LOGO DE LA FIRMA O ENTIDAD

HH/__

Alguna institución pública
NOMBRE DE LA ENTIDAD

Departamento de TIC
ÁREA O UNIDAD EXAMINADA

30 Días
PERÍODO DE OPERACIONES EXAMINADO

HOJA DE HALLAZGOS DE AUDITORÍA

REF. P/T	No se aplica de forma óptima la Unidad de Seguridad Informática TÍTULO
	No se ha planteado la creación de una Unidad de Seguridad Física y Lógica CONDICIÓN
	No cumple la norma 1.4 acerca de la Gestión de la seguridad de la información de las Normas técnicas para la gestión y el control de las Tecnologías de Información CRITERIO
	Se cuenta con una directriz de la no creación de plazas ni de contratación de personal y la falta de conocimiento por parte de la administración. CAUSA
	Esto conllevo a accesos no autorizados a información sensible, la cual fue vulnerada repercutiendo en una pérdida económica para atender el incidente y securizar la información lo más pronto posible. EFECTO
	No aplica CONCLUSIÓN
	1. Reconsiderar la creación de nuevas plazas para la creación de la unidad de seguridad fisica y lógica. 2. Implementar controles de seguridad en temas de acceso a información sensible. 3. Realizar la contratación de terceros que puedan brindar servicios de seguridad de la información de la institución si no se abren nuevas plazas. RECOMENDACIÓN
	No aplica REACCIÓN DE LA ADMINISTRACIÓN

Auditoría Informática

IF8200

Caso #2

Indicaciones:

El estudiante debe identificar las partes correspondientes al hallazgo conforme a las características que lo componen: criterio, condición, causa, efecto y recomendación, según sea el caso, y que han sido analizadas en el curso. Las características faltantes debe redactarlas.

El caso ocurrió en una institución pública:

UNIDAD DE SEGURIDAD FÍSICA-LÓGICA.

El tema de la seguridad en Tecnologías de Información, incluye: a nivel físico (Controles de acceso a centros de trabajo) y nivel lógico (control en claves de acceso para programas y bases de datos), partiendo de la necesidad de contar con una información Integra, Confidencial, Disponible e Irrefutable, una deficiencia en este tema podría generar a la institución, pérdidas económicas por la posibilidad de robos de información o de equipos, accesos indebidos a nivel físico y lógico y daños en la imagen y prestigio.

El Licenciado Montero, menciona que aunque al igual que la Unidad de Proyectos, formalmente no ha sido planteada la necesidad de la creación de una Unidad de Seguridad Física y Lógica, a la Administración, considera que la creación de esta unidad para el control más eficiente de la seguridad informática, es un asunto de inversiones que parecen de muy difícil comprensión para quienes no están en el ámbito informático, situación que tratará de implementarlo con la nueva administración, siempre tomando en cuenta que existen las mismas limitantes de directriz de la no creación de plazas ni de contratación de personal.

La norma 1.4 acerca de la Gestión de la seguridad de la información de las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE, establece:

> *"La organización debe garantizar, de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizados, daño o pérdida u otros factores disfuncionales.*

Para ello debe documentar e implementar una política de seguridad de la información y los procedimientos correspondientes, asignar los recursos necesarios para lograr los niveles de seguridad requeridos y considerar lo que establece la presente normativa en relación con los siguientes aspectos:

-La implementación de un marco de seguridad de la información.

-El compromiso del personal con la seguridad de la información.

-La seguridad física y ambiental.

-La seguridad en las operaciones y comunicaciones.

-El control de acceso.

-La seguridad en la implementación y mantenimiento de software e infraestructura tecnológica.

-La continuidad de los servicios de TI.

Además debe establecer las medidas de seguridad relacionadas con:

-El acceso a la información por parte de terceros y la contratación de servicios prestados por éstos.

-El manejo de la documentación.

-La terminación normal de contratos, su rescisión o resolución.

-La salud y seguridad del personal.

Las medidas o mecanismos de protección que se establezcan deben mantener una proporción razonable entre su costo y los riesgos asociados."

Para mencionar el tema marco de estándares internacionales, COBIT en sus apartados P04.7 y P04.8, menciona:

"P04.7. Responsabilidad de Aseguramiento de Calidad de TI.

Asignar la responsabilidad para el desempeño de la función de aseguramiento de calidad (QA) y proporcionar al grupo de QA sistemas de QA, los controles y la experiencia para comunicarlos. Asegurar que la ubicación organizacional, las responsabilidades y el tamaño del grupo de QA satisfacen los requerimientos de la organización.

P04.8. Responsabilidad sobre el Riesgo, la Seguridad y el Cumplimiento.

Establecer la propiedad y la responsabilidad de los riesgos relacionados con TI aun nivel superior apropiado. Definir y asignar roles críticos para administrar los riesgos de TI, incluyendo la responsabilidad específica de la seguridad de la información, la seguridad física y el cumplimiento. Establecer responsabilidad sobre la administración del riesgo y la seguridad a nivel de toda la organización para manejar los problemas a nivel de toda la empresa. Puede ser necesario asignar responsabilidades adicionales de administración de la seguridad a nivel de sistema específico para manejar problemas relacionados con seguridad. Obtener orientación de la alta dirección con respecto al apetito de riesgo de TI y la aprobación de cualquier riesgo residual de TI."

Para el tema de seguridad, se hace mención del análisis de la estructura presentada y descrita en el punto anterior y aunque se identifica en ella una Unidad de Seguridad Informática, la misma no se desempeña de la manera más óptima, actualmente el tema de seguridad se mantiene a nivel interno del Departamento de Informática pero como una tarea más de la labor informática, sin dar la importancia que este tema requiere de manera integral en el cual se tome en cuenta la seguridad lógica y física en la institución.