ISSN-E: 2542-3401, ISSN-P: 1316-4821

Universidad, Ciencia y Tecnología,
vol.26, Núm. 114, (pp. 39-49)

https://doi.org/10.47460/uct.v26i114.589

Gestión de riesgos en aulas de innovación pedagógica

José Fortunato Zuloaga Cachay
https://orcid.org/0000-0003-2363-0817
jzuloaga@usat.edu.pe
Universidad Católica Santo Toribio de Mogrovejo
Chiclayo, Perú

Freddy William Campos Flores
https://orcid.org/0000-0002-9624-2930
fcampos@ucvvirtual.edu.pe
Universidad César Vallejo
Chiclayo, Perú

Denny John Fuentes Adrianzén
https://orcid.org/0000-0003-4864-1352
dfuentesad@unprg.edu.pe
Universidad Nacional Pedro Ruiz Gallo
Lambayeque, Perú

Johnny Cueva Valdivia
https://orcid.org/0000-0001-8167-109X
jcuevav@unasam.edu.pe
Universidad Nacional Santiago Antúnez de Mayolo
Ancash, Perú

Recibido (28/02/2022), Aceptado (10/04/2022)

Resumen.- El propósito de la gestión de riesgos es proteger el equipamiento de Tecnologías de la información y comunicación (TIC) frente a posibles vulneraciones de seguridad interna y externa. La evaluación de riesgos se trabajó con la técnica de análisis documental respecto a los riesgos asociados a la instalación y equipamiento de las AIP, asimismo se utilizó la encuesta para recabar información por medio de un cuestionario virtual, el cual se aplicó a los docentes DAIP con la finalidad que estos puedan evaluar la gestión de riesgos en relación con la sustentabilidad del equipamiento TIC. Información que permitió proponer un plan, así como su evaluación de los activos computacionales en áreas seguras y seguridad de equipos obteniendo niveles de riesgo alto y muy alto que comprometen la funcionalidad de la infraestructura TIC y consecuente perjuicio al servicio educativo, por lo que se plantearon medidas de prevención para mitigar los efectos adversos.

Palabras clave: Vulnerabilidad computacional, plan de gestión de riesgos, seguridad de los equipos

Risk management in innovative pedagogical classrooms

Abstract.- The purpose of risk management is to protect the Information and Communication Technologies (ICT) equipment against possible internal and external security breaches. The risk assessment worked with the technique of documentary analysis regarding the risks associated with the installation and equipment of the AIP, also used the survey to collect information through a virtual questionnaire, which was applied to teachers DAIP in order that they can assess the risk management in relation to the sustainability of ICT equipment. This information made it possible to propose a plan, as well as an evaluation of the computer assets in secure areas and equipment security, obtaining high and very high risk levels that compromise the functionality of the ICT infrastructure and consequently harm the educational service, so prevention measures were proposed to mitigate the adverse effects.

Keywords: Computational vulnerability, risk management plan, equipment security

I. Introducción

Los riesgos en la Tecnología de la Información y Comunicación (TIC) están relacionados con los eventos e incidentes que podrían comprometer la infraestructura computacional y causar impactos desfavorables en los procesos de negocio de una organización vinculados con su misión y visión [1].

En este sentido, la gestión de riesgos es una herramienta que posibilita la toma de decisiones en situaciones que pueden ir mal, y el firme propósito de identificar los riegos más importantes que se pueden presentar en determinado escenario y la gestión de estrategias para minimizar los efectos de los eventos perjudiciales y garantizar la continuidad del negocio [2].

Los daños personales y materiales ante sucesos naturales o provocados deliberadamente o por deficiencia de acciones preventivas en la infraestructura material o lógica del equipamiento computacional, son susceptibles de prevenirse mediante una adecuada gestión de riesgos con el propósito de establecer acciones y procedimientos para controlar el peligro [3].

Los ambientes de las Aulas de Innovación Pedagógica (AIP) de las instituciones educativas son vulnerables a eventos climáticos de orden natural, así como debido a fallas de carácter eléctrico o a los accesos al equipamiento computacional que provoca averías de componentes lógicos o físicos [4].

La propuesta de plan de gestión de riegos tiene como objetivo proteger al equipamiento TIC instalados en las aulas AIP, de posibles fallas en la conexión a cableados de energía eléctrica, conexiones de red, accesos a componentes físicos y lógicos, exposición a temperaturas por encima de lo permitido y otros acontecimientos que dañan los componentes o incluso, la pérdida de los mismos [5].

Consecuentemente la gestión de riesgos en la institución educativa implica la reducción de la vulnerabilidad en la infraestructura y el equipamiento para generar espacios que beneficien al proceso educativo [6].

Esto conlleva la consideración de tres aspectos fundamentales: evitar el riesgo siempre que resulte posible, supervisar el riesgo y, por último, gestionar el riesgo y establecer unos planes de contingencia [7].

Los procesos de gestión de riesgos enmarcados en la usabilidad de infraestructura TIC [8] se encuentran estandarizados y normalizados en gran medida, sin embargo, cuando se requiere tratar solo un aspecto del conjunto de procesos, como el de seguridad física y ambiental, es necesario referirse a una norma técnica en específico, tal como lo alude Lopez y Ruiz [9] al considerar el proceso de Seguridad Física y ambiental forman parte del dominio 11 de la norma técnica ISO 27001, indicando que dichos procesos contiene 2 objetivos de control y 15 controles.

Para los fines de la investigación consideraremos los siguientes controles de las áreas seguras y de la seguridad de equipos. El objetivo de las Áreas seguras es evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información, mientras que el objetivo de la Seguridad de los equipos es evitar la pérdida, los daños, el robo o el compromiso de activos y la interrupción a las operaciones de la organización.

II. Desarrollo

La Dimensión de Gestión de Riesgos permite determinar, analizar, valorar y clasificar el riesgo que se presenta en la dinámica de la usabilidad de infraestructura TIC, con la finalidad de implementar mecanismos que permitan controlarlo.

La Gestión de Riesgos es necesario implementarlo por fases tales como: el análisis para determinar las vulnerabilidades de un sistema; la clasificación para tipificar los riesgos encontrados; la reducción para implementar las medidas de protección; y el control para determinar los ajustes en las deficiencias encontradas, en este sentido, los riesgos en aulas AIP configura como riesgo operativo [13].

El riesgo operativo es la probabilidad de que una institución tenga afectación en sus procesos por la interrupción del servicio que brinda, debido principalmente a fallas en los procesos internos, las personas, las causas naturales, los siniestros y las fallas de sistemas de información [14].

En este contexto, para la implementación de la Gestión de Riesgos en las aulas AIP se tuvo en cuenta la norma técnica emitida por la Organización Internacional de Normalización ISO/IEC 27001:2013, cuya filosofía principal se basa en la gestión de riesgos implícitos o explícitos que se presentan en cualquier organización, con la finalidad de evitar incidentes de seguridad que detengan el normal funcionamiento del equipamiento computacional. Para efectos de la usabilidad de la infraestructura TIC se tomó en cuenta el dominio 11 de la Norma Técnica relacionado con la Seguridad Física y Ambiental, que contiene 2 objetivos (áreas seguras y seguridad de los equipos) y sus correspondientes controles [9].

A. Áreas seguras

Es la prevención del acceso físico no autorizado, los daños e interferencias a la Información que se suministra en el Aula de Innovación Pedagógica y los perjuicios físicos a las instalaciones donde se encuentra funcionando la infraestructura TIC.

El objetivo consiste en explicitar los factores de riesgo que afectan la infraestructura TIC, Determinando los controles de riesgo para reducir la afectación al sistema computacional, y la elaboración de un plan de prevención de riesgos considerando los factores que afectan a la infraestructura TIC, tales como: Malfuncionamiento del equipamiento computacional por sobrecalentamiento y destrucción de dispositivos sensibles a la corriente por descarga estática.

La operacionalización de áreas seguras toma en cuenta los siguientes factores de riesgo:

Daños Físicos: Por efecto del agua (por gotera en el techo del aula AIP, por el servicio de limpieza, por ingreso y derramamiento del líquido por los estudiantes o docente de aula sobre el equipamiento computacional); por fuego (incendio provocado por el malfuncionamiento de algún equipo, por falla en la instalación eléctrica, por la utilización de sustancias sensibles al fuego como el alcohol, bencina, gasolina, etc); destrucción de equipos (por el deficiente almacenamiento del equipamiento, por la precariedad de la instalación del equipo, por falla en el transporte); polvo (por acumulación excesiva en el interior del equipamiento computacional, refrigeración deficiente de componentes por ventiladores defectuosos, destrucción de dispositivos sensibles a la corriente por descarga estática); Corrosión (afectación a la distribución adecuada de corriente eléctrica en el interior del equipamiento computacional, destrucción de soportes metálicos).

Eventos naturales: Precipitaciones (lluvias que afectan el equipamiento computacional por el ingreso de agua del techo o por la puerta del aula AIP); calor intenso (falta de ventilación natural que posibilita el sobrecalentamiento en el equipamiento computacional); movimientos sísmicos (desplome del equipamiento afectando a su normal funcionamiento); inundaciones (afectación del equipamiento por el ingreso de agua al interior del aula AIP).

Pérdida de servicios esenciales: Energía eléctrica (el corte de servicio eléctrico provoca la suspensión en la atención que brinda el aula AIP); telecomunicaciones (el corte de servicio de internet provoca la reducción a intranet en la

atención que brinda el Aula de innovación pedagógica; aire acondicionado (provoca sobrecalentamiento en el sistema computacional, como el malestar e incomodidad en los usuarios de tecnología); servicio de agua (provoca la suspensión del mantenimiento preventivo que se realiza en mobiliario que soporta la infraestructura TIC.

Afectación por radiación: Electromagnética (cuando el aula AIP se encuentra muy cerca de torres de alta tensión, así como cerca de los retransmisores de señal de telefonía móvil).

Manipulación de hardware y software: cuando personal no autorizado o no capacitado realiza mantenimiento preventivo o correctivo de hardware y/o de software y, cuando efectúa desplazamientos del equipamiento sin el cuidado respectivo.

Controles de riesgo: son los parámetros de seguridad de acceso a áreas no autorizadas. Perímetro de seguridad física; controles físicos de entrada; seguridad de oficinas, despachos y recursos; protección contra las amenazas externas y ambientales.

Trabajo en áreas seguras: Áreas de acceso público, carga y descarga.

Indicadores: Informes de inspecciones periódicas de seguridad física de instalaciones, incluyendo actualización regular del estado de medidas correctivas identificadas en inspecciones previas que aún estén pendientes.

B. Seguridad de los equipos

Es la prevención para evitar la pérdida, los daños y el robo parcial o total de la infraestructura TIC con la consecuente interrupción del servicio que brindan las aulas AIP.

El objetivo consiste en explicitar los factores de riesgo que afectan la seguridad de la infraestructura TIC, determinando los controles de riesgo de seguridad para prevenir la afectación a la infraestructura TIC, elaborando un plan de prevención de riesgos considerando la seguridad de los equipos que afectan la seguridad en instalaciones, ingreso de personal y fallas técnicas. Entre los factores de riesgo se pueden mencionar la clausura del aula de AIP por no contar con el suficiente recurso tecnológico debido a la sustracción de sus equipos y la ejecución de rutinas de mantenimiento y reparación sin contar con la debida capacitación.

Además, es importante resaltar lo siguiente para la evaluación de la seguridad de los equipos:

Perjuicio en equipamiento computacional: Robo de equipos (puertas y ventanas sin rejas de protección quedando vulnerable el acceso al aula y la subsecuente acción de sustracción de equipos); manipulación de hardware y de software (personal no autorizado realiza la apertura del equipamiento computacional con la finalidad de sustraer partes y componentes importantes)

Fallas técnicas: Mala práctica en la mantenibilidad del sistema computacional (personal ejecuta rutinas de mantenimiento y reparación sin contar con la debida capacitación, asimismo, utiliza herramientas e instrumentos incorrectos para la realización de determinada acción)

Acciones no autorizadas: Uso no autorizado de equipos por personal ajeno al aula AIP en la manipulación y utilización de equipos sin la debida autorización del docente DAIP o del director de la Institución Educativa; corrupción de datos con acceso al equipamiento computacional a causa de virus alojados en memorias USB, asimismo, por la descarga de programas de sitios web no confiables y por el borrado intencional o accidental de datos importantes;

comportamientos no autorizados como la desactivación de la energía eléctrica del tablero de mando, desconexión de cable de red, cerrar o abrir la puerta de acceso al aula AIP.

Compromiso de las funciones: Suplantación de identidad (personal del Ministerio de Educación o de la Unidad de Gestión Educativa puede ser suplantado y tener acceso a la infraestructura TIC); exposición de información de los recursos tecnológicos (personal de vigilancia u otro difunde información del equipamiento con que cuenta el aula AIP)

Controles de riesgos: Son los parámetros de seguridad en la infraestructura TIC, emplazamiento y protección de equipos, instalaciones de suministro eléctrico protegido, seguridad del cableado, mantenimiento de los equipos con estándares de calidad, salida de equipamiento fuera de las dependencias de la Institución con la debida guía de remisión.

Control de ingreso de dispositivos de almacenamiento en equipamiento computacional.

Indicadores: Informes de inspecciones periódicas a los equipos, incluyendo actividades para la revisión de rendimiento, capacidad, eventos de seguridad y limpieza de los diversos componentes (aplicaciones, almacenamiento, CPU, memoria, red, etc).

C. *Plan de prevención de Riesgos*

El plan de prevención de riesgos es una herramienta de gestión que integra las actividades de evaluación de amenazas, vulnerabilidades y riesgos, con las medidas de prevención, con la finalidad de evitar o disminuir los daños producidos en las instalaciones de las aulas AIP y en el entorno del equipamiento computacional,

Caracterización de las Aulas de Innovación Pedagógica: Las AIP son el escenario donde se organizan los recursos TIC para su aplicación en el proceso enseñanza aprendizaje.

En este ambiente se administran tecnológicamente la infraestructura TIC de los servidores escuela, las computadoras personales de escritorio, laptops, laptops XO, tabletas, proyector multimedia, modem, cableado de red, entre otros, asimismo, se administra el software que da funcionalidad a todo el equipamiento computacional.

El Aula de innovación pedagógica se encuentra dentro del recinto de la Institución Educativa y dependiente administrativa y pedagógicamente de las políticas educativas instauradas por la dirección del plantel de acuerdo a la normatividad vigente emanadas desde el Ministerio de Educación como de la Unidad de Gestión Educativa Local.

Actividad: la actividad principal del AIP es la de proveer de equipamiento computacional operativo para la realización de actividades de aprendizaje que desarrollan los estudiantes con sus docentes de aula o docentes de asignatura, empleando software de aplicación y recursos de internet con el fin de mejorar los aprendizajes de los estudiantes.

Estrategia: determinar en qué medida las principales metas y políticas del aula vinculadas con la usabilidad e infraestructura TIC se logran con la implementación de diversas acciones a nivel tecnológico.

Misión: Integrar las TIC en favor de la educación peruana, contribuyendo en la optimización del proceso enseñanza aprendizaje, de acuerdo con las normas y estándares nacional en el marco de la interculturalidad.

Visión: Lograr que la comunidad educativa tenga pleno acceso a las TIC, usándolas integralmente e incorporándolas gradualmente a su actividad cotidiana; de manera que puedan mejorar sus capacidades de socialización, creatividad e innovación, participando así del desarrollo de la sociedad.

Recursos humanos: Director, es el responsable de la gestión administrativa y pedagógica de la Institución Educativa y de los recursos tecnológicos del aula AIP e interviene en el proceso enseñanza aprendizaje con TIC; Docente AIP, responsable del aula AIP y el encargado de realizar funciones de registro de inventario y de incidencia de fallas, asimismo, mantiene operativos y disponibles los servicios y recursos tecnológicos de hardware y de software empleado en el aula AIP e inspecciona la seguridad de la infraestructura TIC; Docentes de Aula y/o Asignatura, utiliza la infraestructura TIC del aula AIP con la intencionalidad de mejorar los aprendizajes de los Estudiantes y recibe el apoyo tecnológico del docente DAIP; Estudiantes, niños y niñas en edad escolar de Educación Básica Regular matriculados en un grado y sección del nivel primario o secundario. Utiliza la infraestructura TIC del aula AIP monitoreado por el docente de aula o docente de asignatura con la finalidad de mejorar sus aprendizajes con el soporte tecnológico del docente responsable de Aula de innovación.

III. Metodología

La investigación fue de tipo descriptivo propositivo por cuanto se fundamenta en la necesidad de gestionar los riesgos en la funcionalidad del equipamiento computacional en aulas AIP de las instituciones educativas de la provincia de Lambayeque con un enfoque asociado a los riesgos en equipos e instalaciones así como a la integridad y continuidad operativa de la infraestructura TIC [10] necesario para la sustentabilidad del equipamiento computacional [11].

La población estuvo conformada por 50 docentes de aulas AIP (DAIP) de las Instituciones Educativa de la provincia de Lambayeque y un docente experto en TIC para la educación. El tamaño de muestra es de 37 docentes DAIP calculado por muestreo para proporciones [12].

Se trabajó con la técnica de análisis documental respecto a los riesgos asociados a la instalación y equipamiento de las aulas AIP, asimismo se utilizó la encuesta para recabar información por medio de un cuestionario virtual, el cual se aplicó a los docentes DAIP responsables de las AIP con la finalidad que estos puedan evaluar la influencia de la gestión de riesgos en relación con la sustentabilidad del equipamiento computacional empleando un instrumento que abarca la dimensión de prevención de riesgos.

IV. Resultados

En el Proceso de evaluación de seguridad en aulas AIP de las Instituciones Educativas se ha constatado que su principal activo es el equipamiento computacional con el que cuentan (Fig.1), cuya vulnerabilidad a las amenazas externas (precipitaciones y condiciones ambientales) e internas (acumulación de polvo, corrosión), compromete la funcionalidad de la infraestructura TIC y susceptible al daño físico como lógico, cuyo impacto repercute considerablemente en el proceso enseñanza aprendizaje.

Con la finalidad de amortiguar el impacto negativo en el proceso enseñanza aprendizaje es necesario la implementación de medidas de prevención para disminuir la vulnerabilidad de las aulas AIP.

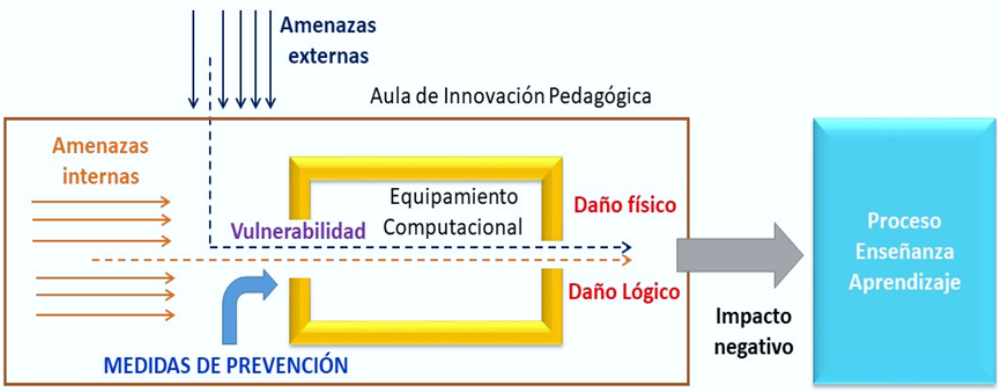

Fig. 1. Evaluación de seguridad en Aula de Innovación Pedagógica

Las principales medidas de prevención propuestas según el nivel de Riesgo Alto y Muy Alto, evaluadas por los docentes AIP son:

El polvo es un factor de Alto nivel de riesgo (Tabla 1) que provoca aislamiento térmico de los principales dispositivos y componentes electrónicos que dañan o provocan fallas de funcionamiento [15], motivo por el que se programa rutinas de mantenimiento preventivo para mejorar el funcionamiento del equipamiento computacional, así como minimizar el ingreso de polvo sustituyendo los vidrios de las ventanas.

Tabla 1. Medidas de prevención áreas seguras - daños físicos

Áreas seguras	Amenaza	Vulnerabilidad	Riesgo	Nivel de Riesgo	Medidas de prevención
Daños físicos	Polvo	- Acumulación excesiva de polvo en el interior del equipamiento computacional - Ventiladores defectuosos. - Ubicación del aula AIP en zona polvorienta. - Falta de mantenimiento preventivo.	- Refrigeración deficiente - Sobrecalentamiento del hardware. - Malfuncionamiento del equipamiento computacional. - Destrucción de dispositivos sensibles a la corriente por descarga estática.	- Alto - Alto - Muy Alto - Alto	- Programar rutinas de mantenimiento preventivo. - Realizar limpieza de polvo con aspiradora en el exterior e interior del aula de innovación. - Gestionar la sustitución de vidrios de ventanas.

Elaboración: Los autores

La calidad de energía eléctrica (Tabla 2) depende de la cadena de valor de los sistemas eléctricos (generación, transmisión, distribución), sin embargo, un alto nivel de calidad requiere de un buen sistema de puesta a tierra y de instalaciones eléctricas que cumplan con los estándares establecidos desde la fuente de suministro hasta el punto de suministro. Asimismo, un buen mantenimiento de del sistema de tierra de una aula AIP evitaría los problemas de interrupciones y perturbaciones en el suministro eléctrico debido a la variabilidad del voltaje y frecuencia en instalaciones eléctricas a causa de una elevada resistividad de los sistemas de puesta a tierra o por deficiencias en la continuidad en los sistemas de protección por acción de descargas eléctricas [16].

Tabla 2. Medidas de prevención en áreas seguras - pérdida de servicios esenciales

Áreas seguras	Amenaza	Vulnerabilidad	Riesgo	Nivel de Riesgo	Medidas de prevención
Pérdida de servicios esenciales	Energía eléctrica	- Falta de Ups - Puesta a tierra defectuosa o inexistente	- Afectación física a los usuarios de tecnología. - Falla en hardware o software por interrupción de energía eléctrica. - Pérdida de garantía. - Suspensión de la atención que brinda el Aula de innovación pedagógica por corte de servicio eléctrico.	- Alta - Muy Alta - Alta - Muy Alta	- Inspeccionar el sistema de puesta a tierra. - Programar rutinas de mantenimiento de la puesta a tierra. - Gestionar la adquisición de Ups para garantizar el funcionamiento de los recursos tecnológicos. - Gestionar la revisión del sistema de seguridad en el tablero de control. - Señalizar cables energizados.

Elaboración: Los autores

El extravío, la pérdida o robo de equipamiento computacional, es un evento que a nivel mundial se calcula en millones de unidades anuales, desde celulares, laptops hasta computadores de escritorio [17].

Las aulas AIP son lugares de riesgo (Tabla 3) por el contenido tecnológico que poseen y no están exentas de pérdidas o robos del equipamiento computacional y el enorme coste que ello implica para la renovación o restitución de la infraestructura perdida o dañada y su consecuente afectación al proceso educativo.

Con la finalidad que el servicio que brindan las aulas AIP se mantenga adecuadamente, es necesario que los accesos al aula AIP cuenten con seguridad confiable e inspeccionados constantemente.

Tabla 3. Medidas de prevención para seguridad de los equipos – perjuicio en equipamiento

Seguridad de los equipos	Amenaza	Vulnerabilidad	Riesgo	Nivel de Riesgo	Medidas de prevención
Perjuicio en equipamiento computacional	- Robo de equipos	- Puertas y ventanas del aula AIP sin rejas de protección. - Ausencia de cámaras de vigilancia. - Ausencia de alarmas contra robo. - Ausencia de personal de vigilancia	- Sustracción del equipamiento computacional tanto hardware como software. - Clausura del aula de AIP por no contar con el suficiente recurso tecnológico debido a la sustracción de sus equipos.	- Alto - Alto	- Inspeccionar los protectores de seguridad de puertas y ventanas. - Comprobar el funcionamiento de los sistemas de seguridad. - Gestionar la cobertura del aula AIP con sistemas de seguridad confiables.

Elaboración: Los autores

El principal activo de las aulas AIP están constituidos por la infraestructura TIC que brindan soporte tecnológico al servicio educativo, es por este motivo que el mantenimiento y reparación del equipo computacional (Tabla 4) debe ser ejecutado siguiendo protocolos establecidos y procedimientos de buenas prácticas coadyuvado con los instrumentos y herramientas físicas y lógicas para que el servicio se reestablezca en el menor tiempo posible [18].

Tabla 4. Medidas de prevención para seguridad de los equipos - Fallas técnicas

Seguridad de los equipos	Amenaza	Vulnerabilidad	Riesgo	Nivel de Riesgo	Medidas de prevención
Fallas técnicas	- Mala práctica en la mantenibilidad.	- Falta de protocolos para la realización del proceso de mantenibilidad del equipamiento computacional. - Déficit de herramientas para la reparación y mantenimiento de equipos de cómputo.	- Personal ejecuta rutinas de mantenimiento y reparación sin contar con la debida capacitación, asimismo - Personal utiliza herramientas e instrumentos incorrectos para la realización de determinada acción	- Alto - Alto	- Verificar la acreditación del personal para la realización del proceso de mantenibilidad del equipamiento computacional. - Gestionar la adquisición de instrumentos y herramientas para el mantenimiento y reparación.

Elaboración: Los autores

Conclusiones

Se diagnosticó el estado actual de vulnerabilidad del equipamiento computacional frente a las amenazas externas e internas que impactan en el proceso educativo de los estudiantes.

Se elaboró el plan de gestión de riesgos en aulas AIP con la finalidad de proteger el equipamiento computacional frente a las amenazas externas e internas, las vulnerabilidades y los riesgos potenciales que afectan el proceso de aprendizaje de los estudiantes.

Se evaluó la seguridad en aulas AIP de los activos computacionales en áreas seguras y seguridad de equipos obteniendo niveles de riesgo alto y muy alto que comprometen la funcionalidad de la infraestructura TIC y consecuente perjuicio al servicio educativo de los estudiantes, por lo que se plantearon medidas de prevención para mitigar los efectos adversos.

Referencias

[1] M. F. Molina Miranda, "Propuesta de un plan de gestión de riesgos de tecnología aplicado en la Escuela Superior Politécnica del Litoral," Universidad Politécnica de Madrid, 2015. [Online]. Available: http://www.dit.upm.es/~posgrado/doc/TFM/TFMs2014-2015/TFM_Maria_Fernanda_Molina_Miranda_2015.pdf
[2] W. M. Barrera, Ricardo Jesús; Sánchez Delgado, Maritza del Pilar; Rojas Contreras, "Modelo de gestión del riesgo en proyectos informáticos Mogripi Model," I+D Rev. Investig., vol. 8, no. 2, pp. 15–24, 2016, doi: https://doi.org/10.33304/revinv.v08n2-2016002.
[3] M. Erb, "Gestión de riesgo en la seguridad informática," 2020. https://protejete.wordpress.com/gdr_principal/ (accessed Dec. 22, 2020).
[4] M. I. Romero et al., Introducción a la seguridad informática y el análisis de vulnerabilidades. Alicante: Área de Innovación y Desarrollo,S.L., 2018. doi: http://dx.doi.org/10.17993/IngyTec.2018.46.
[5] L. Salazar, L. Cortez, and J. Mariscal, "Gestion comunitaria de riesgos," Foro Ciudad. para la vida, vol. 2, pp. 1–21, 2002, [Online]. Available: file:///C:/Users/Personal/Desktop/BIBLIOGRAFIA/VULNERABLIDAD/GES COM RIE - Peru.pdf

[6] H. D. Díaz Tamayo, Alejandra María; Gil Mayorga, Jorge Iván; Arboleda Millán, Gestión del riesgo en instituciones educativas, vol. 18. Lima - Perú: Soluciones Pácticas, 2015. [Online]. Available: http://eds.b.ebscohost.com/eds/detail/detail?vid=0&sid=b55c7f51-edd9-4512-985a-95a8364e5f7c%40sessionmgr101&bdata=JkF1dGhUeXBlPXNzbyZsYW5nPWVzJnNpdGU9ZWRzLWxpdmUmc2NvcGU9c2l0ZQ%3D%3D#db=asn&AN=124305155

[7] J. S. Sánchez Garreta, R. Chalmeta Rosaleñ, O. Coltelll Simon, P. Monfort Manero, and C. Campos Sanchez, Ingeniería de proyectos informáticos: Actividades y procedimientos. Castelló, España: UNIVERSIDAD JAUME I. SERVICIO DE COMUNICACION Y PUBLICACIONE, 2003.

[8] E. Edel Navarro, Ruben; Colorado Aguilar, Brenda Luz; Del Hierro Para, "Usabilidad de las tecnologías de la información y comunicación (TIC) en el desarrollo de competencias docentes," in Actores y recursos educativos, Mexico: Pearson Educación, 2014, pp. 123–133. [Online]. Available: https://www.researchgate.net/publication/328269020_Usabilidad_de_las_tecnologias_de_la_informacion_y_comunicacion_TIC_en_el_desarrollo_de_competencias_docentes

[9] A. Lopez Neira and J. Ruiz Sphor, "Seguridad física y ambiental-Anexo 11 ISO 27001," 2020. https://www.iso27000.es/iso27002_11.html (accessed Dec. 27, 2020).

[10] Dupont Sustainable Solutions, "Nuevos paradigmas y postulados en la gestión de riesgos," 2021. [Online]. Available: https://latam.consultdss.com/content/dam/files/products-and-services/consulting-services-and-process-technologies-redesign/operational-risk-management/documents/nuevos-paradigmas-informacion.pdf

[11] P. Martínez Moreno, J. A. Vergara Camacho, and J. Pino Herrera, "La sustentabilidad en equipos de cómputo portátiles. Un estudio experimental," RECAI Rev. Estud. en Contaduría, Adm. e Informática, vol. 25, pp. 1–16, 2020, doi: 10.36677/recai.v9i25.13215.

[12] A. Rodriguez Dominguez and M. García Minjares, Estadística II, vol. 01, no. 01. México: Sistema Universidad Abierta yEducación a Distancia, 2013. [Online]. Available: http://fcasua.contad.unam.mx/apuntes/interiores/docs/20172/contaduria/3/apunte/LC_1353_03106_A_estadisticaII.pdf

[13] Y. A. Sánchez, C. J. A. P. Soler, and C. F. M. Delgado, "Procedimiento para determinar el impacto de la gestión de riesgos en la sostenibilidad de las organizaciones," Dir. y Organ., vol. 73, no. 73, pp. 39–49, 2021, doi: 10.37610/DYO.V0I73.591.

[14] I. H. Solana González, Pedro; Bello Pérez, Rafael E; Garcia Lorenzo, Maria Matilde; Vanti, Adolfo Alberto; Vey, "Data Mining para evaluar el riesgo operativo en procesos tecnológicos," Perspect. em Gestão Conhecimento, João Pessoa, vol. 9, no. 2, pp. 40–55, 2019, doi: http://dx.doi.org/10.21714/2236-417X2019v9n2p40.

[15] E. Monroy Garcia, "Análisis de fallas de una computadora personal en el Perú enfocados desde el punto de vista de mantenimiento, análisis térmico y refrigeración, utilizando modelo simulado por software," 8o Congr. Iberoam. Ing. Mec., no. 18, p. 8, 2007, doi: 10.1016/j.riai.2012.02.005.

[16] M. Polo, J. Bernardo, and J. B. Peña, "Calidad de la energía eléctrica bajo la perspectiva de los sistemas de puesta a tierra," Cienc. e Ing., vol. 38, no. 2, pp. 167–176, 2017.

[17] J. Ranchal, "10 consejos para prevenir la pérdida o robo de un dispositivo electrónico," 25/01/2017, 2017. https://www.muycomputer.com/2017/01/25/robo-de-un-dispositivo/ (accessed Jan. 02, 2022).

[18] M. Marquez, "Gestion de mantenimiento," in Manual de Ingeniería de la Calidad, Caracas, 2010, p. 34. [Online]. Available: http://repository.unimilitar.edu.co:8080/bitstream/10654/11765/1/SISTEMAS DE GESTIÓN DE CALIDAD INTEGRADOS %28HSEQ%29%2C CÓMO ALTERNATIVA A LOS DESAFÍOS ECONÓMICOS%2C SOCIALES Y AMBIENTALES DEL MANTENIMIENTO AERONÁUTICO .pdf

Los autores

José Fortunato Zuloaga Cachay, Ingeniero de Sistemas y Computación, Doctor en Ciencias de la Computación y Sistemas, docente adscrito al Departamento de Ingeniería de la Universidad Católica Santo Toribio de Mogrovejo Chiclayo Perú.

Freddy William Campos Flores, Ingeniero en Computación e Informática. Maestro en Ingeniería de Sistemas, estudiante del Doctorado en Educación de la Universidad César Vallejo, Chiclayo Perú.

Denny John Fuentes Adrianzén, Ingeniero Informático y de Sistemas, Maestro en Administración con Mención en Gerencia Empresarial, Doctor en Ciencias de la Computación y Sistemas. Adscrito al Departamento Académico de Computación y Electrónica de la Universidad Nacional Pedro Ruiz Gallo de Lambayeque, Perú.

Johnny Cueva Valdivia, Ingeniero Informático y de Sistemas, Magister en Docencia Universitaria y Gerencia Educativa, Doctor en Gestión Pública y Gobernabilidad. Adscrito al Departamento Académico de Ingeniería de Sistemas y Telecomunicaciones de la Universidad Nacional Santiago Antúnez de Mayolo de Huaraz, Ancash, Perú.