

Auditoría de gestión de seguridad informática, en entidades públicas y privadas en Loja

Carlos Miguel Jaramillo Castro, Luis Roberto Jácome Galarza, Ángel José Ordóñez Mendieta, María Esperanza Gaona, Jorge Tulio Carrión González, Mario Andrés Palma Jaramillo

Facultad de Energía, Universidad Nacional de Loja, Av. Pío Jaramillo Alvarado y Reinaldo Espinosa, La Argelia, Loja, Ecuador.

Autor para correspondencia: litosjc_21@hotmail.com

Fecha de recepción: 17 de mayo 2017 - Fecha de aceptación: 18 de agosto 2017

RESUMEN

Este documento exhibe información sobre normas, estándares y metodologías, utilizados para la gestión de seguridad de un Data Center y Red LAN. Para este trabajo se utilizó el estándar ANSI/TIA/EIA 942 y la norma ISO/IEC 27002, con metodología MAGERIT. Además, se desarrolló un cuadro comparativo, en donde se expone las ventajas y características que ofrece cada una, lo cual permite llegar a la conclusión del por qué aplicarlas. A continuación, se presenta el análisis y evaluación de los riesgos a los que está expuesto el Data Center y la red LAN de entidades públicas y privadas de la ciudad de Loja. La información se obtuvo mediante la aplicación de cuestionarios, entrevistas y formularios a cada persona responsable de las direcciones y subdirecciones tecnológicas, recabando información sobre 19 secciones tales como redes, servidores, etc., las mismas que se especificarán más adelante en el documento. Al finalizar el desarrollo del estudio, se realizó la socialización de los resultados obtenidos con las entidades auditadas, permitiendo con ello validar la evaluación y comunicar los resultados que se obtuvieron, como por ejemplo, la solución para la mitigación de los riesgos asociados a los activos de información, que son propiedad de dichas entidades.

Palabras clave: Activo informático, auditoría informática, gestión de riesgos, seguridades, ISO/IEC 27002, MAGERIT.

ABSTRACT

This paper presents the available information on norms, standards and methodologies used for the management of a Data Center and the security of LAN networks. A comparative table, depicting the advantages and features that each of them offers was developed, and the conclusions that encourage to apply them were formulated. To achieve this, we applied the 942 ANSI/TIA/EIA and ISO/IEC 27002 standards, and the MAGERIT methodology. The manuscript presents thereafter the analysis and evaluation of the risks the Data Center and the LAN networks of public and private entities from the city of Loja are exposed. The information thereto was obtained via the application of questionnaires, interviews and forms to each person responsible for the branches and sections of these institutions. The authors worked with a total of 19 sections. The obtained results were socialized with the audited entities allowing the validation and communication of the results, and the improvement of the mitigation of the risks associated with the information assets that are owned by surveyed entities.

Keywords: Computer asset, computer audit, risk management, securities, ISO/IEC 27002, MAGERIT.

1. INTRODUCCIÓN

Hoy en día, las instituciones públicas y privadas han experimentado grandes cambios tecnológicos, teniendo que implementar infraestructura tecnológica y física que les permita ofrecer a sus funcionarios, empleados e investigadores, la posibilidad de conectarse con el mundo, esto con el propósito de brindar una calidad de servicio óptima, con la capacidad de decisión, creatividad e innovación, y de esta manera mejorar sus niveles de rendimiento.

Un aspecto importante que debe resguardar una institución es la información. La información, en todas sus formas, es uno de los principales activos de cualquier institución, necesaria para su normal funcionamiento. Uno de los retos más importantes que deben enfrentar los departamentos de Tecnologías de Información (TI) es mantener en operatividad los servicios que ofrece una institución para preservar, procesar y administrar eficientemente la información que se encuentra en los Data Center y en el envío, operación y recepción de la misma. En este aspecto, la infraestructura física y lógica son factores que influyen en la tarea de garantizar la disponibilidad, integridad y confidencialidad de la información para la continuidad de las operaciones.

Las entidades públicas y privadas actualmente poseen un Data Center con infraestructura física y tecnológica adecuada, donde se maneja de forma centralizada la información de toda la institución, denominada por lo general Departamento de Sistemas, Departamento de TI, entre otras nomenclaturas. Dichas unidades le permiten trabajar de forma ágil y segura, sin embargo, los Data Center no cumplen con todos los requisitos establecidos en los estándares y normas aceptados internacionalmente, igual es el caso de la Red LAN, ya que no tiene en consideración factores importantes para preservar un servicio continuo, sin fallas y con seguridad. Es por ello, que estas normas y estándares se encargan de describir los procedimientos para asegurar que se encuentren correctamente protegidos y/o documentados, y evitar que cualquier tipo de evento no programado, cause pérdidas significativas que puedan llegar a comprometer a la institución de alguna manera.

Los proyectos de auditoría que se plantearon fueron los siguientes: realizar una auditoría de gestión de seguridad física y lógica al Data Center y la Red LAN, esto permitió determinar la posibilidad de la existencia de vulnerabilidades para posteriormente generar un plan de acción, y mitigar el riesgo que estos puedan provocar en la institución. Para el desarrollo de este trabajo, dentro de la ciudad de Loja se escogieron a 7 instituciones públicas, conformadas por entidades educativas, de control y servicios. Por otro lado, también se seleccionaron a 15 instituciones privadas, comprendidas entre entidades educativas, financieras, de servicios, de producción entre otras. En el presente artículo, se omiten los nombres de las instituciones evaluadas por motivos de acuerdos de confidencialidad y por seguridad de las mismas.

2. METODOLOGÍA

Para la realización de este proyecto se siguieron las fases establecidas en cada uno de los objetivos, las fases incluyen las actividades descritas a continuación:

Fase I

Revisión de normas, buenas prácticas y casos de éxito para la gestión de la seguridad del Data Center y de la red LAN. Para el cumplimiento de esta fase se realizó un estudio minucioso de Tesis Doctorales, Artículos Científicos y demás documentos, que abarcan información sobre la creación, seguridad y funcionamiento de un Centro de Datos y red LAN.

Posterior a ello, se realizaron cuadros comparativos de las normas, estándares y metodologías con las características, herramientas y su utilización en la sociedad, determinando cuál de ellas es la más óptima para llevar a cabo la ejecución de la auditoría en las entidades públicas y privadas de la ciudad de Loja.

Dentro de los trabajos de auditoría realizados en empresas creadas y que se tomó como referencia podemos mencionar “*La auditoría informática de la Empresa Municipal de Agua Potable y Alcantarillado de Ambato*” que fue implementada en el año 2007 en los departamentos: financiero,

tesorería, proveeduría, en las agencias norte y sur de la misma. Este trabajo fue desarrollado y culminado en su totalidad, determinando las falencias en sus sistemas de cómputo, y realizando las respectivas recomendaciones (Espinoza, 2007).

Igualmente, entre los años 2011 y 2012, se realizó una auditoría de seguridad informática a la empresa de alimentos “*Italimentos Cía. Ltda.*”, en la ciudad de Cuenca, la misma que fue culminada con éxito y, como resultado final, se pudo determinar el nivel de seguridad en los procesos críticos de la empresa (Cadme, 2011).

Fase II

Realizar la auditoría al nivel de seguridad físico y lógico del Data Center y Red LAN de las entidades públicas y privadas de la ciudad de Loja, para determinar la situación actual. Para llevar a cabo esta fase, se dividió en las etapas típicas que conlleva una auditoría, empezando por el diagnóstico general de las entidades, en el cual se obtuvo información organizacional y administrativa de las mismas. Posteriormente, se realizó la planificación previa a la ejecución de la auditoría, estableciendo su fecha de inicio, fecha final, el personal involucrado en el trabajo, el objetivo que se llegó a cumplir, el alcance y las herramientas necesarias. También se definieron los criterios de aceptación del riesgo y finalmente, se elaboraron los formularios para la evaluación.

Después de la planificación, se ejecutó todo lo expuesto anteriormente, evaluando cada una de las secciones, para luego realizar el respectivo análisis de la gestión de riesgos, en la cual se determinó el nivel de riesgo que actualmente llevan las áreas de tecnología de las entidades. Dentro de esta etapa, también se realizó la determinación de los hallazgos positivos y negativos en base a su criterio, condición, causa y efecto, los mismos que sirvieron para elaborar el informe de la auditoría.

Por último, se realizó la socialización de los resultados, a los funcionarios de las entidades auditadas, lo cual permitió acoger sugerencias, recomendaciones y demás factores que permitieron concluir el informe final para la siguiente fase.

Fase III

Elaborar el informe final de auditoría para mitigar los riesgos, en base al análisis realizado. En esta etapa, se realizaron las recomendaciones para los cambios en las falencias detectadas, elaborando el informe final, el cual detalla la situación actual de las seguridades físicas y lógicas que lleva cada una de las entidades públicas y privadas de la ciudad de Loja.

3. NORMAS, ESTÁNDARES Y METODOLOGÍA PARA LA AUDITORÍA

Las normas y estándares para la evaluación de la situación actual de las seguridades de la Unidad de Tecnología de las entidades fueron las siguientes:

TIA/EIA-568-C

Es una revisión del ANSI/TIA/EIA 568-B, publicada entre los años 2001 y 2005. El nuevo estándar consolida los documentos centrales de las recomendaciones originales y todos los “adendum” (Espinoza, 2007), pero cambia la organización, generando una recomendación “genérica” o “común” a todo tipo de edificios. Está estructurados de las siguientes partes:

- TIA/EIA 568-C.0 tiene como objetivo permitir la planificación y la instalación de un sistema de cableado estructurado para todo tipo de instalaciones. Esta norma especifica un sistema que soporte cableados de telecomunicaciones genéricos en un entorno multi-producto y multiproveedor. Varios de los conceptos originalmente indicados en la recomendación ANSI/TIA/EIA 568-B.1 (que era específica para edificios comerciales) fueron generalizados e incluidos en la 568-C.0.
- TIA/EIA 568-C.1 provee información acerca del planeamiento, instalación y verificación de cableados estructurados para edificios comerciales. Los aspectos de la anterior recomendación

ANSI/TIA/EIA 568-B.1 que aplican únicamente a este tipo de edificios fueron detallados y actualizados en esta nueva recomendación.

- TIA/EIA 568-C.2 detalla los requerimientos específicos de los cables de pares trenzados balanceados, a nivel de sus componentes y de sus parámetros de transmisión.
- TIA/EIA 568-C.3 especifica los componentes de cable de fibra óptica, incluyendo aspectos mecánicos, ópticos y requisitos de compatibilidad (Alcalá, 2015).

ANSI TIA/EIA-569

Este estándar provee especificaciones para el diseño de las instalaciones y la infraestructura edilicia necesaria para el cableado de telecomunicaciones en edificios comerciales (Joskowicz, 2013; p. 7-8). Este estándar tiene en cuenta tres conceptos fundamentales relacionados con telecomunicaciones y edificios:

- Los edificios son dinámicos. Durante la existencia de un edificio, las remodelaciones son comunes, y deben ser tenidas en cuenta desde el momento del diseño. Este estándar reconoce que existirán cambios y los tiene en cuenta en sus recomendaciones para el diseño de las canalizaciones de telecomunicaciones.
- Los sistemas de telecomunicaciones son dinámicos. Durante la existencia de un edificio, las tecnologías y los equipos de telecomunicaciones pueden cambiar dramáticamente. Este estándar reconoce este hecho siendo tan independiente como sea posible de proveedores y tecnologías de equipo.
- Telecomunicaciones es más que “voz y datos”. El concepto de Telecomunicaciones también incorpora otros sistemas tales como control ambiental, seguridad, audio, televisión, alarmas y sonido. De hecho, las telecomunicaciones incorporan todos los sistemas que transportan información en los edificios.

Es de fundamental importancia entender que para que un edificio quede exitosamente diseñado, construido y equipado para soportar los requerimientos actuales y futuros de los sistemas de telecomunicaciones, es necesario que el diseño de las telecomunicaciones se incorpore durante la fase preliminar de diseño arquitectónico.

El estándar identifica seis componentes en la infraestructura edilicia:

- Instalaciones de entrada
- Sala de equipos
- Canalizaciones de “Montantes” (“Back-bone”)
- Salas de telecomunicaciones
- Canalizaciones horizontales
- Áreas de trabajo

ANSI TIA/EIA-606-A

El propósito de este estándar es proporcionar un esquema de administración uniforme que sea independiente de las aplicaciones que se le den al sistema de cableado, esto es vital para el buen funcionamiento de un cableado estructurado, pues pueden cambiar varias veces durante la existencia de un edificio. Este estándar habla sobre la identificación de cada uno de los subsistemas basado en etiquetas, códigos y colores, con la finalidad de que se puedan identificar cada uno de los servicios que en algún momento se tengan que habilitar o deshabilitar¹.

Para esto, se establece guías para dueños, usuarios finales, consultores, contratistas, diseñadores, instaladores y administradores de la infraestructura de telecomunicaciones y sistemas relacionados. Esto es muy importante, ya que en la documentación que se debe entregar al usuario final, la norma dice que se tendrá que especificar la forma en que está distribuida la red, por dónde viaja, qué puntos conecta y los medios que utiliza (tipos de cables y derivaciones), así se facilitara la localización de fallas, detallando cada cable tendido por características².

¹ <http://herramientas-telamiticas.webnode.es/estandar/ansi-tia-eia-568-2-/estandar-ansi-eia-tia-606/>

² ITCA Escuela de Computación: http://virtual.itca.edu.sv/Mediados/irmfi2/ITRMFI_02.htm

Estándar ANSI/TIA/EIA 942

Fue desarrollado por la Asociación de la Industria de Telecomunicaciones (TIA)³, tiene como alcance definir una guía de diseño para Infraestructuras TI (Tecnologías de la Información), que garantice (Polo, 2012):

- Seguridad operacional
- Continuidad del servicio
- Disponibilidad
- Solidez

Brinda información acerca de:

- Disposición espacial
- Infraestructura de cableado
- Niveles de redundancia

Especifica los requerimientos mínimos para la infraestructura de telecomunicaciones de Data Centers, además está basado en el Uptime Institute y contiene algunas recomendaciones Eléctricas, Mecánicas, Telecomunicaciones y Arquitectónicas.

Norma ISO/IEC 27002

Fue desarrollada por la Organización Internacional de Normas Técnicas. Es una guía que contiene un conjunto de buenas prácticas para la seguridad de la información. Está conformada por un total de 39 objetivos de control y 133 controles que se encuentran agrupados en 11 dominios que cubren aspectos específicos de la seguridad de la información. La norma está estructurada en 16 capítulos de los cuales los cuatro primeros hacen referencia a los aspectos generales de la norma, mientras que los capítulos siguientes describen cada uno de los dominios que son parte de esta norma. A continuación, se describen de manera resumida los dominios integrantes de esta norma⁴:

- Políticas de seguridad
- Aspectos organizativos de la seguridad de la información
- Gestión de activos
- Seguridad ligada a los recursos humanos
- Seguridad física y ambiental
- Gestión de comunicación y operaciones
- Control de acceso
- Adquisición, desarrollo y mantenimiento de los sistemas de información
- Gestión de incidentes de seguridad de la información
- Gestión de la continuidad del negocio
- Cumplimiento

Metodología MAGERIT

Fue desarrollado por el Consejo Superior de Administración Electrónica de España, como respuesta al crecimiento acelerado de la tecnología de información y al uso que hacen las organizaciones, esto con la finalidad de concientizar a los responsables de los sistemas de información de la existencia de riesgos, para de esta manera prevenirlos y saber mitigarlos a tiempo (Lucero & Valverde, 2012).

Está estructurada actualmente por tres libros:

- El primero denominado “Método”, que describe los pasos y tareas básicas para realizar un proyecto de análisis y gestión de riesgos.
- El segundo denominado “Catálogo”, ofrece criterios de valoración, para que, al momento de realizar el análisis de los riesgos, se tenga una idea más homogénea para asignar el valor de riesgo. Estos valores dependen del impacto que causen y la probabilidad de su ocurrencia, unos

³ Telecommunications Industry Association: “Norma Tia 942”, <http://www.tiaonline.org>

⁴ Portal de ISO 27002 (en español) - Otros estándares de seguridad de la información: <http://www.iso27000.es/iso27002.html>

serán de valoración económica, que son muy fácil de situar, mientras que otros serán asignados cualitativamente, quedando a discreción del usuario, es decir, respondiendo a criterios subjetivos.

- El tercero denominado “Guía de Técnicas”, describe algunas técnicas que se emplean habitualmente para llevar a cabo los proyectos de análisis y gestión de riesgos⁵.

4. EJECUCIÓN DE LA AUDITORÍA

Diagnóstico general de las entidades públicas y privadas

Se recolectó información organizacional de cada una de las entidades auditadas y de las Unidades de Tecnología e Información, con el fin de tener una idea clara de las funciones y servicios que las entidades prestan a la comunidad en general, dentro de la información que se obtuvo, tenemos:

- Orgánico Estructural de las entidades públicas y privadas
- Misión y Visión
- Objetivos Estratégicos
- Unidad de Tecnología e Información (UTI)
- Misión de la UTI
- Orgánico Estructural de la UTI
- Atribuciones y Responsabilidad
- Productos y Servicios

Planificación específica

Se definieron estrategias, actividades, objetivos, alcance, herramientas y demás elementos que permitieron elaborar el programa de auditoría. Entre los puntos que resaltan está el objetivo y el alcance de la auditoría, que consiste en:

Objetivo

Conocer el estado actual de las seguridades físicas y lógicas del Data Center y Red LAN de las entidades públicas y privadas de la ciudad de Loja, evaluando las políticas de seguridad informática y la percepción de las personas entrevistadas, con el fin de plantear sugerencias técnicas para mejorar los procesos que se llevan a cabo en las instituciones.

Alcance

Para el desarrollo de la auditoría se limitará el alcance a la evaluación del cumplimiento de normas y estándares, con la finalidad de realizar el análisis de los riesgos, y en base al análisis, emitir recomendaciones que permitan mitigar los riesgos en cuanto a las seguridades físicas y lógicas del Data Center y la red LAN de las Unidades de Tecnología e Información.

Definición de secciones de auditoría

Tomando en consideración la norma BICSI¹, Los formularios pertenecen a dos categorías: seguridades físicas y seguridades lógicas, ambos en base a las normativas antes indicadas. Para la parte física se individualizó 12 secciones, de las cuales 6 abarcan la gestión de riesgos (General, Secundarias, Incendios, Inundaciones, Ambientales, Eléctricas), 2 están dedicadas a la red LAN (Networking y Telecomunicaciones), 2 tratan sobre la seguridad de Datos (Respaldo y Servidores) y 2 sobre el Control de Ingreso al Data Center (Visitas y Personal).

En la Figura 1 se indica la representación de las secciones para el análisis de las seguridades físicas del Data Center y de la Red LAN.

En el caso de las Seguridades Lógicas, se definieron 7 secciones: una general que trata de aspectos mínimos de seguridad que se necesita en un Data Center, otra para Sistemas Operativos, otra para

⁵ Gobierno de España, Ministerio de Hacienda y Administraciones Públicas - MAGERIT, Versión 3.0: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Disponible en http://administracionelectronica.gob.es/pae_Home_pae_Documentacion/pae_Metodolog/pae_Magerit.html

Software y otra destinada al Firewall, 2 para la seguridad de Datos (Servidores y Bases de Datos) y finalmente, una sección para la red LAN denominada Comunicación como se indica en la Figura 2.

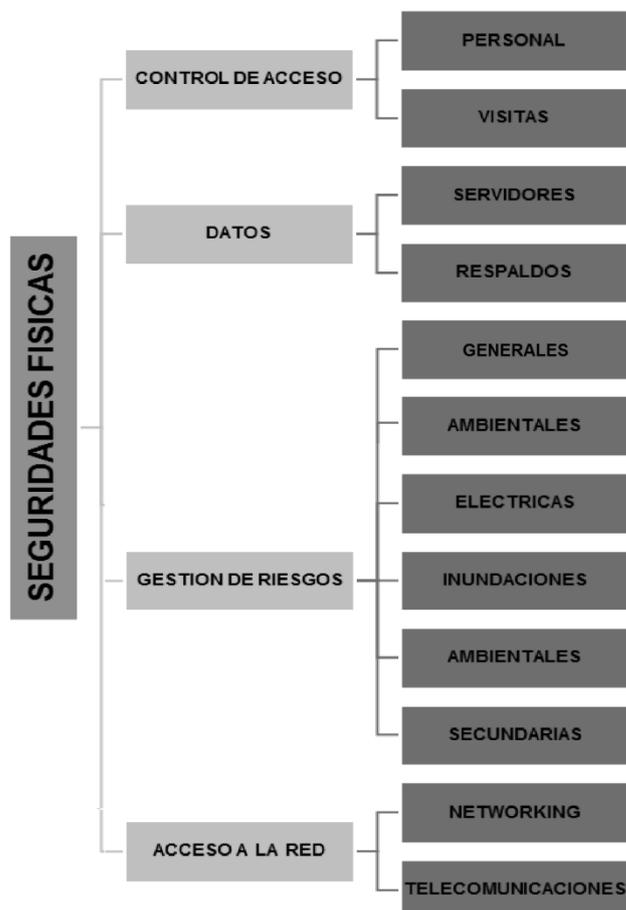


Figura 1. Secciones de seguridades físicas.

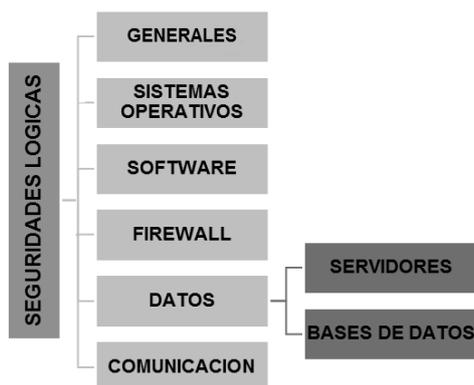


Figura 2. Secciones de seguridades lógicas.

Valoración de activos

La valoración de activos se realizó a partir de tres dimensiones: integridad, disponibilidad y confidencialidad. A continuación, en las Tablas 1 y 2, se presenta la definición de los activos de información y las amenazas respectivamente.

Tabla 1. Activos de información.

Activos de información	
Tipo	Descripción
Tecnología	Servicios auxiliares para organizar, gestionar y manipular la información y comunicación.
Instalaciones	Lugar donde se alojan los equipos informáticos y de comunicaciones.
Aplicaciones (software)	Software para la gestión de la información.
Equipo Informático (hardware)	Hardware que permite hospedar datos, aplicaciones y servicios.
Soporte de Información	Dispositivos de almacenamiento de datos.
Datos / Información	Activo abstracto que será almacenado, transferido o destruido en la institución.
Personas	Encargadas que operan los activos mencionados anteriormente.

Tabla 2. Amenazas.

Amenazas	
Tipo	Descripción
Accidentales	Eventos que pueden ocurrir sin intención de ocasionar daños a los activos e instalaciones, por empleados internos o externos.
Deliberadas	Eventos que pueden ocurrir con la intención de ocasionar daños a los activos e instalaciones, por empleados internos o externos.

Niveles o criterios de aceptación del riesgo

En este caso, para definir estos criterios nos basamos en tres aspectos: las vulnerabilidades de cada activo en base a las amenazas, la probabilidad de ocurrencia del fallo a partir de la amenaza, y el nivel de impacto o daño que se tendría sobre el activo. A continuación, se presentan las tablas que permitirán determinar el nivel de aceptación del riesgo en función del impacto y probabilidad de ocurrencia Tabla 3, 4 y 5, la misma que será aplicada en la tercera fase de la auditoría donde se determinarán los riesgos a ser tratados o minimizados.

Tabla 3. Escala de probabilidad.

Escala probabilidad		
1	Bajo	No es probable que suceda
2	Medio	Bastante probable que suceda
3	Alto	Probable que suceda inmediatamente

Tabla 4. Escala de impacto.

Escala de impacto		
1	Insignificante	El daño no tiene consecuencias relevantes para la organización.
2	Bajo	Los daños son menores, pueden ocasionar pérdida financiera y/o publicidad negativa para la institución.
3	Medio	Los daños son graves, pueden ocasionar pérdida financiera considerable y/o publicidad negativa para la institución.
4	Alto	Los daños traen consecuencias muy graves, pueden ocasionar la suspensión del negocio por un tiempo prudencial.

5	Extremo	Los daños traen consecuencias extremadamente graves, puede ocasionar la suspensión del negocio por un tiempo extendido o su desaparición.
---	---------	---

Tabla 5. Escala de riesgo en función del impacto y probabilidad de ocurrencia.

Escala de riesgo		
11 >= 15	Riesgo extremo	Riesgo muy probable y de muy alto impacto. Cubre un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables, pero de impacto bajo o muy bajo.
6 >= 10	Riesgo moderado	Riesgo improbable y de muy bajo impacto.
1 >= 5	Riesgo bajo	

Preguntas realizadas durante la auditoría

Una vez definido el diagnóstico de las entidades a ser auditadas, se procedió a definir la planificación específica para cada una de ellas, estableciendo los objetivos y el alcance. Al haber estipulado cada una de las secciones de auditoría, determinado y valorado cada uno de los activos, y haber especificado los criterios de aceptación del riesgo, en base a las normativas mencionadas anteriormente, se procedió a crear las diferentes preguntas que conformarían las encuestas realizadas, dentro de cada una de las secciones, tanto para las seguridades físicas como para las seguridades lógicas.

Proceso:	Seguridades Físicas Generales	Fecha:
Preguntas		
1. ¿Existen documentos de políticas de seguridad física?		
2. ¿Existen procedimientos relativos a la seguridad física?		
3. ¿Existe un responsable de las políticas, normas y procedimientos?		
4. ¿Existen mecanismos para la comunicación a los usuarios de las normas?		
5. ¿Existen controles regulares para verificar la efectividad de las políticas?		
6. ¿Existen roles y responsabilidades definidos para las personas?		
7. ¿Existen condiciones contractuales de seguridad con terceros y outsourcing?		
8. ¿Existen criterios de seguridad en el manejo de terceras partes?		
9. ¿En las áreas seguras existen controles adicionales al personal propio y ajeno?		
10. ¿Existe un inventario de activos en forma detallada actualizado?		
11. ¿Se recogen datos de los incidentes de forma detallada?		
12. ¿Posee seguridad física y del ambiente?		
13. ¿Existe perímetro de seguridad física (paredes, puertas con llave, etc.)		
14. ¿Existen controles de entrada para protegerse frente al acceso de personal no autorizado?		
15. ¿Existe circuito cerrado de video para el control de accesos a DataCenter?		
16. ¿Un área segura ha de estar cerrada, aislada y protegida de eventos naturales?		
17. ¿Existen controles ambientales del DataCenter?		
18. ¿Existen controles para eventos generados por fuego?		
19. ¿La ubicación de los equipos esta ubicada para minizar accesos innecesarios?		
20. ¿Existe Seguridades para el acceso a los servidores?		
21. ¿Se asegura la disponibilidad e integridad de todos los equipos?		
22. ¿Existe algún tipo de seguridad para los equipos retirados o ubicados exteriormente?		
23. ¿Existen protecciones frente a fallos en la alimentación eléctrica?		
24. ¿Existen protecciones frente a las variaciones electricas?		
25. ¿Existe seguridad en el cableado general del DataCenter, frente a daños e intercepciones?		

Figura 3. Muestra de preguntas de las encuestas realizadas.

Ejecución del trabajo

En la fase de ejecución del trabajo, se procedió a evaluar los formularios elaborados en la etapa anterior, en cada subdirección o sección que corresponda según el tema, determinando las inconformidades o situaciones no deseadas que deben ser corregidas de forma inmediata.

Para detectar los riesgos, se realizó la evaluación a partir de dos perspectivas: Probabilidad e Impacto, como se había indicado en la etapa anterior, esto se presta porque no se puede conocer con exactitud cuándo y dónde un evento pueda ocurrir, así como tampoco las consecuencias materiales y financieras que puede traer consigo.

En la evaluación de riesgos, se tienen dos tipos de riesgos, riesgos inherentes, que es el riesgo en ausencia de acciones que podrían alterar el impacto o la frecuencia de ocurrencia de los riesgos, y los riesgos residuales que resulta después que la dirección ha implantado efectivamente salvaguardas para mitigar el riesgo inherente.

Entidades públicas

Resumen de los niveles de seguridades físicas

Una vez culminado la auditoría de la gestión de seguridad al Data Center y red LAN, en entidades públicas que manejan sus propias Unidades de Tecnología e Información en la ciudad de Loja, el análisis de las seguridades físicas, identificó que existen grandes riesgos y vulnerabilidades como lo indica la Tabla 6, que pueden llegar a ocasionar problemas y catástrofes de gran magnitud para las entidades públicas, el estado del entorno físico y social de los activos requieren de decisiones inmediatas.

Tabla 6. Evaluación y porcentajes de riesgos de seguridades físicas a nivel general.

Total de porcentajes	Riesgos		
	Alto	Medio	Bajo
Seguridades físicas	50.29	3.78	45.93

A continuación, en la Figura 4, se detalla a modo de pastel, la cantidad de riesgos y sus porcentajes encontrados en las Unidades de Tecnología e Información de las entidades públicas auditadas en la ciudad de Loja.

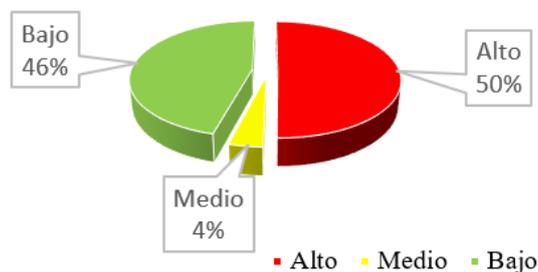


Figura 4. Porcentajes totales de seguridades físicas a nivel general.

Analizando los resultados obtenidos, se determina que en total existe un promedio del 50.29% de riesgos altos, en las diferentes secciones auditadas de las entidades públicas, lo cual determina que el Data Center se encuentra en peligro constante, y es más probable la suspensión total del negocio. De igual manera posee un porcentaje del 3.78% de riesgo medios, lo cual significa que las instituciones podrían seguir funcionando, sin embargo, no se debe dejar por alto y tomar acciones con un tiempo prudencial debido que con el tiempo estos riesgos pueden incrementar su magnitud. Finalmente, un porcentaje del 45.93% de riesgos bajos, es decir, las instituciones cuentan con un gran porcentaje de seguridades de protección frente a vulnerabilidades.

Resumen de los niveles de seguridad lógica

Una vez culminado el análisis de las seguridades lógicas, se han determinado vulnerabilidades y falencias de alto riesgo en los activos y medios de seguridad implementados de acuerdo a la Tabla 7,

por lo cual se debe tomar decisiones inmediatas. En esta tabla se detalla la cantidad de riesgo y sus porcentajes encontrados.

Tabla 7. Evaluación y porcentajes de riesgos de seguridades lógicas a nivel general.

Total de porcentajes	Riesgos		
	Alto	Medio	Bajo
Seguridades lógicas	50.43	6.47	43.10

A continuación, en la Figura 5, se detalla a modo de pastel, la cantidad de riesgos y sus porcentajes encontrados en las Unidades de Tecnología e Información de las entidades públicas auditadas en la ciudad de Loja.

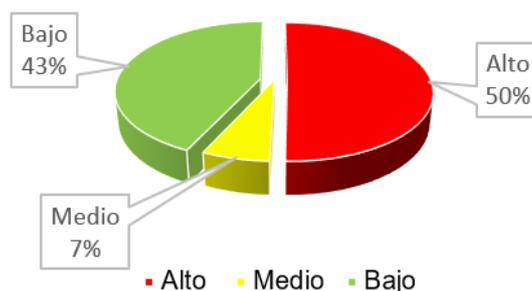


Figura 5. Porcentajes totales de seguridades lógicas a nivel general.

De igual manera, al analizar los resultados de la auditoría, existe un porcentaje de 50.43% de riesgos potencialmente altos, que deben ser tratados de manera urgente, tomando en consideración los nuevos estándares y normas que se aplican a nivel mundial, así como la implementación de nuevas políticas, métodos y mecanismos de acuerdo a las tecnologías existentes. Un porcentaje de 6.47% corresponde a riesgos de nivel medio, es decir, son riesgo que probablemente no lleguen a suceder y su impacto no sea de gran magnitud para ocasionar daños en la institución, sin embargo, se debe considerar la implementación de procesos de seguridad prudencial para evitar que lleguen a suceder y evitar eventos que perjudiquen o lleguen a incrementar el riesgo. Por último, un porcentaje de 43.1% corresponde a riesgos de nivel bajo, es decir, se cuenta con las medidas adecuadas para la seguridad lógica y, consecuentemente, las instituciones pueden continuar normalmente con las actividades de acuerdo a lo planificado.

Entidades privadas

Resumen de los niveles de seguridades físicas

De igual forma, en las entidades privadas que manejan sus propias Unidades de Tecnología e Información en la ciudad de Loja, el análisis de las seguridades físicas se identificó que existen problemas en este campo, como lo indica la Tabla 8, que pueden llegar a ocasionar el acceso no autorizado a los activos informáticos, pudiendo generar pérdidas económicas grandes.

Tabla 8. Evaluación y porcentajes de riesgos de seguridades físicas a nivel general.

Total de porcentajes	Riesgos		
	Alto	Medio	Bajo
Seguridades físicas	39.45	10.18	50.36

A continuación, en la Figura 6, se muestra la cantidad de riesgos y sus porcentajes encontrados en las Unidades de Tecnología e Información de las entidades privadas, auditadas en la ciudad de Loja.

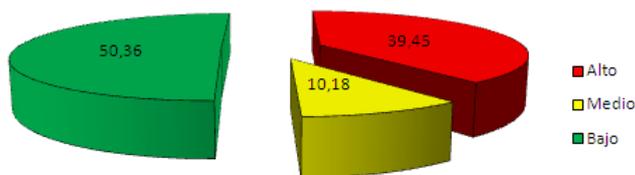


Figura 6. Porcentajes totales de seguridades físicas a nivel general.

Analizando los resultados obtenidos, se determinó que, en las diferentes secciones auditadas de las entidades privadas, existe un promedio del 39.45% de riesgos altos, con una clara diferencia con las públicas. Un porcentaje del 10.18% corresponde a riesgos medios, lo cual significa que las instituciones podrían seguir funcionando, con una brecha pequeña en referencia a las entidades públicas. Finalmente, un porcentaje del 50.36% ha sido contabilizado para riesgos bajos, es decir, las instituciones cuentan con un gran porcentaje de seguridades de protección frente a vulnerabilidades y se puede apreciar que es mucho mejor referente a las entidades públicas.

Resumen de los niveles de seguridad lógica

Para el sector privado, terminada la auditoría y con los resultados obtenidos se ejecutó el análisis de las seguridades lógicas, determinado vulnerabilidades y falencias de alto riesgo en los activos y medios de seguridad implementados de acuerdo a la Tabla 9, por lo cual se debe tomar decisiones inmediatas.

Tabla 9. Evaluación y porcentajes de riesgos de seguridades lógicas a nivel general.

Total de porcentajes	Riesgos		
	Alto	Medio	Bajo
Seguridades lógicas	55.05	17.01	27.93

En la Figura 7, se muestran los porcentajes de riesgos encontrados en las Unidades de Tecnología e Información de las entidades privadas, auditadas en la ciudad de Loja.

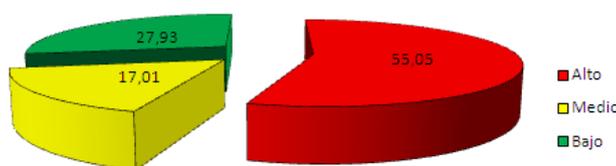


Figura 7. Porcentajes totales de seguridades lógicas a nivel general.

En las instituciones privadas, existe un porcentaje promedio de 55.05% de riesgos potencialmente altos a nivel lógico, que deben ser tratados de manera urgente, de acuerdo a las normas existentes, para evitar daños irreparables al negocio. Posee un porcentaje de 17.01% de riesgos a nivel medio, es decir, son riesgo que pueden afectar a la continuidad del negocio, pero pueden esperar para tomar medida, pero no descuidarlos porque se pueden convertir en riesgos altos y constituir un riesgo fatal para el negocio de las entidades privadas. Por último, un porcentaje de 27.93% corresponde a riesgos de nivel bajo, es decir, se cuenta con las medidas adecuadas para la seguridad lógica y las instituciones puede continuar normalmente con las actividades de acuerdo a lo planificado.

Con ambos resultados obtenidos, podemos deducir que, en la actualidad, tanto empresas públicas y privadas de la ciudad de Loja, no tienen enraizada la conciencia sobre la seguridad de la información, a pesar de haber implementado ciertas medidas de seguridad, aún faltan mitigar riesgos que puedan afectar la continuidad del negocio, por lo cual se deben realizar auditorías adicionales posterior a la corrección de los riesgos altos, para determinar los nuevos niveles de seguridad.

Es importante acotar que es imposible alcanzar un 100% de seguridad de la información, debido al cambio constante de las tecnologías y de nuevos tipos de ataques y vulnerabilidades que se descubren a diario. Por tal motivo, a pesar de no aplicar necesariamente a una certificación, es recomendable siempre utilizar las normativas internacionalmente aceptadas como forma para garantizar buenos niveles de seguridad.

Por ética y confidencialidad de la información, no se citan las entidades auditadas, tanto públicas como privadas, para evitar que sean vulnerados de alguna manera, por el contenido del presente artículo.

Comunicación del trabajo

La fase de comunicación de este trabajo tiene como propósito impulsar la toma de decisiones correctivas inmediatas, el objetivo es exponer los hallazgos de la auditoría ante las partes interesadas y asegurar que los resultados de la auditoría sean comprendidos y aceptados, determinando lo que se va a proteger y lo que se debe hacer para protegerlo, ya sea evaluar, reducir, transferir, cambiar o simplemente aceptar el riesgo.

5. CONCLUSIONES

- Con la realización de las auditorías a las Unidades de Tecnología e Información, se obtuvo la situación actual, no siendo esta la más óptima tanto en públicas como privadas, debido a que se determinó la ausencia total de controles de seguridad en ciertos puntos.
- Los actuales manuales de políticas de seguridad de la información, que se encuentran desarrollados e implementados en las instituciones tanto públicas como privadas, no están basados en normativas internacionalmente aceptadas, lo cual no garantiza la correcta protección de los activos de información que se gestionan en ella.
- Con los resultados obtenidos, los altos directivos de las entidades públicas o privadas podrán tomar medidas para la mitigación de los riesgos que pueden provocar pérdidas económicas o cortes prologados en el servicio, afectando considerablemente la imagen de la entidad.
- La aplicación de la Norma ISO/IEC 27002 y el Estándar TIA/EIA 942, son idóneas para el análisis, permiten cubrir la insuficiencia de la gestión de seguridad de la información y la infraestructura para la adecuada implementación, debido a que éstas engloban las mejores prácticas recopiladas de normas y estándares anteriores para el mejoramiento de la seguridad física y lógica.

REFERENCIAS

- Alcalá, T. (2015). *Ansi/Tia/Eia-568 a, b y c. Cableado de telecomunicaciones para edificios comerciales*. Disponible en <http://cdalcala-upsum.blogspot.com/2015/06/ansitiaeia-568-b-y-c.html>
- Cadme, C. (2011). *Auditoría de seguridad informática ISO 27001 para la empresa de alimentos "Italimentos Cía. Ltda"*. Disponible en <http://dspace.ups.edu.ec/handle/123456789/2644>
- Espinoza, M. (2007). *Auditoría Informática de la Empresa Municipal de Agua Potable y Alcantarillado de Ambato*. Disponible en <http://repo.uta.edu.ec/bitstream/handle/123456789/214/t288s.pdf?sequence=1>
- Joskowicz, J. (2013). *Cableado estructurado*. Disponible en: <https://iie.fing.edu.uy/ense/assign/ccu/material/docs/Cableado%20Estructurado.pdf>
- Lucero, A. J., & Valverde, J. O. (2012). *Análisis y gestión de riesgos de los sistemas de la Cooperativa de Ahorro y Crédito Jardín Azuayo, utilizando la metodología MAGERIT*. Tesis de Pregrado, 175 pp., Universidad de Cuenca, Cuenca, Ecuador.

Polo, N. L. (2012). *Diseño de un data center para el ISP READYNET CÍA.LTDA. Fundamento en la norma ANSI/TIA/EIA-942*. Tesis de Pregrado, 203 pp. Facultad de Ingeniería Eléctrica y Electrónica, Escuela Politécnica Nacional, Quito, Ecuador.