Abril 2016 - ISSN: 1988-7833

EL USO DE LAS NUEVAS TECNOLOGÍAS AL SERVICIO DEL BUEN VIVIR Y LAS GESTIONES ADMINISTRATIVAS DEL SERVICIO PÚBLICO

1 Ing. Karla Maribel Ortiz Chimbo. MSc.

2 Ing. José Medina Moreira; MSc

3 Jennifer Alexandra Astudillo Galarza,

4 Kenys Elizabeth Holguín Quijije,

1 Coordinadora de la Comisión de Evaluación y Acreditación de la Facultad de Filosofía y Docente de la Carrera Ingeniería en Networking

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS) de la Universidad de Guayaquil,

2 Subdirector y Docente de la Carrera Ingeniería en Networking

(FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS) de la Universidad de Guayaquil

3 Estudiante de la Carrera Ingeniería en Networking

(FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS) de la Universidad de Guayaquil

4 Estudiante de la Carrera Ingeniería en Networking

(FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS) de la Universidad de Guayaquil

1 karla.ortizch@ug.edu.ec

2 jose.medinam@ug.edu.ec

3 jenlady_202009@hotmail.com

4 elizaholguin16@hotmail.com

Para citar este artículo puede uitlizar el siguiente formato:

Karla Maribel Ortiz Chimbo, José Medina Moreira, Jennifer Alexandra Astudillo Galarza y Kenys Elizabeth Holguín Quijije (2016): "El uso de las nuevas tecnologías al servicio del buen vivir y las gestiones administrativas del servicio público", Revista Contribuciones a las Ciencias Sociales, (abril-junio 2016). En línea: http://www.eumed.net/rev/cccss/2016/02/servicios.html

RESUMEN

Dentro del uso de nuevas tecnologías al servicio del buen vivir, un centro de datos es importante para todo tipo de empresa, porque es allí donde se almacena la información crítica, razón por la cual se debe mantener una administración rápida, segura y centralizada. El objetivo principal es realizar una evaluación técnica de la nueva tecnología utilizada, para que cuente con una infraestructura tecnológica adecuada que permita la aplicación de nuevos servicios que mejoren los procesos internos al servicio público. Por tal motivo, es de interés conocer las normas que existen así como realizar un análisis riguroso a toda la infraestructura tecnológica para lograr un adecuado diseño del centro de datos siguiendo las recomendaciones que los estándares brindan, además de saber cómo aplicarlas.

PALABRAS CLAVES: Tecnología, buen vivir, gestión, servicio, redes, centro de datos.

SUMMARY

Within the use of new technologies in the service of good living, a data center is important for all types of business, because that is where critical information is stored, why should maintain a fast, secure and centralized management. The main objective is to conduct a technical assessment of the new technology used, so that it has an adequate technological infrastructure for the implementation of new services that will improve public service internal processes. For this reason, it is interesting to know that there are rules and a rigorous entire technological infrastructure analysis for proper data center design following the recommendations that standards provide, and know how to apply them.

Keywords: Technology, good living, management, service, networking, data center.

I.- INTRODUCCIÓN:

El uso de las nuevas tecnologías en un centro de datos es de gran importancia para una empresa sea esta pública o privada, ya que tiene una misión en común: proteger la información más importante y relevante de la organización, además de ser el lugar donde se albergan todos los recursos dedicados al procesamiento de los datos, los cuales se consideran ambientes críticos por lo que están expuestos a diferentes amenazas.

Por tanto, el ambiente o la infraestructura donde se va a alojar a los equipos es un aspecto fundamental, ya que se debe establecer las mejores condiciones tanto físicas como ambientales para su conservación, las mismas que deben estar definidas por estándares técnicos (tecnología). Además, es necesario considerar el tema de la seguridad para el acceso a las instalaciones y así impedir que existan fugas de información o robo de los equipos, se debe disponer de las herramientas apropiadas ante cualquier posible siniestro humano o natural y tener una temperatura adecuada para evitar sobrecalentamiento en los equipos, lo que podría provocar su deterioro.

Por tal motivo se debe tomar en consideración estándares como: “ANSI/TIA/EIA-942 Telecommunications Infrastructure Standard for Data Centers”, aplicable para centro de datos de todo tamaño descritos en 4 niveles, que nos ayudarán a conocer cuáles son los requerimientos mínimos de la infraestructura en cada nivel, sin olvidar que la información es uno de los activos más importantes de toda empresa por lo que se deben desarrollar políticas de seguridad en base al estándar ISO 27002 que proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información.

Se debe tener en cuenta que las empresas públicas, no están exentas a ataques informáticos siendo blanco fácil de personas malintencionadas

que buscaran sustraer información para fines ilícitos, dañinos o de carácter lucrativo, por lo que se debe emprender un plan de acción que permita proteger su información, para lo cual se han considerado procedimientos, con la finalidad de fortalecer los equipos, garantizando el cumplimiento de los derechos de los ciudadanos.

II.- ANTECEDENTES:

En las instituciones públicas debe ser prioritario mejorar la seguridad en los sistemas tecnológicos, es por ello que, habitualmente, se deben realizar procesos de fortificación de sistemas además de la ejecución de test de intrusión que comprueben hasta donde se puede llegar y que se pueda obtener. Los test de intrusión forman parte de las auditorias de seguridad informática (Álvarez Martín & González Pérez, 2013).

Un centro de datos es el responsable de brindar servicios de procesamiento y almacenamiento de la información de forma sistematizada y automática ya que aquí reside información crítica por lo que su objetivo principal es garantizar la integridad, confidencialidad y disponibilidad de los datos, para esto se necesita de un correcto diseño y administración de su infraestructura para institución de cualquier tamaño.

Un centro de datos consiste en uno o varios locales, una planta o un edificio completo que alberga el sistema principal de redes, ordenadores y recursos asociados para procesar toda la información de una empresa u organismo (Aguilera López, 2010, pág. 45).

El diseño del centro de datos es un proceso que involucra el espacio físico, climatización adecuada, alimentación eléctrica, cableado estructurado, sistemas contra incendios, control de acceso, sistemas de cámaras de vigilancia, control de temperatura y humedad. Sin embargo, no podemos olvidar el tema de la seguridad de la información para poder aprovechar plenamente las ventajas del centro de datos con el fin de proporcionar una infraestructura gestionable y que cumpla las normativas pertinentes.

En lo que se refiere a los nudos críticos que se presentan en la infraestructura de un centro de datos, tenemos los siguientes:

- La falta de espacio produce mala distribución de los equipos.
- La falta de diagramación de la red y documentación que especifique características de los equipos.
- La falta de UPS no permite suministrar energía en caso de fallo en un tiempo corto para proteger los equipos.
- La falta de climatización adecuada provoca fallas y reduce el tiempo de vida de los equipos.
- La falta de un sistema puesta a tierra para disminuir el daño a los equipos en caso de sobrecargas de energía.
- No existe un sistema de detección y extinción de incendios.
- Las baterías utilizadas no son las adecuadas.
- La falta de un sistema de vigilancia para controlar el personal que tiene acceso al centro de datos.
- La falta de bitácoras y un sistema de control de acceso.
- Falta de monitoreo en el rendimiento de los equipos.
- Falta de licenciamiento en los servidores.
- Cambio de equipos para que soporten nuevas tecnologías.

En los primeros centro de datos su diseño e implementación se basaba en arquitectura clásica por lo grande que era, y lo mucho que pesaban sus equipos. Estos criterios no eran negociables en ese entonces, en la que los equipos eran "apilables" en mesas, armarios o racks, los sistemas informáticos utilizaban mucha energía y eran propenso recalentamiento (Taborda, Escobar, & Torres, 2011, pág. 2)**.**

La necesidad de la optimización del espacio y la fácil administración de los sistemas informáticos han hecho que evolucionen los equipos cuyas dimensiones permiten aprovechar al máximo el volumen disponible en los racks, logrando una alta densidad de equipos por unidad de espacio.

Los Centro de Datos inicialmente no estaban diseñados para proporcionar facilidades de red avanzadas, ni los requerimientos mínimos de ancho de banda y velocidad de las arquitecturas actuales. La evolución del Internet y la necesidad de estar siempre conectados en todo momento y en todo lugar han obligado a las instituciones a mejorar su infraestructura tecnológica, de tal manera que se proteja la información y esté disponible sin interrupciones, con el objetivo de no poner en riesgo sus negocios, sin importar el tamaño. Por ejemplo: Al igual que banco es el mejor sitio para guardar el dinero, un centro de datos lo es para alojar equipos y sistemas de información.

En toda institución pública o privada la información ha llegado a ser un activo que al igual que los demás activos tangibles pueden llegar a ser esenciales para la continuidad del negocio y en consecuencia necesitan ser protegidos de tal forma que garanticen su confidencialidad, integridad y disponibilidad (Guambuguete , 2012, pág. 30).

- **Causas del problema y consecuencias:**

Uno de los inconvenientes en la infraestructura es el espacio físico porque es reducido lo que dificulta la distribución de los equipos, ya que estos disipan mucho calor en el ambiente por lo que se necesita de una climatización apropiada que mantenga la temperatura y humedad interna en niveles constantes para que garantice el rendimiento de los equipos y aumente su tiempo de vida.

Otro problema es el cableado estructurado mal organizado por lo que se vuelve complicada la identificación y administración del mismo, ya que no se tiene la documentación de la red y esto dificulta el mantenimiento. La falta de un sistema puesta a tierra y la inadecuada instalación eléctrica es otro aspecto que perjudica al centro de datos ya que no tiene una acometida apropiada lo que afectaría a los equipos e incluso provocaría su daño.

Al no existir un sistema de detección y extinción de incendios no se puede detectar cualquier indicio de fuego para poder contrarrestar a tiempo el desastre que podría ocasionar daños en los equipos y pérdidas económicas en la institución.
En cuanto a su seguridad el no disponer de un sistema de control de acceso y cámaras de seguridad lo cual no permite controlar y monitorear lo que sucede en el centro de datos para de esta forma evitar robos y sabotajes.

Por otra parte los equipos actualmente no soportan nuevas tecnologías debido a que se requiere equipos con mayores recursos, también la falta de herramientas, técnicas, procesos y equipos de seguridad que ayuden a reducir las posibles vulnerabilidades de un sistema pueden poner en riesgos la información, haciendo que se pierda la confidencialidad de los datos de la institución.

III.- PILARES FUNDAMENTALES DE LA SEGURIDAD INFORMÁTICA EN EL USO DE LAS NUEVAS TECNOLOGIAS:

Seguridad Informática

La seguridad informática se debe considerar como un tema importante para las entidades por lo que no debe aislarse de los demás procesos que se manejen en ella, debido a que la información está expuesta a diferentes amenazas y vulnerabilidades. Es un conjunto de elementos físicos y lógicos dedicados a imposibilitar el acceso a un sistema informático a todo aquel que no se encuentra autorizado, brindando protección a la infraestructura tecnológica.

Para lograr la seguridad en los sistemas se debe implementar un conjunto de controles en software, hardware, políticas de control y acceso.
Los sistemas de información se consideran seguros cuando cumple con:

- Integridad.
- Confidencialidad.
- Disponibilidad.

Integridad: Garantiza que la información sea auténtica y precisa, que no sufra ningún tipo alteraciones, o dicho de otra manera, que no hayan sido borrados, ni destruidos de modo no autorizado.

Confidencialidad: Se garantiza que la información sea de uso exclusivo para las personas o entidades que se encuentren autorizados, cualquier otra no deberá poder visualizar dicha información.

Disponibilidad: Asegura que la información debe estar disponible para los usuarios autorizados, sin interrupción de ningún tipo. Se deben emplear medidas que resguarden la información, así como realizar copias de seguridad y mecanismos para restaurar los datos que se hubiesen dañado o destruido de manera accidental o intencionadamente.

La aplicación de estos 3 pilares es esencial para toda la estructura de la red, ya que nos permitirán mantener segura y disponible la información, ya que es el bien más preciado que tienen las entidades.

"La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable" (Aguilera, 2010, pág. 9)**.**

IV.- CLASIFICACIÓN DE LA SEGURIDAD INFORMÁTICA AL SERVICIO DEL BUEN VIVIR:

Seguridad física

Hace referencia a la protección del hardware y de los soportes de datos. Es un aspecto importante que se debe de tener en cuenta a la hora de realizar un diseño de redes o una ampliación ya que permite emplear procedimientos de control, tomar medidas de prevención y contramedidas ante amenazas a los recursos e información reservada, cuyo objetivo es proteger los sistemas informáticos de una entidad.

Las amenazas que se pueden presentar en un centro de datos a nivel físico pueden ser desastres naturales, accidentales e intencionales (Ej. terremotos, inundaciones, robos, incendios, el polvo y la humedad pueden causar daños irreparables) por tanto, se debe guardar copias de seguridad de la información mediante respaldos de los datos que se deben alojarse en un lugar seguro, también no debemos dejar atrás la utilización de cortafuegos ya sea por hardware o software, alarma contra incendios, detector de humo, extintor, video vigilancia, control biométrico, tarjetas inteligentes , bitácoras de acceso entre otros mecanismos de protección que garanticen la seguridad en el entorno donde están ubicados los equipos.

Seguridad Lógica

Se basa en el uso de mecanismo, procedimientos y herramientas de seguridad que protejan la información, procesos y programas a los cual solo debe tener acceso el personal autorizado, tiene como objetivo proteger digitalmente la información.

Para la implementación de la seguridad lógica se debe tomar en consideración lo siguiente:

- Control de acceso: usuario y contraseñas.
- Control mediante el uso de un utilitario de red para proteger la integridad de la información y conservar los datos confidenciales.
- Control en el cifrado de datos mediante un algoritmo de encriptación para fortalecer la confidencialidad.
- Antivirus que permitan detección de virus y software malicioso a tiempo para poder corregirlos o eliminarlos y así poder proteger la integridad de la información.
- Los Cortafuegos (Hardware, software o mixtos) permiten, restringen o deniegan el acceso al sistema.

V.- HERRAMIENTAS DE ANÁLISIS Y GESTIÓN PARA LA SEGURIDAD INFORMÁTICA:

Política de seguridad

Reúne las directrices y objetivos de una entidad con relación a la seguridad de la información, por tanto, debe ser autorizada por la dirección encargada.

El objetivo fundamental de la realización de una política es la de sensibilizar a todo los empleados, y en especial al encargado del sistema informático, para que pueda comprender que principios y normas rigen en la seguridad de la institución. Por tanto, su contenido se debe expresar de tal manera que pueda ser entendible para todos los empleados.

Los objetivos de la empresa en materia de seguridad, incluyen los siguientes:

- Determinar las necesidades de seguridad, los riesgos que pueden afectar al sistema de información y valorar el impacto que puede causar un ataque.

- Se debe relacionar todas las medidas de seguridad necesarias que deben aplicarse para enfrentar posibles riesgos de cada equipo.
- Proveer una visión general de las pautas y los métodos que deben emplearse para enfrentar riesgos identificados en las diferentes áreas de la institución.
- Realizar un plan de emergencia para garantizar la continuidad de las actividades del negocio.

Auditoría de Seguridad

Es una evaluación que se realiza a los sistemas informáticos, para descubrir vulnerabilidades, establecer medidas que permitan proteger la información y analizar de manera periódica los riesgos y amenazas. Su finalidad es comprobar que se cumplen los objetivos de la política de seguridad de la institución.

Una vez conseguidos los resultados se entrega al responsable una documentación en la que se detalla la descripción de los equipos instalados, servidores, sistemas operativos, análisis de seguridad en los equipos y en la red, análisis de la eficiencia de los programas informáticos, gestión de los sistemas instalados y posibles vulnerabilidades.

Metodologías y normativas internacionales para la seguridad informática

Los estándares son recomendaciones que ayudan a la gestión de la seguridad informática ya que establecen un lenguaje común de entendimiento en el que es posible reconocer las necesidades de seguridad de los activos más valiosos de una organización, además estos estándares permiten definir si el valor a invertir en TI es necesario o no para la organización.

Los estándares más importantes son COBIT, ITIL e ISO, ellos se encargan de la administración y la auditoria de seguridad informática a nivel mundial. Por lo que se consideran útiles para el desarrollo y éxito de una organización.

VI.- ITIL.- LIBRERÍA DE INFRAESTRUCTURA DE TECNOLOGÍAS DE INFORMACIÓN:

Information Technology Infrastructure Library es un estándar mundial de facto para la administración y gestión de los servicios tecnológicos, cuya estructura ha demostrado ser beneficiosa para brindar orientación a las entidades de distintos sectores debido a que proporcionan un conjunto de mejores prácticas. ITIL pertenece a la OGC (Oficina de Comercio del Gobierno Británico), pero es de libre utilización a nivel internacional.

ITIL se desarrolló debido a que las entidades necesitan cada vez más de la automatización de sus sistemas informáticos para alcanzar los objetivos del negocio. Por lo que se necesita ofrecer servicios de calidad y que cumplan con los requisitos solicitados para proporcionar una correcta gestión.

Uno de los aspectos principales es que ITIL V3 considera un marco referencial basado en un conjunto de mejores prácticas y estructuras que reflejan el ciclo de vida de los servicios de TI el cual se ajusta al tipo de negocio. También, está dirigida a lograr fines corporativos a través de un enfoque ordenado de los servicios y a establecer estrategias para la gestión operativa de la infraestructura de TI.

Gráfico N. 1

Ciclo de vida de la gestión de servicio de ITIL

Elaboración: Autores

Fuente: http://www.marlonmolina.com/p/2008-2009.html

Ventajas de ITIL

- Los servicios de TI son bien detallados y documentados.
- Uso y aprovechamiento correcto de la tecnología.
- Mejora los canales de comunicación.
- Aumenta la calidad en la entrega de servicios.
- Facilidad de adaptarse a los servicios.
- La entidad desarrolla una distribución clara, eficiente y centrada en sus objetivos.
- Incremento de la calidad en los procesos de negocio.
- Permite a la administración tener control e identificar los cambios y procesos más fáciles de realizar.
- Cambiar la forma de tomar decisiones, porque toma en cuenta las mejores prácticas.

Desventajas de ITIL

- Necesita de tiempo y esfuerzo para su ejecución.
- Que el área implicada no considere el cambio.
- Que por falta conocimiento sobre los procesos y métodos no exista una mejora.
- Que el personal no brinde su colaboración.
- Puede o no ser visible la reducción de costos y mejora del servicio.
- Que no exista presupuesto para invertir debido a que los procesos se consideran inútiles.

Descripción de los procesos de ITIL V3:

1. **Estrategia de servicio.-** Su objetivo es promover que los servicios se conviertan en activos importantes y que cumplan con los objetivos de la empresa.
2. **Diseño del servicio.-** Debe abarcar todas las especificaciones y métodos necesarios que contribuyan a la entrega de servicios de calidad que cumplan las expectativas del cliente y la visión del negocio.
3. **Transición del Servicio.-**Involucra el proceso de cambio para la implementación de nuevos servicios o mejora. Deben proporcionar rapidez, seguridad y costos equilibrados, mientras se garantiza que no se exista inconveniente para su operación.
4. **Operación del Servicio.-**En esta etapa se ejecuta las mejores prácticas para la gestión del día a día en la operación del servicio, para garantizar que se entrega servicio de alta calidad.
5. **Mejora Continua del Servicio.-** Facilita una estructura para crear y mantener la efectividad y operatividad del servicio .Es esta fase es donde se descubre nuevas vías que se pueden cubrir para mejorar el servicio.

CUADRO N. 1

CICLO DE VIDA Y PROCESOS DE ITIL V3

Ciclo de vida	Proceso
Estrategia del servicio	Gestión Financiera y Gestión de Portafolios
Diseño del servicio	Gestión de Nivel de Servicio
	Gestión de la Capacidad
	Gestión de continuidad de servicios TI
	Gestión de la Disponibilidad, Gestión de Riesgos, Gestión de Seguridad
Transición del servicio	Gestión de Configuración y activos
	Gestión del Conocimiento

	Gestión de Cambios
	Gestión de liberaciones de nuevas versiones e implantaciones
Operación del servicio	Service Desk y Gestión de Incidentes
	Gestión de Problema
Mejora continua del servicio	Evaluación de Servicios y Evaluación de Procesos
	Definición de Iniciativas de Mejoramiento y Monitorización

Elaboración: Autores

Fuente: Datos de la Investigación.

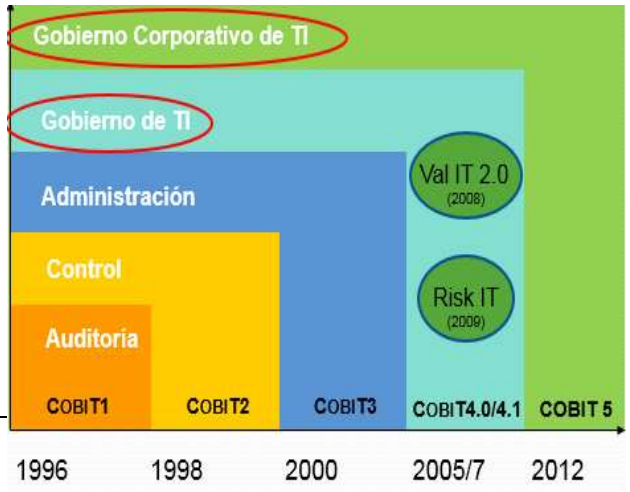
VII.- COBIT - OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS RELACIONADAS[1]

Control Objectives for Information and related Technology. Es un modelo internacional desarrollado por ISACA (Information Systems Audit and Control Association), y el ITGI (IT Governance Institute), es un conjunto de buenas prácticas para la administración y control de las tecnologías de información.

La primera edición de COBIT fue publicada en 1996, la segunda edición en 1998, la tercera edición en el 2000 y el 2003 la versión en línea, la cuarta en diciembre del 2005 y en mayo del 2007 fue publicada 4.1. La quinta edición fue publicada en el año 2012.

Gráfico N. 2

Versiones De COBIT



[1] http//www.isaca.org/

Elaboración: Autores

Fuente: Datos de la Investigación.

COBIT 5 es un marco referencial reconocido internacionalmente que lo utilizan las personas responsables de los procesos del negocio y del área de la tecnología para ayudar a las instituciones a crear un valor óptimo de las TI manteniendo el equilibrio en la realización de sus beneficios, la optimización de los niveles de riesgo y el uso de los recursos.

COBIT 5 es de carácter genérico y útil para las instituciones de todo tamaño sean estas comerciales, públicas o sin fines de lucro.

Beneficios de COBIT

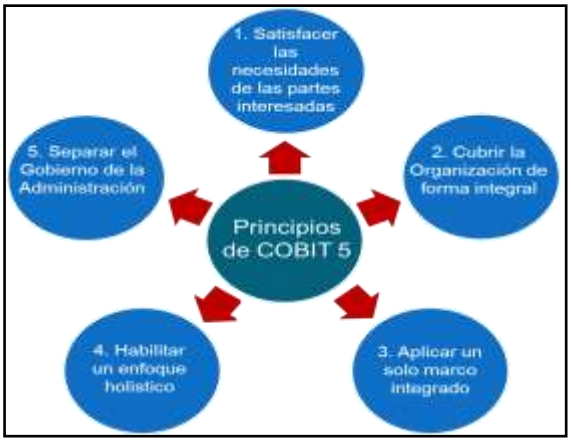
- Aumenta el valor de los objetivos a través un gobierno y gestión efectiva de los servicios tecnológicos. El enfoque del negocio aumenta en basado en las tecnologías de información.
- Satisfacción del usuario.
- Adoptan nuevos estándares.
- Productividad en el trabajo de los empleados para alcanzar los objetivos de la empresa.

Los principios y facilitadores de COBIT 5

Este estándar actúa sobre la base de los 5 principios y 7 facilitadores, COBIT 5 utiliza prácticas de gobierno y de gestión para describir acciones que son ejemplos de mejores prácticas.

Gráfico N. 3

Los 5 principios de COBIT 5



Elaboración: Autores
Fuente: Datos de la Investigación.

Los dominios considerados son los siguientes:

- **Políticas de la seguridad de la información:** Proporcionan orientación y sirven de soporte en la seguridad de información de acuerdo al propósito de la organización.
- **Organización de la Seguridad de la Información:** Busca dirigir la administración de la seguridad de la entidad, así como el mantenimiento de la infraestructura de procesamiento y de los activos que son manejados por terceros.
- **Seguridad en Recursos Humanos:** Se encuentra orientado a minimizar los errores humanos, ya que el usuario es considerado como una de las partes más vulnerables.
- **Gestión de Activos:** Ayuda a cuidar los activos que contengan información, controlando el acceso y solo permitir el acceso a los usuarios autorizados.
- **Control de Acceso:** Cuidar el acceso a la información de usuarios no autorizados.
- **Criptografía:** Protege la confidencialidad, integridad y disponibilidad de la seguridad de la información.

- **Seguridad Física y Ambiental:** Advierte del acceso no autorizado a las instalaciones para evitar posibles pérdidas, daños o robo de información.
- **Seguridad Operacional:** Asegura la operación correcta y segura en el procesamiento de seguridad de información.
- **Seguridad en las comunicaciones:** Busca asegurar la seguridad cuando la información se transfiere a través de las redes, para evitar pérdida, modificación o mal uso de la información.
- **Adquisición, desarrollo y mantenimiento de los sistemas de información:** Garantizar la seguridad de los Sistema Operativo, que los proyectos de TI y el soporte se den de manera confiable.
- **Gestión de la continuidad del negocio:** Busca disminuir las interrupciones de las actividades y proteger las partes más crítica para que esté disponible cuando se la requiera por causa de fallas o desastres.

Consideramos tres dominios los cuales se adaptan a los alcances de la organización que son necesarios para la seguridad de la información de la institución, entre ellos se encuentran:

05. Política de Seguridad

Documento de política de seguridad y su gestión.

09. Seguridad Física y del Entorno

Áreas seguras.

Perímetro de seguridad física.

Controles físicos de entrada.

Protección contra amenazas externas y del entorno.

Seguridad de los equipos.

Instalación y protección de equipos.

Suministro eléctrico.

Seguridad del cableado.

Mantenimiento de equipos.

11. Control de Acceso

Requisitos de negocio para el control de accesos.

Gestión de acceso de usuario.

Responsabilidades del usuario.

Control de acceso en red

VIII.- HARDENING COMO TÉCNICA DE LA SEGURIDAD INFORMÁTICA[2].

El término en inglés Hardening se podría traducir como endurecimiento, fortalecimiento y robustecimiento.

Es el proceso de fortalecer los sistemas informáticos compuesto por un conjunto de actividades que realiza el administrador para la reducción de vulnerabilidades en el mismo, esto se consigue descartando software, servicios, usuarios innecesarios y también cerrando los puertos que no se está utilizando para facilitar la administración y control.

Gráfico N. 4

Hardening de los Sistemas

[2] http://www.magazcitum.com.

Elaboración: Autores

Fuente: http://www.caberseg.es/detalle.php?nid=29

Es una tarea necesaria que tiene la finalidad de proteger la confidencialidad, disponibilidad e integridad de la información almacenada en los activos tecnológicos de la entidad.

> **Indica que toda organización debería contar con una línea base de seguridad para sus equipos productivos, la cual los lleve a un nivel mínimo satisfactorio de seguridad a través de un proceso de hardening. Un análisis de vulnerabilidades, por su parte, tiene como objetivo identificar huecos de seguridad y medir el impacto sobre los activos, y utiliza los hallazgos para visualizar cuáles serían las siguientes acciones para fortalecerlos y puedan soportar ataques a los que podrían estar expuestos.** (Sánchez , 2013)

- **Objetivos de Hardening en los sistemas informáticos:**

- Reducir las posibles vulnerabilidades de un sistema.
- Mejorar la seguridad frente a amenazas internas y externas.
- Disminuir los riesgos relacionados con fraude y error humano.
- Identificar problemas en los sistemas informáticos de manera rápida.

El proceso de hardening tiene que considerar diferentes niveles de fortalecimiento a:

Fortalecimiento a nivel de host

Incluye el sistema operativo y las aplicaciones locales que se ejecuta en los equipos. Considera el fortalecimiento de:

- Funciones y roles de cada usuario.
- Registro de auditoría.

- Privilegios de usuarios.
- Aplicaciones.
- Actualizaciones Instaladas.

Fortalecimiento a nivel de servicios de red

Se refiere a los servicios que tienen acceso a la red interna. Considera el fortalecimiento de:

- La seguridad local (firewalls).
- Las configuraciones de seguridad.

Fortalecimiento a nivel de perímetro

Comprende los flujos de información de entrada y salida a un equipo y puede incluir:

- La segmentación de red.
- El monitoreo de tráfico.
- Los dispositivos de seguridad (firewall).

Sistemas Informáticos en los que se aplica Hardening

- Windows Desktop
- Windows Server
- Router y Switches
- MYSQL Database
- UNIX Server
- Linux

Actividades de un proceso de Hardening

- Protección a ataques físicos (Seguridad del Hardware).
- Aplicar esquemas de seguridad, DMZ, Router apantallados, proxys, Firewalls.

- Seguridad del sistema (Antivirus, antimalware entre otros).
- Sistemas de detección de Intrusos (IDS, IPS, HIDS, NIDS).
- Configuración de protocolos, puertos y servicios (Solo los necesarios).
- Administrar cuentas de usuario, políticas del sistema, ACL. y filtrados.
- Restringir la instalación de Software y Hardware de acuerdo a las políticas de seguridad.
- Realizar la actualización de Firmware
- Prohibir el acceso de unidades externas en servidores (pen drive o memorias USB, unidades de Cd/DVD).
- Proteger las consolas de administración, terminales virtuales y accesos remotos.
- Paquetes de instalación, parches, upgrades, updates, módulos instalables, integridad de archivos y permisos en el sistema.
- Políticas de respaldo.

VI. - ANÁLISIS LEGAL:

CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR

Título II: Derechos

Capítulo segundo: Derechos del buen vivir

Sección tercera: Comunicación e Información

Art. 16.- Todas las personas, en forma individual o colectiva, tienen derecho a:

2. El acceso universal a las tecnologías de información y comunicación.

TÍTULO VII: RÉGIMEN DEL BUEN VIVIR

Capítulo primero: Inclusión y equidad

Sección octava: Ciencia, tecnología, innovación y saberes ancestrales

Art. 385.- El sistema nacional de ciencia, tecnología, innovación y saberes ancestrales, en el marco del respeto al ambiente, la naturaleza, la vida, las culturas y la soberanía, tendrá como finalidad:

1. Generar, adaptar y difundir conocimientos científicos y tecnológicos.

2. Recuperar, fortalecer y potenciar los saberes ancestrales.

3. Desarrollar tecnologías e innovaciones que impulsen la producción nacional, eleven la eficiencia y productividad, mejoren la calidad de vida y contribuyan a la realización del buen vivir.

Art. 388.- El Estado destinará los recursos necesarios para la investigación científica, el desarrollo tecnológico, la innovación, la formación científica, la recuperación y desarrollo de saberes ancestrales y la difusión del conocimiento. Un porcentaje de estos recursos se destinará a financiar proyectos mediante fondos concursables. Las organizaciones que reciban fondos públicos estarán sujetas a la rendición de cuentas y al control estatal respectivo.

REGLAMENTO PARA HOMOLOGACIÓN DE EQUIPOS DE TELECOMUNICACIONES

Capítulo IV

DE LA ELABORACIÓN DE NORMAS TÉCNICAS

Art. 17.- Reconocimiento de normas internacionales.- Si no se dispone de las normas técnicas, el CONATEL podrá adoptar normas internacionales

reconocidas por la UIT y a falta de éstas de otro organismo internacional reconocido por el CONATEL.

Capítulo VIII

ORGANISMOS Y ENTIDADES RECONOCIDOS

Art. 26.- Organismos y entidades reconocidos.- Son válidas las especificaciones técnicas, certificados o documentos de los siguientes organismos: Unión Internacional de Telecomunicaciones (UIT), Federal Communications Commission (FCC), European Telecommunications Standard Institute (ETSI), The Certification and Engineering Bureau of Industry of Canadá (CEBIC), Telecomunications Industries Association (TIA), Electronic Industries Alliance (EIA), Cellular Telephone Industry Association (CTIA), Unión Europea (UE), Comunidad Económica Europea (CEE), Deutsches Institut für Normung (DIN), British Standards Institution (BSI), Ente Nazionale Italiano di Unificazione (UNI), Association Francaise de Normalisation (AFNOR), International Electrotechnical Commission (IEC), Industrial Standards Committee Pan American Standards Commission (COPANT), The African Organization for Standardization (ARSO), The Arab Industrial Development and Mining Organization (AIDMO), Korean Agency for Technology and Standards (KATS), European Committee for Standardization, Standardization Administration of China, Hermon Laboratories y otros que el CONATEL los reconozca.

Norma ISO 27000.- Gestión de la Seguridad de la Información.

Es un conjunto de normas para la seguridad de la información, utilizada por cualquier tipo de organización. Fue publicada por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).

Proporciona información previa de la seguridad de la información y tiene una gama de normas que ayudarán a la organización a gestionar la seguridad de los activos, la propiedad intelectual, documentación financiera entre otros.

Norma ISO 27001.- Especificaciones para un sistema de gestión de seguridad de la Información.

Esta norma define los requerimientos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información.

La certificación en ISO 27001 es posible bajo el esquema de cada país, es la más importante de la familia 27000; se basa en la gestión de riesgos y el mejoramiento continuo de los procesos, el tiempo necesario de implantación es de 6 meses a 1 año, dependiendo del grado de madurez en seguridad de la información.

Algunas organizaciones adoptan esta norma con la finalidad de aprovechar las buenas prácticas que esta norma ofrece, aunque en otro caso quieren tener la certificación para tranquilizar a sus clientes.

Según esta norma que es la primera de la familia 27000, la seguridad de la información es cuidar la confidencialidad, integridad, y disponibilidad de los datos para su buen uso.

Procedimientos para la certificación de ISO 27001.

- Una vez aplicada el SGSI en la entidad se debe demostrar la efectividad 3 meses aproximadamente, para luego pasar a la siguiente fase que es la de auditoria y certificación, en la que se realiza lo siguiente:

- Los interesados deben realizar una solicitud de auditoria a la entidad de certificación.
- La entidad de certificación emitirá una respuesta donde se pondrán de acuerdo en el precio y el tiempo que se supone será evaluado.
- Se debe conocer a las personas responsables encargadas de realizar la auditoria para determinar el plan de trabajo que se llevara a cabo.
- Se deben realizar auditorías internas que aporten información sobre la situación actual y así no tener problemas para superar la auditoria real.
- **Fase 1:** Revisión del nivel de preparación de la organización
- **Fase 2:** Es la fase en la que se revisa a detalle políticas, implantación, y eficacia del sistema.
- Se obtiene la certificación con un periodo de 3 años aproximadamente. En caso de que exista inconvenientes para continuar con la auditoria los interesados deben presentar un plan de acciones correctivas y una vez verificados se podrá emitir un informe el cual puede ser favorable o no dependiendo de la magnitud del inconveniente.
- Se debe realizar auditorías de seguimiento cada 6 meses o 1 año aproximadamente para verificar el mantenimiento y la mejora continua.

Norma ISO 27002 – Código de buenas prácticas.

Su objetivo fundamental es ayudar a mejorar la gestión de la seguridad de la información, así como el desarrollo de nuevos mecanismos de control,

que pueden ser implementados dentro de una entidad, siguiendo la norma de ISO 27001.

Esta norma sirve de guía de buenas prácticas para la ejecución de los controles de seguridad y de las prácticas más eficaces para gestionar la seguridad de la información, pueden ayudar a incrementar su efectividad.

CONCLUSIONES

La seguridad física del centro de datos puede ser vulnerada con facilidad, por tal motivo es necesario la implementación de una puerta metálica que incluya control de acceso al personal mediante el uso de claves, además la instalación de cámaras de vigilancia al interior y fuera del lugar, lo que permite el control y monitoreo de este.

Mediante la instalación de un equipo firewall se podrá filtrar el tráfico e implementar las reglas necesarias para resguardar la red y así evitar los accesos no permitidos, ya que actualmente esta función se lo realiza a través de la interfaz del router mikrotik.

Los respaldos de los servidores se realizan diariamente al finalizar las labores de trabajo, son almacenados en un equipo NAS y las configuraciones de los equipos están archivadas en documentos físicos en el centro de datos. Además no existe copia de seguridad de estos archivos y configuración en otro lugar.

Existe la necesidad de crear políticas internas de seguridad los más clara posible y en lenguaje no técnico para trasmitir conciencia de seguridad a toda la organización y sobre el nivel de importancia que tienen sus activos informáticos. Por tal razón las medidas de seguridad consideradas en este proyecto son tomadas de las consideraciones de normas ISO, entre otras.

RECOMENDACIONES

La aplicación de estándares internacionales permitirá que el centro de datos pueda mejorar de manera contínua, por tanto se debe impulsar el uso de las mismas para la reestructuración de su infraestructura, pues su adecuado dimensionamiento y nivel de disponibilidad ayudará a que la institución puedan prestar nuevos y mejores servicios a sus usuarios internos y externos.

Se recomienda acondicionar el cuarto asignado para los servidores, equipos de almacenamiento de datos y equipos activos de la red, ya que está área debe garantizar el correcto funcionamiento de los sistemas, lo que involucra una correcta iluminación, climatización, control de acceso, vigilancia, sistema de detección y extinción de incendios. Además en este cuarto no deben existir ventanas en su interior, porque puede ingresar aire, polvo u otras partículas que afectan a la integridad de los equipos.

La carga de trabajo que soportan los servidores es constante durante el día, y la tendencia actual es ser cada vez más eficientes y escalables; en consecuencia, se debe promover el cambio a equipos que administren de manera eficiente el consumo de energía y virtualización de servidores. Por tal motivo, se recomienda un servidor con tecnología Blade, ya que en un solo equipo se tienen más opciones de

almacenamiento, capacidad de expansión y un procesamiento más potente para satisfacer cualquier necesidad de carga de trabajo.

El centro de datos deberá contar con sistema puesta a tierra para limitar la sobretensión eléctrica durante el funcionamiento de los equipos y así prevenir que las personas no perciban afectaciones ante una descarga eléctrica en caso de falla del equipo. Además se recomienda contar con un sistema de energía ininterrumpida (UPS) como respaldo del suministro eléctrico que se active una vez que se produzca un corte o fallo eléctrico.

BIBLIOGRAFÍA

LIBROS

- Aguilera, P. (2010). Seguridad Informatica (Vol. Entorno Fisico).Madrid: Editex.
- Arias , F. (2012). El proyecto de Investigación . Caracas : Episteme.
- Fonseca Luna, O. (2011). Sistema de Control Interno para Organizaciones. Lima: IICO.
- Taborda, C., Escobar, L., & Torres, C. (2011). Auditorias Especificas DATACENTER. Colombia Manizales.
- Vara Horna, A. (2012). 7 pasos para una tesis exitosa. Lima.

TESIS

- Briones , C. (2010). Diseño del centro de datos del Banco Central del Ecuador, sucursal Cuenca. Cuenca: s.n. Obtenido de http://dspace.ucuenca.edu.ec/handle/123456789/664
- Buestán, J. R. (2014). Análisis y propuestas de criterios técnicos para diseño de cableado estructurado en proyecto de reestructuración de redes de datos y servidios agregados. Cuenca: s.n.
- Cadme, C. M., & Duque, D. F. (2011). Auditoría de Seguridad Informática ISO 27001 para la empresa de alimentos "ITALIMENTOS CIA.LTDA". Cuenca: s.n. Obtenido de http://dspace.ups.edu.ec/bitstream/123456789/2644/16/UPS-CT002441.pdf
- Córdova , D. C. (2012). Data Center para mejorar la infraestructura de comunicaciones de datos en el departamento de sistemas informaticos y redes de comunicación (DISIR) de la Universidad Técnica de Ambato. Ambato: s.n. Obtenido de http://repo.uta.edu.ec/bitstream/123456789/2379/1/Tesis_t729si.pdf
- Guambuguete , E. X. (2012). Diseño de la infraestructura de comunicaciones de voz, datos y video para el PPA (Programa dee Provisión de Alimentos). Quito. Obtenido de http://bibdigital.epn.edu.ec/handle/15000/4460
- Joskowicz, J. (2013). Cableado estructurado. Montevideo: s.n. Obtenido de http://iie.fing.edu.uy/ense/asign/ccu/material/docs/Cableado%20Estructurado.pdf
- Maldonado, J. (2010). Diseño de un centro de datos basado en estándares caso práctico: Diseño de Centro de Datos del colegio Latinamericano (258 ed.). Cuenca: s.n. Obtenido de

http://dspace.ucuenca.edu.ec/handle/123456789/648

- Miño , P. A., & Muñoz , L. C. (2014). Estudio y diseño de una Red de Infraestructura Multiservicios para el Gobierno Autónomo Descentralizado Municipal de “San Pedro de Huaca” y sus Dependencias. Quito, Ecuador : s.n. Obtenido de http://bibdigital.epn.edu.ec/handle/15000/7392

- Paltán, H. (2013). El desarrollo de estándares y procedimientos para la creación de un data center en la UPSE. Libertad, Santa Elena , Ecuador: s.n.

- Polo, L. N. (2012). Diseño de un data center para el ISP READYNET CIA.LTDA fundamentado en la norma ANSI/TIA/EIA-942. Quito: s.n. Obtenido de http://bibdigital.epn.edu.ec/handle/15000/5431

- Rubio , J. E. (2012). Análisis y diseño de un Data Center en base a los estándares Ansi/Eia/Tia 606, 607 y 942 para el edificio de la Dirección Provincial de Salud de Pichincha. Quito, Ecuador: s.n. Obtenido de http://dspace.ups.edu.ec/handle/123456789/3537

- Sangoluisa, D. P. (2015). Definición de las políticas de seguridad de la información para la red convergente de la presidencia de la república del Ecuador basado en las normas ISO 27000. Quito: s.n. Obtenido de http://bibdigital.epn.edu.ec/handle/15000/11462

- Villegas , J. A. (2013). Optimización de la administración de la red e implementación de servidores de servicio para el Gobierno Provincial de Imbabura. Ibarra, Ecuador: s.n. Obtenido de http://repositorio.utn.edu.ec/handle/123456789/1928

- Yaselga, E. H. (2013). Diseño del Centro de Datos para PETROECUADOR en el Edificio Matriz en Base al Estándar TIA-942-

2. Quito: s.n . Obtenido de http://bibdigital.epn.edu.ec/handle/15000/6426

REVISTAS DE INTERNET

- Cofitel Anduino. (14 de febrero de 2014). Grupo Cofitel. Obtenido de http://www.c3comunicaciones.es/data-center-el-estandar-tia-942/
- Computerworld México. (1 de marzo de 2012). Mexicopcworld. Obtenido de http://www.pcworld.com.mx/Articulos/21733.htm
- Sánchez , E. (13 de 06 de 2013). magazcitum. Obtenido de http://www.magazcitum.com.mx/

SITIOS WEB

- http://www.pedrocarbo.gob.ec
- http://www.ansi.org/
- http://www.tiaonline.org/
- http://www.nfpa.org/
- http://www.iso.org/
- http://www.pinturascondor.com
- http://www.acimco.com/
- http://www.firmesa.com/