestructura tecnológica cambia constantemente en el mundo de la tecnología, cada día surgen nuevas necesidades que llevan a las organizaciones a realizar ampliaciones y cambiar su estructura de la información.

Muchas veces, debido a la necesidad urgente de prestar servicios, las organizaciones improvisan centros de cómputo y crecen en ellos desorganizadamente, poniendo en riesgo la integridad de su información sin darse cuenta que es el activo más preciado del que disponen ya que allí se guarda la vida del negocio sus transacciones, clientes, finanzas, entre otros. Los Centros de datos o Data Centers se basan en normas y estándares internacionales para garantizar su funcionamiento y seguridad en el manejo de la información.

Las instituciones, organizaciones y empresas, poseen un gran volumen de información, y los sitios en donde se almacena esta información deben contar con los diseños apropiados para Centro de Datos con un nivel de disponibilidad aceptable, por tal motivo se usará como referencia la norma internacional establecida por Telecommunications Industry Association (TIA-942), la cual expresa requisitos de diseño y construcción para un Centro de Datos.

Esta norma contempla recomendaciones para infraestructura de obra civil, infraestructura de cableado estructurado, infraestructura del sistema eléctrico y sus servicios auxiliares, entre otros. Sin embargo, no existe un estándar o norma que complete tanto los requisitos de diseño de un Centro de Datos (norma TIA-942) y las políticas de seguridad de la información (norma International Standards Organization en sus siglas ISO).

Para este trabajo de investigación se hablará de temas como la norma TIA 942, las normas ISO 27001 y 27002, junto con la norma ISO 20000, la cual trata de administración de servicios de TI. Estas normas es muy importantes seguirlas como se debe para poder establecer una buena administración en un centro de procesamiento de datos o Data Center. Algunas de estas normas se enfocan en la infraestructura del data center y otras en la seguridad y protocolos presentes que deben de existir en un centro de procesamiento de datos.

2. Introducción a la Norma TIA 942.

En abril de 2005, la Telecomunication Industry Association publica su estándar TIA-942 con la intención de unificar criterios en el diseño de áreas de tecnología y comunicaciones. Este estándar que en sus orígenes se basa en una serie de especificaciones para comunicaciones y cableado estructurado, avanza sobre los subsistemas de infraestructura generando los lineamientos que se deben seguir para clasificar estos subsistemas en función de los distintos grados de disponibilidad que se pretende alcanzar.

La norma TIA 942 considera la estructura de un data center en su conjunto y contiene requerimientos sobre infraestructura de cableado, instalación, accesorios de montaje y la identificación de los sitios para el tendido de cables. Además se centra en el diseño de la red, características arquitectónicas de los edificios, condiciones para la energía, la iluminación, las condiciones climáticas, la seguridad contra incendios y protección contra la humedad, entre otros.

El “punto de partida” de la norma es comenzar el trabajo de diseño antes de la construcción o reconstrucción. Sólo en esta etapa podemos apreciar plenamente todas las características arquitectónicas de los locales del centro de datos y garantizar la integración de todos los sistemas técnicos. Por lo tanto, la norma debe ser un referente principalmente para los diseñadores que tienen que planificar la arquitectura, sistemas técnicos y la infraestructura de cableado para el funcionamiento de un gran número de equipos de cómputo con un diseño de alta densidad. La norma TIA EIA-942 Cubre las siguientes áreas:

- Subsistemas.
- Espacio del sitio y su disposición.
- Infraestructura del cableado.
- Tier y niveles de disponibilidad.
- Consideraciones ambientales.

2.1. Subsistemas.

La norma TIA-942 establece requisito para el diseño de Centro de Datos, considerando cuatro aspectos de los subsistemas que son aplicables para todos los niveles de tiers:

Arquitectura: El diseño de un centro de datos debe basarse en la seguridad, ubicación física, accesos y la necesidad de ajustarse a las especificaciones de la norma del centro de datos.

Sistema eléctrico: El diseño eléctrico tales como la energía, la energía de reserva y puesta a tierra; cumplirá con las normas establecidas. La cantidad de circuitos eléctricos depende de los requisitos de los equipos que se ubicarán en las salas. Las habitaciones deberán contar con sistemas de respaldo (UPS eléctricos y generadores) que son utilizados para la sala de ordenadores.

Sistema mecánico: El sistema de climatización de una instalación incluye unidades individuales o múltiples de aire acondicionado, con la capacidad de refrigeración combinado para mantener la temperatura y la humedad relativa en condiciones óptimas, ya sea por medio de agua o de un condensador de agua fría.

Telecomunicaciones: Por su naturaleza, los centros de datos consumen grandes cantidades de energía, la mayoría de los cuales se convierte en calor, lo que requiere una seria consideración la eficiencia de enfriamiento.

Telecomunicaciones	Arquitectura	Eléctrica	Mecánica
Cableado de racks	Selección del sitio	Cantidad de accesos	Sistemas de climatización
Accesos redundantes	Tipo de construcción	Puntos únicos de falla	Presión positiva
Cuarto de entrada	Protección ignífuga	Cargas críticas	Cañerías y drenajes
Área de distribución	Requerimientos NFPA 75	Redundancia de UPS	Chillers
Backbone	Barrera de vapor	Topología de UPS	CRAC´s y condensadores
Cableado horizontal	Techos y pisos	PDU's	Control de HVAC
Elementos activos redundantes	Área de oficinas	Puesta a tierra	Detección de incendio
Alimentación redundante	NOC	EPO (Emergency Power Off)	Sprinklers
Patch panels	Sala de UPS y baterías	Baterías	Extinción por agente limpio (NFPA 2001)
Patch cords	Sala de generador	Monitoreo	Detección por aspiración (ASD)
Documentación	Control de acceso	Generadores	Detección de líquidos
	CCTV	Transfer switch	

Figura 1: Componentes de los subsistemas.

2.2. Espacio del sitio y su disposición.

Tiene los siguientes componentes:

Cuarto de Entrada.

El cuarto de entrada alberga el equipo de los operadores de telefonía. Puede estar dentro del centro de datos, pero la norma recomienda que esté en un cuarto aparte por razones de seguridad.

Área de distribución principal (Main distribution área MDA).

El área de distribución principal alberga el punto de conexión cruzada central para el sistema de cableado estructurado del centro de datos. Esta área debe estar ubicada en una zona central para evitar superar las distancias del cableado recomendadas.

Área de distribución (Horizontal distribution area HDA).

El área de distribución horizontal es la ubicación de las interconexiones horizontales, el punto de distribución para el cableado hacia las áreas de distribución de los equipos.

Área de distribución de zonas (Zone distribution área ZDA).

Es el área de cableado estructurado para los equipos que van en el suelo y no pueden aceptar paneles de patcheo.

Área de distribución de los equipos (Equipmenet distribution área EDA).

Es la ubicación de los gabinetes y racks de equipos. La norma específica que los gabinetes y racks se deben colocar en una configuración (“pasillo caliente/pasillo frío”) para que disipen de manera eficaz el calor de los equipos electrónicos.

2.3. Infraestructura del cableado.

Racks y gabinetes.

La administración de los cables comienza con los racks y gabinetes, que deben brindar un amplio control de cables horizontales y verticales. Una administración adecuada no sólo mantiene el cableado organizado, sino que también mantiene los equipos frescos al eliminar los obstáculos que impiden el movimiento del aire. Estas características de los administradores de cables deben proteger los cables, asegurar de que no se excedan los límites del radio de curvatura y manejar la holgura de los cables con eficacia

Sistemas de tendido de cable.

Una clave para lograr un tendido de cables óptimo es tener extensas trayectorias de cables superiores y por debajo de piso. Use el trayecto por debajo de piso para el cableado permanente y el trayecto superior para el cableado temporal.

2.4. Tiers.

También se establecen 4 niveles en función de la redundancia necesaria para alcanzar niveles de redundancia, estos niveles van desde el TIER1 al más alto que es TIER 4 en donde se alcanza una disponibilidad de hasta el 99,995%. Estos centros suelen ser creados y mantenidos por grandes organizaciones con objeto de tener acceso a la información necesaria para sus operaciones.

Por ejemplo, un banco puede tener un data center con el propósito de almacenar todos los datos de sus clientes y las operaciones que estos realizan sobre sus cuentas. Prácticamente todas las compañías que son medianas o grandes tienen centros de cómputo que en la mayoría de los casos no cumplen con las mínimas normas necesarias para garantizar la integridad de sus sistemas, siendo este un punto crítico dentro de sus organizaciones.

Entre los factores más importantes que motivan la creación de un Data Center se puede destacar el garantizar la continuidad del servicio a clientes, empleados, ciudadanos, proveedores y empresas colaboradoras, pues en estos ámbitos es muy importante la protección física de los equipos informáticos o de comunicaciones, así como servidores de bases de datos que puedan contener información crítica.

2.4.1. Entendiendo los tiers.

Uno de los mayores puntos de confusión en el campo del uptime (tiempo disponible de los sistemas) es la definición de data center confiable; ya que lo que es aceptable para una persona o compañía no lo es para otra. Empresas competitivas con infraestructuras de data center completamente diferentes proclaman poseer alta disponibilidad; esto puede ser cierto y dependerá de la interpretación subjetiva de disponibilidad que se realice para el tipo de negocio en que se encuentre una compañía.

Lo cierto es que, para aumentar la redundancia y los niveles de confiabilidad, los puntos únicos de falla deben ser eliminados tanto en el data center como en la infraestructura que le da soporte. Los cuatro niveles de tiers que plantea el estándar se corresponden con cuatro niveles de disponibilidad, teniendo que a mayor número de tier mayor disponibilidad, lo que implica también mayores costos constructivos.

Esta clasificación es aplicable en forma independiente a cada subsistema de la infraestructura (telecomunicaciones, arquitectura, eléctrica y mecánica). Hay que tener en cuenta que la clasificación global del data center será igual a la de aquel subsistema que tenga el menor número de tier.

Esto significa que, si un data center tiene todos los subsistemas tier IV excepto el eléctrico que es tier III, la clasificación global será tier III. Es importante tener en cuenta esto porque cuando se pretende la adecuación de data centers actuales a tier IV, en lugares como América Latina, hay limitaciones físicas difíciles de salvar en los emplazamientos edilicios actuales. Prácticamente para lograr un data center tier IV hay que diseñarlos de cero con el estándar en mente como guía.

Un ejemplo claro de esto es que es muy difícil lograr la provisión de energía de dos subestaciones independientes o poder lograr las alturas que requiere el estándar en los edificios existentes. La norma describe, resumidamente, los distintos tiers de la manera que sigue:

2.4.2. Tier I: data center básico.

- Un data center tier 1 puede ser susceptible a interrupciones tanto planeadas como no planeadas.
- Cuenta con sistemas de aire acondicionado y distribución de energía; pero puede o no tener piso técnico, UPS o generador eléctrico; si los posee pueden no tener redundancia y existir varios puntos únicos de falla.
- La carga máxima de los sistemas en situaciones críticas es del 100%.
- La infraestructura del data center deberá estar fuera de servicio al menos una vez al año por razones de mantenimiento o reparaciones.
- Situaciones de urgencia pueden motivar paradas más frecuentes.
- La tasa de disponibilidad máxima del data center es 99.671% del tiempo.

2.4.3. Tier II: componentes redundantes.

- Los data centers con componentes redundantes son ligeramente menos susceptibles a interrupciones, tanto planeadas como las no planeadas.
- Estos data centers cuentan con piso falso, UPS y generadores eléctricos, pero están conectados a una sola línea de distribución eléctrica.
- Su diseño es “lo necesario más uno” (N+1), lo que significa que existe al menos un duplicado de cada componente de la infraestructura.
- La carga máxima de los sistemas en situaciones críticas es del 100%.
- El mantenimiento en la línea de distribución eléctrica o en otros componentes de la infraestructura pueden causar una interrupción del procesamiento.
- La tasa de disponibilidad máxima del datacenter es 99.749% del tiempo.

2.4.4. Tier III: mantenimiento concurrente.

- Permiten realizar cualquier actividad planeada sobre cualquier componente de la infraestructura sin interrupciones en la operación.
- Las actividades planeadas incluyen mantenimiento preventivo y programado, reparaciones o reemplazo de componentes y pruebas de componentes o sistemas, entre otros.
- Para infraestructuras que utilizan sistemas de enfriamiento por agua significa doble conjunto de tuberías.
- Debe existir suficiente capacidad y doble línea de distribución de los componentes, de forma tal que sea posible realizar mantenimiento o pruebas en una línea, mientras que la otra atiende la totalidad de la carga.
- En este tier, las actividades no planeadas como errores de operación o fallas espontáneas en la infraestructura pueden todavía causar una interrupción del data center.
- La carga máxima en los sistemas en situaciones críticas es de 90%.
- Muchos data centers tier III son diseñados para poder actualizarse a tier IV, cuando los requerimientos del negocio justifiquen el costo.
- La tasa de disponibilidad máxima del datacenter es 99.982% del tiempo.

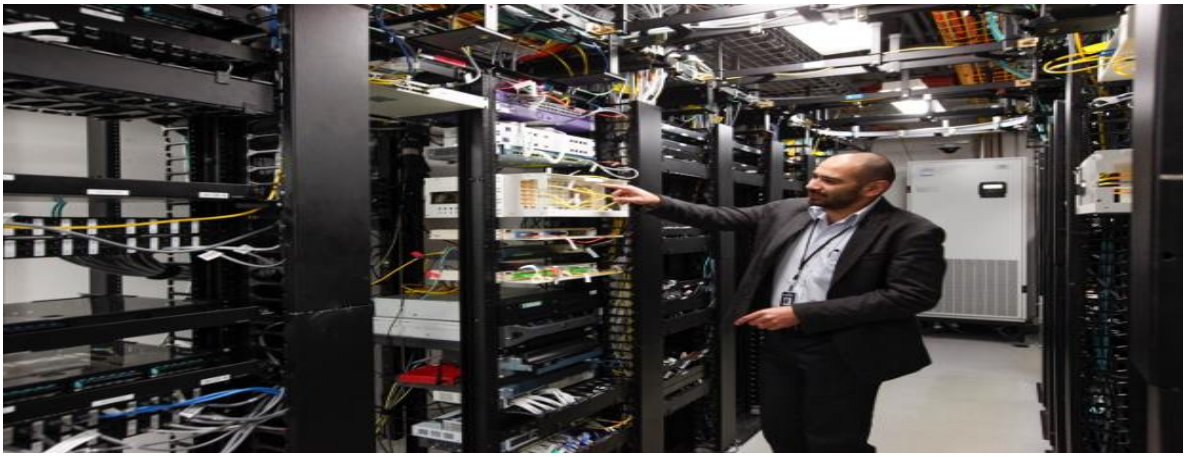

Figura 2: nivel 3 tier, mantenimiento de un data center.

2.4.5. Tier IV: tolerante a fallas.

- Este datacenter provee capacidad para realizar cualquier actividad planeada sin interrupciones en las cargas críticas, pero además la funcionalidad tolerante a fallas le permite a la infraestructura continuar operando aun ante un evento crítico no planeado.

- Esto requiere dos líneas de distribución simultáneamente activas, típicamente en una configuración System + System; eléctricamente esto significa dos sistemas de UPS independientes, cada sistema con un nivel de redundancia N+1.

- La carga máxima de los sistemas en situaciones críticas es de 90% y persiste un nivel de exposición a fallas, por el inicio una alarma de incendio o porque una persona inicie un procedimiento de apagado de emergencia o Emergency Power Off (EPO), los cuales deben existir para cumplir con los códigos de seguridad contra incendios o eléctricos.

- La tasa de disponibilidad máxima del datacenter es 99.995% del tiempo.

- Los porcentajes deben considerarse como el promedio de cinco años.

- Hay que tener en cuenta que para un tier IV se contempla que la única parada que se produce es por la activación de un EPO y esto sólo sucede una vez cada cinco años.

- No obstante, para la exigencia que demanda un tier IV algunas empresas u organizaciones manifiestan necesitar una disponibilidad de “cinco nueves”, esto significa un 99,999% de disponibilidad. Esto es poco más de cinco minutos anuales sin sistemas.

2.5. Consideraciones ambientales.

Las interacciones entre los servidores y su entorno a menudo plantean un riesgo importante para la disponibilidad del servidor, con amenazas potenciales tales como temperatura, humedad, fugas de agua, intrusión, vibración, error humano y cortes de energía.

Los costos de las amenazas ambientales para los centros de datos incluyen: reemplazo de artículos dañados, menor productividad del trabajador debido al tiempo de inactividad, pérdida de ingresos por aplicaciones no disponibles basadas en servidores y tiempo administrativo adicional y dinero invertido en la investigación y resolución de problemas.

Una parte crucial para mantener la alta disponibilidad radica en identificar y monitorear las amenazas ambientales en las salas de servidores, lo que permite una pronta respuesta a los peligros detectados antes de que escalen. Debido a esto existen condiciones ambientales que se deben considerar, estas incluyen:

Energía eléctrica

Determina los requerimientos de energía en base a la disponibilidad y puede incluir uno o más fuentes de alimentación de energía, UPS, entre otros. Para estimar la potencia de consumo de energía se debe realizar un análisis presente y también tener en consideración la redundancia y crecimiento a futuro.

Sistema de Enfriamiento

Se recomienda usar un adecuado sistema de enfriamiento. Adicionalmente indica que los gabinetes y racks deben ser ordenados teniendo en cuenta el patrón de pasillo caliente y pasillo frío. En los pasillos fríos, los equipos pueden ser dispuestos cara a cara. En los pasillos calientes, los equipos pueden ser dispuestos de manera opuesta.

3. Introducción Norma ISO 27001.

La norma ISO 27001 es el estándar internacional para la gestión de la seguridad de la información en las organizaciones, tanto para la información física como para la digital. La implementación de esta normativa, establece un enfoque sistemático para la gestión de la información organizacional confidencial y asegura que se mantenga protegida y disponible. En general, es un estándar amplio que cubre la seguridad técnica, física, de personal y de procesos en la compañía.

3.1. Para qué sirve la ISO 27001.

Concretamente, la norma ISO 27001 establece los requisitos para establecer, implementar, mantener y mejorar de forma continua un Sistema de Gestión de la Seguridad de la Información (SGSI). Estos sistemas son cada vez más comunes en las compañías, debido a los nuevos riesgos digitales inherentes a tecnologías como el aumento de los ciberataques. La norma ISO también incluye los requisitos para la apreciación y el tratamiento de los riesgos de seguridad de información a la medida de las necesidades de la organización.

3.2. Implementación ISO 27001: Principales ventajas.

- La principal ventaja de implementar la norma ISO 27001 es, como es obvio, garantizar que la información que maneja la empresa está bien protegida.
- Su implementación también ayudará a reducir los costes que podrían derivarse de incidentes de seguridad en la empresa.
- Por otro lado, contar con un Sistema de Gestión de Seguridad de la Información (SGSI) también facilitará a la organización cumplir con todos los requerimientos legales que ya existen en el ámbito de la protección de la información.

3.3. Fases para implantar un SGSI.

Las fases del proceso de implantación de un SGSI basado en la norma ISO 27001 pueden resumirse en 10 puntos fundamentales:

1. **Obtención del apoyo de la dirección**: La dirección o gerencia de la organización debe apoyar desde el principio la implantación del SGSI, respaldando y supervisando las medidas adoptadas.
2. **Definición del alcance e inventario de activos**: El alcance describe la extensión y los límites del SGSI. También es necesario elaborar y mantener un inventario de toda aquella información que tiene valor para la empresa.
3. **Análisis de riesgos**: Es importante contar con un buen plan de análisis y de tratamiento de riesgos.
4. **Desarrollo e implementación del programa de implantación del SGSI**: Consiste en el proyecto de implantación en sí.
5. **Herramientas de operación del sistema**: Se trata de los documentos que sustentan la operatividad del SGSI. Entre ellos debe estar el plan de continuidad.
6. **Auditoría interna**: Se debe establecer un plan de auditorías internas para revisar el SGSI dentro del proceso de mejora continua.
7. **Acciones correctivas**: Por cada no conformidad detectada en la auditoría, se deben proponer una o varias medidas de corrección.
8. **Auditoría de certificación**: La tiene que realizar una entidad externa y certificada. Si se supera, se obtiene la certificación ISO/IEC 27001.
9. **Operación integrada en la rutina del SGSI**: En esta fase se entiende que los procesos, políticas y controles de la norma están integrados en el funcionamiento rutinario de la organización.
10. **Auditorías anuales de vigilancia**: Estas auditorías pueden llevarse a cabo por un auditor interno pero lo idóneo es que las realice una entidad externa.

3.4. ¿En qué aporta la ISO 27001 a los centros de datos?

Un centro de datos, que sea considerado globalmente de alto nivel, debe contar estrictamente con varias características para poder asegurar a sus clientes que es un sitio seguro para el almacenamiento de su información, principalmente si ésta es considerada crítica para su negocio.

La primera de ellas, es contar con un diseño de la infraestructura certificado por un tercero con prestigio. Dicho diseño, debe contemplar todos los componentes que se consideran necesarios para ofrecer una solución robusta y redundante desde el punto de vista de generación eléctrica, ups, enfriamiento, seguridad, comunicaciones, respaldo y otros.

La segunda característica, es la experiencia, el conocimiento y las competencias del personal que administra su operación, ya que la infraestructura por sí sola no se gestiona. Dichas cualidades de los líderes de este tipo de empresa, se ven reflejadas cuando logran plasmar excelencia y disciplina en la forma en la que operan la infraestructura con la que se cuenta.

Muchos centros de datos pueden decir que basan su operación en las mejores prácticas de la industria, pero esto no es suficiente, se requiere que su gestión esté basada en normas afines al giro del negocio y que esto sea demostrable mediante una certificación de un tercero acreditado.

La norma ISO 27001 asegura a los clientes que se cuenta con un sistema de gestión de seguridad de la información (SGSI) que protege la disponibilidad, confidencialidad e integridad de la información que almacenan, mediante la gestión de los riesgos relacionados con los activos, contemplando así, toda la cadena de valor. Un SGSI certificado está basado en la mejora continua, lo cual asegura que las empresas constantemente están monitoreando su operación desde todos los puntos de vista posibles con el fin de identificar riesgos, evaluarlos, analizarlos y tratarlos de forma eficaz.

3.5. Políticas de seguridad para un centro de datos.

3.5.1. Políticas de seguridad de la información para el área de Arquitectura.

La ubicación y construcción del centro de datos deberá estar exenta de riesgos naturales (inundaciones, incendios, sismos), vías navegables, carreteras, líneas de ferrocarril, aeropuertos, muelles; con el fin de precautelar accidentes y ataques maliciosos y aplicar políticas de acceso al personal autorizado. Las áreas de estacionamiento, puestos de carga, visitantes deberán ser claramente identificadas y separadas del edificio principal del centro de datos; para precautelar accidentes y ataques maliciosos, e impartir políticas de acceso solo a personal autorizado.

El centro de datos deberá contar con resistencia al fuego, protección contra amenazas externas y ambientales en su diseño arquitectónico como muros, pasillos para prevenir accidentes, ataques maliciosos y garantizar áreas seguras para laborar. También deberá contar con un sistema de control y monitoreo.

3.5.2. Políticas de seguridad de la información para el área del Sistema Eléctrico.

El sistema eléctrico del centro de datos deberá tener redundancia, permitir el mantenimiento concurrente, evitar puntos de fallo, analizar la potencia del sistema, garantizar la alimentación continua y adecuada de los equipos; además del adecuado funcionamiento en caso de algún desastre natural.

El centro de datos deberá contar con un sistema de monitoreo de la vida útil de baterías y UPS, así como su tiempo de respaldo. El sistema eléctrico del centro de datos y todos sus elementos deberán estar protegidos de sobrecargas de energía, protección contra rayos, fallos a tierra; para garantizar la alimentación continua y adecuada de los equipos y su adecuado funcionamiento.

3.5.3. Políticas de seguridad de la información para el área del Sistema Mecánico.

El sistema de tuberías deberá tener la capacidad de rechazar el calor y controlar los niveles de humedad, su enrutamiento no debe estar asociado con los equipos; brindando la seguridad y evitando incidentes que pueden ocasionarse por fallas en el mismo.

El sistema de climatización deberá ser redundante, tener presión positiva, contar con sistemas mecánicos de reserva, unidades aire acondicionado, sistemas de control; brindando la seguridad y evitando incidentes que pueden ocasionarse por fallas en el mismo.

El sistema mecánico del centro de datos deberá contar con sistemas de detección de fuego, rociadores contra incendios, supresión gaseosa, detecciones de humo de alerta temprana y detección de fugas de gas; brindando la seguridad y evitando incidentes que pueden ocasionarse por fallas en el mismo.

3.5.4. Políticas de seguridad de la información para el área de Telecomunicaciones.

En este ítem se identificaron políticas de seguridad de la información para la infraestructura de telecomunicaciones en un centro de datos: equipos, cableado, salas, áreas, proveedor y accesos. Se deberá etiquetar los paneles, el sistema de cableado, armarios y bastidores en concordancia al esquema de clasificación de la organización; los mismos que deberán contar con mecanismos de seguridad contra daños, interferencias e interceptaciones garantizando la continuidad del servicio ya la protección de la información.

Los accesos a las diferentes áreas, salas y equipos del centro de datos; deberán contar con mecanismos de seguridad, protecciones contra fallos, alteraciones en el suministro eléctrico y seguridad contra daños físicos y ambientales, garantizando la continuidad del servicio ya la protección de la información.

4. Introducción Norma ISO 27002.

La norma ISO 27002 (anteriormente denominada ISO 17799) es un estándar para la seguridad de la información que ha publicado la organización internacional de normalización y la comisión electrotécnica internacional. La versión más reciente de la norma ISO 27002:2013.

La norma ISO 27002 proporciona diferentes recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables para iniciar, implementar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como “la preservación de la confidencialidad, integridad y disponibilidad.

La norma ISO 27002 se encuentra enfocada a todo tipo de empresas, independientemente del tamaño, tipo o naturaleza. La norma ISO 27002 se encuentra organizado en base a los 14 dominios, 35 objetivos de control y 114 controles. El documento denominado política es aquel que expresa una intención e instrucción general de la forma que ha sido expresada por la dirección de la empresa.

El contenido de las políticas se basa en el contexto en el que opera una empresa y suele ser considerado en su redacción todos los fines y objetivos de la empresa, las estrategias adoptadas para conseguir sus objetivos, la estructura y los procesos utilizados por la empresa.

Además, de los objetivos generales y específicos relacionados con el tema de la política y los requisitos de las políticas procedentes de niveles mucho más superiores y que se encuentran relacionadas. La política de alto nivel se encuentra relacionada con un Sistema de Gestión de Seguridad de la Información que suele estar apoyada por políticas de bajo nivel, específicas para aspectos concretos en temáticas como el control de accesos, la clasificación de la información, la seguridad física y ambiental, utilizar activos, dispositivos móviles y protección contra los malware.

4.1. ¿Cuáles son los principales ítems que componen la ISO 27002?

La parte principal de la norma se encuentra distribuida en las siguientes secciones, que corresponden a controles de seguridad de la información. Es importante recordar que la organización puede utilizar esas directrices como base para el desarrollo del SGSI. Como sigue:

Política de Seguridad de la Información.

Se debe crear un documento sobre la política de seguridad de la información de la empresa, que debe contener los conceptos de seguridad de la información, una estructura para establecer los objetivos y las formas de control, el compromiso de la dirección con la política, entre tantos otros factores.

Organización de la Seguridad de la Información.

Para implementar la Seguridad de la Información en una empresa, es necesario establecer una estructura para gestionarla de una manera adecuada. Para ello, las actividades de seguridad de la información deben ser coordinadas por representantes de la organización, que deben tener responsabilidades bien definidas y proteger las informaciones de carácter confidencial.

Gestión de activos.

Activo, según la norma, es cualquier cosa que tenga valor para la organización y que necesita ser protegido. Pero para ello los activos deben ser identificados y clasificados, de modo que un inventario pueda ser estructurado y posteriormente mantenido. Además, deben seguir reglas documentadas, que definen qué tipo de uso se permite hacer con dichos activos.

Seguridad en recursos humanos.

Antes de la contratación de un empleado o incluso de proveedores es importante que sea debidamente analizado, principalmente si se trata de información de carácter confidencial. La intención de esta sección es mitigar el riesgo de robo, fraude o mal uso de los recursos. Y cuando el empleado esté trabajando en la empresa, debe ser consciente de las amenazas relativas a la seguridad de la información, así como de sus responsabilidades y obligaciones.

Seguridad física y del medio ambiente.

Los equipos e instalaciones de procesamiento de información crítica o sensible deben mantenerse en áreas seguras, con niveles y controles de acceso apropiados, incluyendo protección contra amenazas físicas y ambientales.

Seguridad de las operaciones y comunicaciones.

Es importante que estén definidos los procedimientos y responsabilidades por la gestión y operación de todos los recursos de procesamiento de la información. Esto incluye la gestión de servicios tercerizados, la planificación de recursos de los sistemas para minimizar el riesgo de fallas, la creación de procedimientos para la generación de copias de seguridad y su recuperación, así como la administración segura de las redes de comunicaciones.

Control de acceso.

El acceso a la información, debe ser controlado con base en los requisitos de negocio y en la seguridad de la información. Debe garantizarse el acceso de usuario autorizado y prevenido el acceso no autorizado a los sistemas de información, a fin de evitar daños a documentos y recursos de procesamiento de la información que estén al alcance de cualquiera.

Adquisición, desarrollo y mantenimiento de sistemas.

Los requisitos de seguridad de los sistemas de información deben ser identificados y acordados antes de su desarrollo y/o de su implementación, para que así puedan ser protegidos para el mantenimiento de su confidencialidad, autenticidad o integridad por medios criptográficos.

Gestión de incidentes de seguridad de la información.

Los procedimientos formales de registro y escalonamiento deben ser establecidos y los empleados, proveedores y terceros deben ser conscientes de los procedimientos para notificar los eventos de seguridad de la información para asegurar que se comuniquen lo más rápido posible y corregidos en tiempo hábil.

Gestión de continuidad del negocio.

Los planes de continuidad del negocio deben ser desarrollados e implementados, con el fin de impedir la interrupción de las actividades del negocio y asegurar que las operaciones esenciales sean rápidamente recuperadas.

Conformidad.

Es importante evitar la violación de cualquier ley criminal o civil, garantizando estatutos, regulaciones u obligaciones contractuales y de cualesquiera requisitos de seguridad de la información. En caso necesario, la empresa puede contratar una consultoría especializada, para que se verifique su conformidad y adherencia a los requisitos legales y reglamentarios.

5. Introducción Norma ISO 20000(Administración de servicios TI).

La serie de Normas ISO/IEC 20000 (UNE-ISO/IEC 20000 en la versión española) es el primer conjunto de normativa internacional específica para la gestión de los servicios basados en las Tecnologías de la Información (TI). Presentan una organización cabal de las principales actividades necesarias para gestionar estos servicios, agrupadas en un conjunto de procesos considerados esenciales para la creación, prestación y evolución de los servicios de las TI. Al aplicar sus requisitos y recomendaciones, las organizaciones de TI emprenderán un camino indudable de mejora en el control y la calidad de su actividad.

Es el primer gran salto hacia la excelencia demandada por la sociedad a las TI. Se pueden considerar como normas “troncales” en la gestión de las TI, pues estructuran en torno a procesos las actividades más esenciales. Alrededor del eje vertebrador que crean las Normas ISO/IEC 20000 se irán construyendo y transformando el resto de las funciones de la organización de las TI.

Sobre este núcleo central, creado para la gestión de las TI, se irán incorporando otras mejores formas de hacer proporcionadas por otras normas, otros marcos de mejores prácticas, por la experiencia propia de la empresa o por las aportaciones de consultores externos. Las Normas ISO/IEC 20000 introducen en la organización de las TI una forma de trabajo metódica, integrada y orientada a los procesos, haciendo especial énfasis en garantizar la calidad del servicio a los distintos clientes de las TI.

Además, articulan su implantación con un sistema de gestión específico, que incorpora la disciplina y el rigor de ISO 90000 en la implantación del modelo de trabajo en las TI. Las Normas ISO/IEC 20000 forman parte del conjunto de normas producidas por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC).

Entender las Normas ISO/IEC 20000 esencial de la actividad de gestión de los servicios, pero no abarcan la totalidad de la actividad de TI. No son unas normas sobre la tecnología en sí misma, sino que se centran en las actividades de las personas para gestionarlas (procesos) y en identificar los roles necesarios para llevarlas a cabo. Existen algunas disciplinas que hay que tener en cuenta para lograr la excelencia del proveedor de TI, como son:

- La alineación de TI con las necesidades del negocio.
- La gestión de la demanda de las necesidades del negocio.
- La planificación de la cartera anual de proyectos.
- La madurez de los procesos de desarrollo y sus metodologías.
- El imprescindible conocimiento técnico.
- La arquitectura de las aplicaciones y de la infraestructura.
- La renovación de las infraestructuras.
- La calidad de los proveedores y de los servicios contratados.
- El liderazgo de la dirección, la motivación del personal.

Si realizásemos un esquema que reflejara toda la actividad llevada a cabo en TI, las funciones y los recursos tecnológicos, tendríamos:

Para coronar el esquema, en la parte más alta, se definirían las actividades de gobierno de TI: estrategia, alineación con el negocio. Por debajo de ellas estarían los procesos de gestión del servicio de TI. En el siguiente nivel se situarían los equipos que constituyen las fuerzas de trabajo de TI: con la operación, funciones técnicas, el desarrollo de software, y el resto de especialidades y conocimientos tecnológicos.

A continuación, aparecería la capa de herramientas: de soporte a la gestión, de administración técnica, de monitorización, es decir, las herramientas que hacen que la actividad sea más fluida y controlada. Por último, la capa en la base del esquema, que alojaría la tecnología: sistemas, aplicaciones e infraestructura de TI (tecnología suministrada por los fabricantes, comunicaciones, edificios para alojarlos, entre otros.)

5.1. Principios básicos de ISO/IEC 20000.

El servicio. Es fundamental orientar las TI hacia el objetivo de prestar servicio a sus áreas de negocio. La actividad de TI se debe estructurar completamente bajo el concepto de servicio y no centrarse exclusivamente en el dominio de tecnologías aisladas.

La orientación al cliente. De forma complementaria a la anterior, los departamentos de TI tienen que desarrollar la capacidad de orientarse al cliente. Cambiar las formas de trabajar para que los objetivos del negocio sean asumidos como propios. Se pone foco en las relaciones con el negocio y con los usuarios de los servicios.

La comunicación interna. Potenciar la comunicación interna entre las diversas áreas y entre las personas.

Los procesos internos. Organizar la actividad y el trabajo de todo el equipo para que fluya sin fricciones y al ritmo demandado por el negocio. Todo ello, dentro de un entorno de calidad y mejora continua.

5.2. Comprender el concepto de “servicio de TI”.

El término servicio ya se da por conocido en estas normas y, por tanto, no se define en ellas, pero para las áreas de TI internas de las empresas no les es fácil encajarlo en su actividad. Resulta importante profundizar sobre su alcance para poder entender el ámbito de aplicación de estas normas, ya que se centran en establecer los requisitos necesarios para prestar estos servicios.

Con frecuencia se contamina el concepto de servicio que el negocio o cliente quiere recibir de TI, con los componentes tecnológicos que lo soportan. En cambio, cuando los servicios se ofrecen al exterior, es el propio mercado y la competencia los que van perfilando su alcance y correcta definición.

Así, podríamos definir servicio como toda contraprestación por la que el cliente paga. Pero en el caso de prestación de servicios internos, su alcance no está tan claro y hay que hacer un cierto esfuerzo por conceptualizarlo.

En el ámbito interno de TI se podría definir servicio como “una funcionalidad necesaria para los usuarios”, semejante al concepto utilizado en las relaciones comerciales del mercado. Se entiende que un servicio de TI es una solución informática completa que cubre unas necesidades específicas del negocio, que TI entrega y mantiene de forma autocontenida y empaquetada, liberando al cliente y a los usuarios de las complejidades internas de su tecnología. De esta forma, los servicios de TI se deben convertir en una parte esencial en la cadena de valor del negocio.

Algunos ejemplos de servicios bajo el alcance de estas normas son lo los siguientes:

- La provisión del puesto de trabajo: el ordenador del puesto de trabajo conectado, operativo y soportado.
- El correo electrónico.
- El sitio web de la empresa.
- El portal web interno de la empresa (la intranet).
- El servicio de ERP (Enterprise Resource Planning) de una empresa.
- El servicio de alojamiento de aplicaciones o portales web.
- El servicio de alojamiento de servidores ofrecido por un Data Center.
- El servicio de facturación.
- El servicio de gestión del conocimiento.
- El servicio de colaboración.

6. Conclusión.

El propósito del estándar TIA 942 es proveer una serie de recomendaciones y guidelines para el diseño e instalación de un datacenter. La intención es que sea utilizado por los diseñadores que necesitan un conocimiento acabado del facility planning, el sistema de cableado y el diseño de redes.

El estándar TIA 942 y la categorización de tiers lleva al replanteo de las necesidades de infraestructura de una manera racional y alineada con las necesidades propias de disponibilidad del negocio en que se encuentran las organizaciones.

La norma ISO 27001, a diferencia de otras normas que también podrían ser implementadas, no solo viene a aportar en temas de administración, operación y calidad de los servicios que se entregan a los clientes, sino que además de cumplir con esas características, lo hace con un enfoque especializado en la seguridad de la información, lo cual al fin de cuentas es el propósito de un centro de datos, asegurar la información de los clientes.

Seguir los principios de la certificación, **ISO/IEC 27002** es un paso altamente relevante para garantizar la seguridad de la información en las empresas. En este sentido, es primordial resaltar la importancia de empresas poseer profesionales certificados en sus equipos de seguridad, dando mayor respaldo al proceso de implantación de las buenas prácticas relacionadas a la norma, así como la obtención de certificación corporativa ISO 27001.

La norma ISO 20000 fue una de las primeras normas que se utilizaron para la administración de servicios de TI. Además, dicha norma brinda diferentes servicios para TI dependiendo del área de la informática que se esté trabajando, en este caso los data center.