FORMULACIÓN DE UNA GUÍA DE AUDITORIA PARA LA INFRAESTRUCTURA FÍSICA DE LOS CENTROS DE DATOS DE LAS ENTIDADES PÚBLICAS DEL ECUADOR

Christian Llerena
Departamento de Gestión de Infraestructura; Contraloría General del Estado
cllerena@contraloria.gob.ec

RESUMEN.

En los últimos años el auge de los servicios tecnológicos y procesos automatizados que se realizan en las diferentes entidades públicas del Ecuador ha provocado una innegable necesidad en los departamentos de Tecnología de la Información de las mismas, de mantener disponibles dichos servicios y proteger adecuadamente la información que se almacena y procesa en todos los equipos que se utilizan para este fin. Ante esto se encuentra la creciente demanda de mitigar cualquier riesgo que pueda ocasionar la pérdida o la indisponibilidad de la información, entre estos riesgos se encuentra la evidente posibilidad de que ocurra una falla en la infraestructura física del lugar en el que se encuentran alojados los dispositivos encargados de prestar los servicios de Tecnología de la Información, pudiendo ser una falla de tipo eléctrica, un sobrecalentamiento de los equipos o cualquier otro tipo de falla en los servicios externos o en la infraestructura propia del Centro de Datos. Por tal motivo, es de suma importancia realizar la verificación de los componentes de la infraestructura física de los Centros de Datos para evitar o minimizar la posibilidad de que un fallo en alguno de ellos produzca interrupciones en los servicios que brindan las unidades de Tecnología de la Información de las entidades del sector público del Ecuador, por lo que es de vital importancia para el Auditor Informático de la Contraloría General del Estado contar con una Guía de Auditoría, que le permita la revisión de dicha infraestructura de una manera eficiente y con el propósito de generar las debidas recomendaciones que garanticen que el Centro de Datos auditado este en capacidad de garantizar la disponibilidad de los servicios tecnológicos.

Palabras claves: servicios de Tecnología de la Información, Centro de Datos, disponibilidad, Guía de Auditoría

ABSTRACT.

In recent years the rise of technology services and automated processes that are performed in different public entities in Ecuador has caused an undeniable necessity in their departments of Information Technology, to keep available the services and adequately protect information that is stored and processed on all machines that are used for this purpose. Given this, there is an increasing demand to mitigate any risks that may result in the loss or unavailability of information, among these risks is the obvious possibility that a failure occurs in the physical infrastructure of the place in which devices that are responsible for providing Information Technology services are housed, can be an electric failure type, overheating of equipment or any other failure in the external services or data center itself infrastructure. For this reasons, it is very important to perform the verification of the components of the physical infrastructure of data centers to avoid or minimize the possibility that a fault in any of them produce interruptions in services offered by Information Technology units of Ecuador´ public sector entities, so it is

vitally important for the IT Auditors of the Comptroller General Office to have an Audit Guide, which allows the review of that infrastructure in an efficient manner and for the purpose of generate appropriate recommendations to ensure that the audited data center is able to guarantee the availability of technology services.

Keywords: Information Technology services, Data Center, Availability, Audit Guide.

I. Introducción

Mantener operativos los servicios de Tecnologías de la Información (TI) así como preservar, procesar y administrar eficientemente la información que se encuentra en los Centros de Datos o, Data Center, constituye uno de los retos más importantes que deben enfrentar los departamentos de TI, siendo la infraestructura física del Centro de Datos, que incluye el acondicionamiento eléctrico, mecánico, de telecomunicaciones, seguridad y diseño del mismo, un factor de suma importancia que influye en la tarea de garantizar la disponibilidad de la información y la continuidad de las operaciones.

En este contexto, la presente trabajo se enmarca en la formulación de una Guía para auditar la infraestructura física de los Centros de Datos de las entidades públicas del Ecuador, la misma que será utilizada por los auditores de la Dirección de Auditoría de Tecnología de la Información de la Contraloría General del Estado y tiene como objetivo evaluar las instalaciones e infraestructura física de los Centros de Datos, con el uso de adaptaciones sugeridas en los marcos de referencia, estándares internacionales y buenas practicas relacionadas a mantener la continuidad de las operaciones de tecnología de la información.

Como paso preliminar, y debido a que cada una de las entidades públicas del Ecuador tiene diferentes objetivos, así como misión y visión distintas, se considera de suma importancia que el Auditor realice un análisis del impacto que tiene la Tecnología de la Información en la entidad auditada para deducir el nivel de disponibilidad que debe tener su respectivo Centro de Datos. Para esto primeramente se elaborará un cuestionario, que tiene por objeto analizar la criticidad e impacto que representan los servicios de TI dentro de la entidad, el mismo que será desarrollado con las directrices de las principales normas y buenas prácticas de gestión de servicios tecnológicos y de gobierno de tecnología de la información. El resultado de este cuestionario permite determinar el impacto de TI dentro de cualquier entidad y por ende se desprende el nivel de disponibilidad requerido para el Centro de Datos, posteriormente realiza el análisis de los riesgos presentes en un Centro de Datos y finalmente se evaluará la infraestructura física con los parámetros establecidos en los marcos de referencia relacionados y que serán analizados para la formulación de la Guía.

Es así que la Guía constituye una herramienta que permite realizar todo el proceso de auditoría, del cual se obtendrá el respectivo nivel de madurez del Centro de Datos auditado, a partir del cual formularán las debidas conclusiones y recomendaciones que servirán para asegurar que su infraestructura física se encuentre en condiciones óptimas para asegurar la continuidad de las operaciones de la entidad y proteger los valiosos activos que se encuentran hospedados en el mismo.

II. Metodología

La metodología analítica, con la cual se han identificado los principales marcos de referencia que permitirán la elaboración de la Guía de Auditoría para la Infraestructura física de los Centros de

Datos dan lugar al establecimiento de tres fases, para de esta manera brindar las pautas necesarias que el Auditor necesita con el propósito de realizar el proceso de evaluación de un Centro de Datos perteneciente a cualquier entidad del sector público del Ecuador. Cabe indicar que basado en el cumplimiento de las Normas de Control Interno que rigen el sector público del Ecuador, el auditor basará sus recomendaciones citando el cumplimiento del subgrupo 410-10 Seguridad de tecnología de información, que dispone a las unidades de TI la gestión de "Instalaciones físicas adecuadas que incluyan mecanismos, dispositivos y equipo especializado para monitorear y controlar fuego, mantener ambiente con temperatura y humedad relativa del aire contralado, disponer de energía acondicionada, esto es estabilizada y polarizada, entre otros;". Es así que para la formulación de la Guía de Auditoría, se establecieron las siguientes fases:

- Guía para obtener el Nivel de Disponibilidad requerido en un Centro de Datos
- Guía para el Análisis de Riesgos en un Centro de Datos
- Guía para auditar un Centro de Datos

II.1. Guía para obtener el Nivel de Disponibilidad requerido en un Centro de Datos

El procedimiento a seguir para determinar el Nivel de Disponibilidad requerido en un Centro de Datos consiste primeramente en realizar una serie de preguntas al Administrador del Centro de Datos a ser auditado, este cuestionario de 25 preguntas que será utilizado por el Auditor Informático, se ha definido mediante las directrices del modelo denominado Análisis de Impacto al Negocio, el mismo que es parte fundamental de la norma ISO 22301 – Sistemas de Gestión de la Continuidad del Negocio, y que básicamente está orientado a identificar los procesos críticos del negocio, considerando aspectos como: procesos críticos de sistemas, dependencias de la entidad, impacto sobre las operaciones y los tiempos de recuperación óptimos para los procesos críticos. Adicionalmente es necesario complementar y fortalecer el cuestionario planteado mediante el uso de los lineamientos de Cobit (Control Objectives for Information and Related Technology), que es un marco de gobierno de TI, basado en controles y que organiza las actividades de TI en 34 procesos con sus respectivas métricas. Es decir, en base a los lineamientos del Análisis de Impacto al Negocio y tomando en cuenta las métricas propuestas en Cobit se ha formulado un cuestionario, con su respectivo criterio de evaluación para cada una de las preguntas, lo cual dará como resultado el Nivel de Disponibilidad requerido en el Centro de Datos.

Entre las preguntas que forman parte del cuestionario planteado se toma como ejemplo las siguientes:

- ¿Frecuencia en la que se realizan los procesos de Tecnología?
- ¿Los procesos críticos de TI se realizan en línea?

Con el criterio de evaluación definido en la guía, el auditor procede a ponderar las respuestas obtenidas, como ejemplo con la pregunta relacionada a la frecuencia en la que se realizan los procesos de tecnología, se han definido cuatro posibles respuestas: mensual, semanal, 8x5 y 24x7; la ponderación implica asignar el valor de 1 si la respuesta es mensual, 2 si es semanal, 3 si es 8x5 y 4 si es 24x7. En relación a la segunda pregunta de este ejemplo, se considera una ponderación de 1 si la respuesta es NO y 4 si la respuesta es SI.

Una vez que el Auditor ha completado la evaluación de las respuestas obtenidas a las 25 preguntas del cuestionario, estará en capacidad de determinar el nivel de disponibilidad requerido en el Centro de Datos, en base al criterio que se muestra en la siguiente tabla:

Puntaje obtenido	Disponibilidad requerida
Hasta 50	Baja
Entre 51 y 75	Media
Entre 76 y 90	Alta
Mayor a 90	Muy Alta

Tabla 1. Disponibilidad requerida según puntaje obtenido en el cuestionario

En conclusión se determina que el impacto y criticidad de los procesos de Tecnología de la Información están directamente relacionados con la Disponibilidad requerida en el Centro de Datos.

También es necesario considerar otra herramienta para determinar el nivel de disponibilidad requerido, la misma que se basa en la publicación realizada por el Uptime Institute, que es una organización conocida mundialmente por el desarrollo de la clasificación de los Centros de Datos según su disponibilidad en categorías denominadas TIER, y en la cual determina dicha categorización según el negocio u objetivos de las organizaciones, estableciendo 4 categorías TIER, el nivel 1 para menor disponibilidad y 4 para la máxima disponibilidad. Con estos antecedentes determina la orientación de cada una de sus categorías:

- TIER 1: pequeñas empresas sin presencia en la web, que pueden optar por centro de datos externo.
- TIER 2: empresas que comúnmente requieren de los servicios de TI en horario laborable, o sus objetivos son a largo plazo.
- TIER 3: empresas que dan servicios a clientes internos y externos 24 x 7 en varias zonas horarias y distintas regiones.
- TIER 4: empresas que requieren presencia internacional todo el año, proveedores de internet o servicios de Data Center.

Con estas herramientas el Auditor está en capacidad de determinar el nivel de disponibilidad requerido en un Centro de Datos, y procederá a realizar el Análisis de Riesgos, ya que el este análisis es necesario conocer los activos (hardware) que existen en el Centro de Datos.

II.2. Guía para el Análisis de Riesgos en un Centro de Datos

La realización del Análisis de Riesgos permitirá identificar los principales riesgos a los que están expuestos los activos en relación directa con la infraestructura física de los Centros de Datos. Existen varias metodologías para realizar el Análisis de Riesgos, tales como Magerit, Octave, etc., en los cuales se definen las fases para determinar el riesgo en base al impacto y probabilidad.

El procedimiento para realizar el análisis de riesgos consiste en varios pasos tal como se describe a continuación:

- Identificación de Activos: permite identificar los activos que se encuentran dentro del Centro de Datos y que serán recopilados por el Auditor.

- Tasación de Activos: consiste en asignar un grado de valor, según la importancia que representa que se encuentre disponible dicho activo para los objetivos de la entidad, basado en la Disponibilidad, el Auditor dará un valor en la escala de 1 a 5.
- Identificación de las Amenazas y Vulnerabilidades: se identifican las amenazas y vulnerabilidades de tipo físico presentes en un Centro de Datos.

N°	Amenazas
1	Temperatura
2	Humedad
3	Fugas de líquidos o agua
4	Falta de refrigeración y falla de circulación de aire
5	Error humano y acceso del personal
6	Humo, Incendios
7	Pérdida de energía

Tabla 2. Amenazas al Entorno Físico de un Centro de Datos

Dentro de las vulnerabilidades se pueden citar las siguientes:

- Falla en los sistemas de Aire Acondicionado
- Falla o ruptura de las tuberías o desagües cercanos
- Falla en el diseño arquitectónico
- Falla en la distribución del aire
- Falla en los dispositivos de seguridad de acceso
- Falla en el suministro eléctrico
- Falla en los ups o generador eléctrico
- Acceso de personal no autorizado
- Falla del sistema contra incendios

- Con las amenazas y vulnerabilidades definidas se procede a calcular la probabilidad de la amenaza, para lo cual se utiliza un cuestionario basado en las vulnerabilidades presentes y que permiten detectar si el Centro de Datos está siendo correctamente protegido ante las mismas. Entre las preguntas que forman parte del cuestionario se puede mencionar la siguiente: ¿Se realiza periódicamente el mantenimiento del Sistema de aire acondicionado?
  El criterio para valorar la probabilidad es asignando un puntaje según la respuesta, es decir si la respuesta es SI=0, NO=2, Parcial=1, para obtener las respuestas el auditor utilizará el método de la entrevista o de la inspección física del Centro de Datos. El resultado del valor total obtenido para cada amenaza en términos de probabilidad, se especifica en la siguiente tabla:

Valor	Significado
0	Muy bajo
1	Bajo
2	Medio
3	Alto
4	Muy alto

Tabla 3. Valoración de la Probabilidad de Amenaza

- Una vez que se ha determinado el proceso para obtener el impacto de cada uno de los activos y la probabilidad que tiene cada una de las amenazas se procede a realizar la Evaluación de Riesgos, el mismo que se obtiene con la fórmula Riesgo=Probabilidad x Impacto.

MATRIZ DE RIESGOS		Temperatura	Humedad	Fugas de agua	Falta de refrigeración y falla de circulación de aire	Error humano y acceso del personal	Humo, Incendios	Pérdida de energía
Probabilidad de la Amenaza								
Activo	Impacto	Cálculo de Riesgos de los Activos						

Tabla 4. Matriz de Riesgos

De este modo se han obtenido los riesgos que tienen los activos en relación a la infraestructura física y se puede determinar la prioridad de cada uno de ellos.

Una vez que el auditor ha identificado los activos que tienen alto riesgo de sufrir alguna falla asociada a las amenazas que existen en la Infraestructura Física del Centro de Datos, es menester tomar las medidas correspondientes para mitigar el riesgo, para esto se utilizará el estándar principal en el diseño e implementación de Centros de Datos que es el estándar TIA 942, ya que el mismo contiene los lineamientos que ayudan a garantizar que la Infraestructura Física proteja correctamente a los activos que se encuentran en el Centro de Datos.

II.3. Guía para auditar un Centro de Datos

Con la clasificación ideada por el Uptime Institute que se plasma en el estándar TIA 942, y que se utilizará en la Guía de Auditoría para evaluar los Centros de Datos, se procede a elaborar las especificaciones mínimas que debe cumplir el Centro de Datos de conformidad al análisis respectivo del estándar con el cual se ha establecido un grupo de requerimientos generales para todos los Centros de Datos y un grupo de requerimientos específicos según la disponibilidad requerida obtenida previamente, con lo cual el auditor procederá a verificar la infraestructura física y según el caso realizará las pruebas necesarias para determinar el cumplimiento de los requerimientos de cada uno de ellos.

Estándar TIA 942	Guía de Auditoría	Disponibilidad Requerida
Tier I	Centro de Datos TIPO I	Baja
Tier II	Centro de Datos TIPO II	Media
Tier III	Centro de Datos TIPO III	Alta
Tier IV	Centro de Datos TIPO IV	Muy Alta

Tabla 5. Definición de Tipos de Centro de Datos para la Guía de Auditoría

Con las directrices del estándar se procede a establecer un grupo de requerimientos generales para todos los Centros de Datos, independiente del nivel de disponibilidad requerido.

REQUERIMIENTOS GENERALES
El administrador del Centro de Datos dispone de un estudio de la carga del suelo
Existen espacios libres a los lados de los equipos que se encuentran en el cuarto de equipos
¿Se constata que existe un correcto flujo del aire al verificar la ubicación de las bandejas de cables dentro del piso elevado?
¿Existen estudios eléctricos que determinen la correcta alimentación de corriente hacia los equipos?
¿Están los equipos situados lejos de fuentes de interferencia electromagnética?
El cuarto de equipos no debe tener ventanas al exterior.
El cuarto de equipos debe contar con puertas que faciliten el acceso sólo al personal autorizado
Se permite el hospedaje en el cuarto de equipos de los equipos de control eléctrico, tales como distribución de energía o sistemas acondicionamiento y UPS hasta 100 kVA
Los pisos, paredes y techos deberán ser sellados, pintados o construidos de un material para minimizar el polvo. Los acabados deben ser de color claro para mejorar la iluminación de la habitación y los pisos deben tener propiedades anti- estáticas.
Las luminarias no deben ser alimentadas desde el mismo panel de distribución eléctrica de los equipos de telecomunicaciones
Debe existir señalización de salidas y emergencia igual a las de todo el edificio
El sistema de climatización del cuarto de equipos debe ser soportado por el generador eléctrico del cuarto de equipos o generador del edificio

Tabla 6. Requerimientos generales de un Centro de Datos

Posterior a la evaluación de los requerimientos generales, el Auditor procederá a la revisión de los requerimientos específicos, para esto hará uso de las guías correspondientes, en las cuales se constata que existen mayores exigencias en la infraestructura física cuando la disponibilidad requerida es mayor. Para lograr el nivel de disponibilidad requerido, el estándar define niveles de redundancia en los componentes de la infraestructura, como se muestra en la tabla 7.

Redundancia	Necesidad de redundancia de la infraestructura
N	Requerimiento básico sin redundancia
N+1	Provee una módulo, unidad, vía o sistema adicional al requerimiento básico.
N+2	Provee dos módulos, unidades, vías o sistemas adicionales al requerimiento básico.
2 N	Provee dos unidades completas, vías o sistemas por cada uno de los requerimientos básicos.
2 (N+1)	Provee dos unidades completas, vías o sistemas de tipo N+1.

Tabla 7. Redundancia de la infraestructura

Una vez que el auditor, mediante la inspección del Centro de Datos ha verificado el cumplimiento de los requerimientos generales y específicos que planteados en la presente Guñia de Auditoría, procederá a la evaluación de los resultados obtenidos.

III. Evaluación de resultados y discusión

Los resultados son evaluados mediante el uso de un Modelo Genérico de Madurez, el mismo que consiste en desarrollar un método de asignación de puntos para calificar la infraestructura física del Centro de Datos en un parámetro que va desde Inexistente hasta Optimizada. Este modelo consta en Cobit y se basa en el modelo ideado por Software Engineering Institute, el mismo que fue orientado a la madurez de la capacidad del desarrollo de software y actualmente es aplicable a cualquier área de TI. Es así que se procede a determinar la cantidad de respuestas positivas del total de ítems evaluados en cada uno de los sub sistemas, siendo ese resultado el valor que permite obtener el porcentaje de cumplimiento. Es decir, si el sub sistema mecánico consta de 8 ítems a ser evaluados y el auditor constata la existencia de 4 de ellos, se determina que tiene un cumplimiento del 50%. Posteriormente el auditor se referirá a la tabla previamente definida de Nivel de Madurez en relación al porcentaje de cumplimiento, con la cual determinará el nivel de madurez del Centro de Datos.

Porcentaje de cumplimiento obtenido	Nivel de madurez
0-16	0
17-33	1
34-50	2
51-67	3
68-84	4
85-100	5

Tabla 8. Nivel de Madurez en relación al porcentaje de cumplimiento

Cabe indicar que el nivel obtenido puede ser representado gráficamente según se muestra en la figura 1. Es necesario indicar que el nivel ideal en este estudio es el nivel de madurez 5, en vista de que se propone alcanzar un nivel óptimo en la disponibilidad de los Centros de Datos a ser auditados mediante la implementación de los requerimientos que se solicitan en cada una de las Guías que se han elaborado en este trabajo.

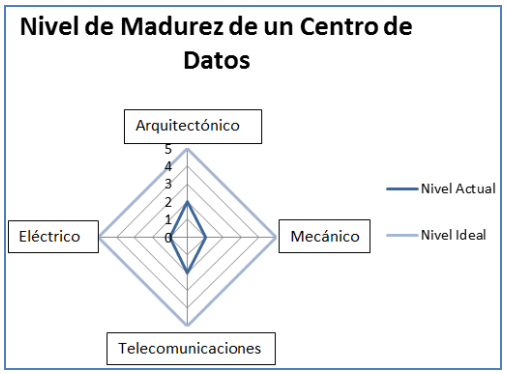

Figura 1. Nivel de Madurez de un Centro de Datos

En consecuencia es menester definir una definición que describa la condición que refleja cada uno de los niveles de madurez que se pueden obtener de la evaluación realizada:

Nivel	Definición
0	No Existente- Carencia de infraestructura física en el Centro de Datos que este alineada con algún estándar o buena práctica.
1	Inicial- Existe evidencia que la entidad ha reconocido la necesidad de alinear la Infraestructura física con algún estándar relacionado. Sin embargo dicha infraestructura no se encuentra correctamente organizada y no se han tomado medidas para mejorar dicha infraestructura.
2	Repetible- Se ha implementado una infraestructura física en el Centro de Datos según los lineamientos de algún estándar pero no existe una completa eficiencia en cada uno de los sub sistemas que forman parte de dicha infraestructura.
3	Definido- Toda la infraestructura física del Centro de Datos se encuentra organizada, sin embargo no todos los sub sistemas que forman parte de la infraestructura física cumplen con los requerimientos del estándar.
4	Administrado- La infraestructura física del Centro de Datos está alineada con el estándar y pueden existir umbrales que no presentan un nivel óptimo en su adecuación
5	Optimizado- Toda la infraestructura física se encuentra correctamente alineada con un estándar y con las mejores prácticas actuales.

Tabla 8. Definición de los niveles de madurez de la infraestructura física de un Centro de Datos

Los resultados obtenidos de la evaluación del Centro de Datos permiten que el Auditor Informático este en capacidad de recomendar el tipo de acciones a tomar en cada uno de los sub sistemas que forman parte de la Infraestructura Física de un Centro de Datos, para esto se debe referir a los ítems de cada sub sistema en los que las respuestas obtenidas en la evaluación han sido negativas y con base en esas premisas procede a recomendar la implementación o adecuación de la infraestructura física necesaria a fin de prever cualquier falla que puede afectar al Centro de Datos, cabe indicar que la tabla de requerimientos generales es de carácter mandatorio, por lo que el Auditor concluirá en el informe que se adopten las medidas necesarias para cumplir cada uno de los ítems que se muestran en dicha tabla.

IV. Trabajos relacionados

Durante el proceso de formulación de la Guía de Auditoría para la infraestructura física de un Centro de Datos, se ha constatado que existen varios métodos, técnicas y procedimientos que se han desarrollado para evaluar a un Centro de Dato específico, y que están orientados a verificar el cumplimiento del estándar TIA 942 u otras normas relacionadas con la infraestructura física de estos, sin embargo, no existe una guía ideada para evaluar a los Centros de Datos de las entidades públicas del Ecuador, ya que para realizar este tipo de auditoría primeramente se ha considerado que el auditor debe tener conocimiento de la naturaleza de la entidad y sus objetivos, es decir, los marcos de referencia de TI existentes proporcionan las directrices generales hacia cualquier tipo de organización, razón por la cual estas deben ser ajustadas y complementadas entre sí mediante un análisis de las mismas acorde a los objetivos que se pretenden alcanzar en la Guía propuesta. Partiendo desde los principales marcos de referencia de TI utilizados a nivel mundial hasta llegar a las normas principales de cumplimiento obligatorio en las entidades del sector público del Ecuador que son las Normas de Control Interno de la Contraloría General del Estado se ha definido una Guía de Auditoría fundamentada en varios de estos marcos de referencia de TI, y mediante las debidas adaptaciones, las mismas permiten que el proceso de evaluación de un Centro de Datos contenga un procedimiento organizado y definido.

V. Conclusiones y trabajo futuro

- Es necesario realizar Auditorías a los Centros de Datos de las entidades públicas del Ecuador ya que se ha evidenciado que las mismas contribuyen a mantener una adecuada infraestructura física del mismo, con el propósito de asegurar que los activos que se encuentran hospedados en este lugar estén correctamente protegidos ante los riesgos causados por las amenazas físicas que comprometen su normal funcionamiento.
- Existen varios marcos de referencia de TI que pueden ser aprovechados para la realización de una Guía de Auditoría, por lo que se ha utilizado varios estándares que fundamentan los procedimientos que se han diseñado para la realización de la evaluación de la infraestructura física de los Centros de Datos de cualquier entidad pública del Ecuador.
- Con la realización de una auditoría al Centro de Datos se apoya de gran manera a la tarea de garantizar la disponibilidad de los activos que son fundamentales para el desarrollo normal de las actividades y procesos tecnológicos que se desarrollan en cualquier entidad del sector público del Ecuador.
- Una adecuada infraestructura física en un Centro de Datos minimizará el riesgo de que factores como: fuego, sobre calentamiento de equipos, cortes de energía, fuga de agua, acceso de personal no autorizado, entre otros; paralicen o dañen los activos que procesan y generan información para la entidad y detengan sus operaciones.
- La ejecución de auditorías periódicamente permite asegurar que las entidades públicas del Ecuador estén en capacidad de mantener disponibles sus servicios de TI, siendo necesario también por parte de la Contraloría General del Estado, la conformación de equipos de auditoría multidisciplinarios para que se puedan verificar de mejor manera el cumplimiento de los requerimientos planteados en la presente Guía de Auditoría.

AGRADECIMIENTOS:

Mi más profundo agradecimiento a los profesores de la ESPE: Ing. Mario Ron MSc, Ing. Luis Escobar MSc y al Ing. Jairo Navarro, quienes con su apoyo han aportado en la elaboración de este proyecto.

Referencias Bibliográficas:

[1] Chamorro, V. (2013). Plan de Seguridad de la Información basado en el estándar ISO 13335. Quito.
[2] Eduardo, A. I. (2010). Desarrollo de una propuesta metodológica para la implementación de Dc. Esmeraldas, Ecuador.
[3] Figueroa, I. M. (2007). Departamento Académico de Informática - Unsaac. Obtenido de http://in.unsaac.edu.pe/
[4] Guagalango Ricard, M. P. (2011). Evaluación técnica de la seguridad informática del Data Center de la ESPE. Sangolquí.
[5] Institute, I. G. (2008). Alineando Cobit 4.1, ITIL v3 e ISO 27002 en beneficio de la empresa. Estados Unidos: ITGI.
[6] Isaca. (2007). www.isaca.org.
[7] Spera, C. (2012). Las claves en la administración de energía del Data Center. Logicalis Now, 13-14.