InvestiGO
Revista Científica Multidisciplinaria
ISSN 2953-6367
http://revistainvestigo.com

Julio - diciembre 2026
Vol. 7 No. 20, PP. 941-963
https://doi.org/10.56519/6x3eg917

DIAGNÓSTICO Y PLAN DE MEJORA DE LA CIBERSEGURIDAD EN LOS LABORATORIOS DE CÓMPUTO DE LA FACULTAD DE ADMINISTRACIÓN DE EMPRESAS - ESPOCH

CYBERSECURITY ASSESSMENT AND IMPROVEMENT PLAN FOR THE COMPUTER LABORATORIES OF THE FACULTY OF BUSINESS ADMINISTRATION AT ESPOCH

Byron Napoleón Cadena Oleas [1], Anjuly Michelle Villagómez Puebla [2], Carlos Patricio Arguello Mendoza[3], Oscar Iván Granizo Paredes [4], Willian Geovanny Yanza Chávez[5]

{bcadena@espoch.edu.ec [1], anjuly.villagomez@espoch.edu.ec[2], carguello@espoch.edu.ec [3], ogranizo@espoch.edu.ec [4], willian.yanza@espoch.edu.ec[5])

Fecha de recepción: 16/06/2026 / Fecha de aceptación: 08/07/2026 / Fecha de publicación: 08/07/2026

RESUMEN: Hoy en día, la rápida evolución tecnológica en las universidades ha hecho que proteger la infraestructura digital y la información académica sea más urgente que nunca. Bajo esa premisa, este trabajo se enfocó en evaluar el estado real de la seguridad informática en los laboratorios de cómputo de la Facultad de Administración de Empresas de la Escuela Superior Politécnica de Chimborazo (ESPOCH). La meta final de la investigación fue diseñar un plan de acción concreto que asegure la confidencialidad, integridad y disponibilidad de todos los datos. Para lograrlo, se llevó a cabo un estudio descriptivo con un enfoque mixto, combinando metodologías cualitativas y cuantitativas. La recolección de datos se hizo directamente en el lugar mediante una lista de verificación respondida por el encargado técnico del área, además de encuestas estructuradas para los profesores y los estudiantes. Los resultados de este diagnóstico sacaron a la luz problemas institucionales serios, donde sobresalen la falta de normativas de seguridad claras, la ausencia de sistemas de autenticación y la falta de copias de seguridad para los archivos. De igual forma, se detectaron fallas en el control de acceso a las salas, una respuesta muy lenta ante incidentes y un nivel de cultura digital bastante bajo en la comunidad respecto a los riesgos informáticos. A partir de este escenario, se estructuró una propuesta de mejora que incluye la creación de reglamentos internos, controles de ingreso más

[1]Escuela Superior Politécnica de Chimborazo (ESPOCH), Facultad de Administración de Empresas, Riobamba - Ecuador, https://orcid.org/0000-0002-4535-5265
[2]Escuela Superior Politécnica de Chimborazo (ESPOCH), Dirección de Comunicación, Riobamba – Ecuador, https://orcid.org/ 0009-0008-1371-7314
[3]Escuela Superior Politécnica de Chimborazo (ESPOCH), Facultad de Administración de Empresas – Ecuador, https://orcid.org/ 0000-0001-6672-2610
[4]Escuela Superior Politécnica de Chimborazo (ESPOCH), Facultad de Administración de Empresas – Ecuador, https://orcid.org/0009-0008-6965-8333
[5]Escuela Superior Politécnica de Chimborazo (ESPOCH), Facultad de Administración de Empresas – Ecuador, https://orcid.org/0000-0002-9688-7309

estrictos, cronogramas de respaldo de datos, la actualización de los planes de contingencia y talleres de capacitación. Implementar estas medidas ayudará a mitigar las amenazas detectadas y a optimizar la gestión de la seguridad, logrando un entorno tecnológico mucho más blindado y confiable para toda la universidad.

Palabras clave: Ciberseguridad, seguridad de la información, gestión de riesgos, laboratorios de cómputo, educación superior, ESPOCH

ABSTRACT: Today, rapid technological advancements at universities have made protecting digital infrastructure and academic information more urgent than ever. With this in mind, this study focused on assessing the actual state of IT security in the computer labs of the School of Business Administration at the Escuela Superior Politécnica de Chimborazo (ESPOCH). The ultimate goal of the research was to design a concrete action plan to ensure the confidentiality, integrity, and availability of all data. To achieve this, a descriptive study with a mixed-methods approach was conducted, combining qualitative and quantitative methodologies. Data collection was carried out on-site using a checklist completed by the area's technical manager, as well as structured surveys for faculty and students. The results of this assessment brought to light serious institutional problems, most notably the lack of clear security policies, the absence of authentication systems, and the lack of backup copies for files. Similarly, flaws were detected in access control to the rooms, a very slow response to incidents, and a fairly low level of digital literacy within the community regarding IT risks. Based on this assessment, an improvement plan was developed that includes the creation of internal regulations, stricter access controls, data backup schedules, the updating of contingency plans, and training workshops. Implementing these measures will help mitigate the identified threats and optimize security management, resulting in a much more secure and reliable technological environment for the entire university.

Keywords: Cybersecurity, information security, risk management, computer laboratories, higher education, ESPOCH

INTRODUCCIÓN

En la era digitalización, la ciberseguridad constituye un aspecto esencial para proteger los datos, la información y los sistemas frente a amenazas cada vez más sofisticadas, el Ecuador no es ajeno a esta realidad mundial. Con el aumento de la conectividad y el uso de tecnologías de la información (1), tanto en las empresas como las personas se enfrentan a nuevos retos y desafíos en cuanto a seguridad de la información. Desde la protección de datos personales hasta la seguridad de los recursos informáticos y su infraestructura.

El equipo de Experto en Ciencia y Tecnología, de la Universidad Internacional de Valencia sobre el análisis de la ciberseguridad en el Ecuador, refieren que:

La seguridad informática es fundamental para prevenir y mitigar los riesgos asociados al uso de los recursos tecnológicos. En este contexto, se destacan varios tipos de medidas, esenciales tanto

para empresas como para las personas. Esta clase de recursos, que van desde los cortafuegos de siempre hasta programas antivirus y sistemas que detectan intrusos, son esenciales para sostener una red bien protegida. Por suerte, el mercado tecnológico actual ofrece una gran variedad de plataformas especializadas que facilitan el control diario de estos niveles de defensa, haciendo que su administración sea mucho más sencilla (1).

Al mirar el escenario en Ecuador, las normativas y políticas del gobierno son fundamentales para fijar los estándares mínimos que orientan la ciberseguridad a nivel nacional. A pesar de esto, el compromiso no es exclusivo del sector público; el verdadero desafío lo tienen las organizaciones y los propios usuarios, quienes necesitan incorporar hábitos seguros y acciones de prevención para proteger sus datos cotidianamente (1).

Lo cierto es que, en el último tiempo, el entorno digital del país se ha vuelto un tema crítico, sobre todo por la ola de ataques cibernéticos y brechas de seguridad que han golpeado a ministerios y empresas privadas. Vivir completamente conectados ha expuesto fallas profundas que exigen soluciones urgentes. Hoy por hoy, las prioridades locales se centran en proteger la privacidad de los datos personales, blindar los sistemas financieros y combatir tanto el malware como el robo físico de los dispositivos de cómputo (1).

El avance en las herramientas de seguridad informática es crucial para enfrentar estos desafíos. En Ecuador, se han implementado soluciones tecnológicas avanzadas, como sistemas de detección y respuesta ante intrusos, cifrado de datos y autenticación multifactorial y seguridades físicas con apoyo de la tecnología. Además, se promueve la capacitación continua del personal encargado de gestionar la seguridad de la información, lo que garantiza una respuesta efectiva ante posibles incidentes. A medida que Ecuador avanza hacia un entorno digital más seguro, es esencial continuar invirtiendo en tecnología, infraestructura y educación para fortalecer las capacidades nacionales frente a las amenazas cibernéticas (1).

Por otra parte, en el contexto de la educación superior, los aspectos relacionados a la ciberseguridad generan una preocupación, ya que existe una carencia de profesionales capacitados en esta temática, generando la necesidad de rediseñar planes de estudio de carreras profesionales inherentes a los Sistemas de Información (2), o, a su vez, crear carreras profesionales de ciberseguridad, de modo que permita satisfacer las necesidades del contexto actual a nivel de usuario y a nivel empresarial (3).

La Escuela Superior Politécnica de Chimborazo (ESPOCH) es una institución de Educación Superior Pública, con personería jurídica, autonomía administrativa y financiera, su presupuesto es otorgado por el estado ecuatoriano, con ello, busca garantizar una formación integral para sus estudiantes de grado, posgrado y educación continua con calidad y pertinencia social, generando así un aporte al desarrollo sustentable y sostenible del país, en la actualidad cuenta con 17.232 estudiantes (3); tiene 3 sedes, 47 carreras y 7 facultades, una de ellas, la Facultad de Administración de empresas (FADE).

Esta Facultad empresas cuenta con 5 carreras: Administración de empresas, Contabilidad y auditoría, Mercadotecnia, Finanzas y Gestión del transporte, con un total de 2.241 estudiantes y

60 docentes (4). Parte de sus actividades académicas se realizan en el Centro de Cómputo, que principalmente acoge a docentes y estudiantes en asignaturas en las que se requiere el uso de sistemas, plataformas o aplicaciones informáticas propias para el desarrollo de cada asignatura; el centro de cómputo, cuenta con 7 laboratorios y dos personas encargadas de gestionar su uso y mantenimiento.

A pesar de que se viene desarrollando sus actividades de manera regular, es importante observar algunos aspectos que afectan la seguridad de la información relacionada a las funciones propias que cumple el centro de cómputo, comprometiendo la confidencialidad, integridad y disponibilidad de la información. No se advierten controles hacia las personas, controles físicos y tecnológicos, comprometiendo tanto la seguridad física como lógica de los recursos informáticos. Los dispositivos informáticos, computadores, red de datos, accesos inalámbricos, programas informáticos, telecomunicaciones, bases de datos, teléfonos celulares e Internet, son grandes herramientas para la generación y almacenamiento de datos personales y confidenciales que pueden ser fácilmente vulnerados por el uso indebido o inadecuado de todos estos recursos.

Hoy en día analizar los riesgos, identificar vulnerabilidades y amenazas, comprobar el origen de los ataques e incluso identificar a un atacante puede ser una tarea realmente difícil (5), gestionarlos es un aspecto que requiere formación o especialización en temas Informáticos y de seguridad. Los atacantes buscan vulnerabilidades, identificarlas permitirá evitar la pérdida o mal uso de información, el daño o deterioro recursos informáticos, lo que se constituye a través de este trabajo de fin de cursos en uno de los principales propósitos, al mismo tiempo entregar a través de un plan de acción, estrategias y actividades que permitan mejorar la gestión del centro de cómputo como apoyo a la gestión docente.

La seguridad de la información

Cuidar los recursos digitales se ha vuelto un pilar fundamental para toda organización que maneje volúmenes de datos, puesto que exige el desarrollo de estrategias, reglas de juego internas y soluciones tecnológicas enfocadas en neutralizar peligros tanto de adentro como de afuera. Esta metodología de trabajo se basa por completo en tres pilares clave: asegurar que solo entren las personas autorizadas, cuidar la veracidad de la información y mantener las plataformas siempre operativas, elementos que juntos conforman la famosa tríada CID (6)

Cuando observamos el día a día de las organizaciones, el activo tecnológico que se necesita blindar es sumamente variado; incluye desde documentos en físico y bases de datos estructuradas, hasta programas informáticos, equipos físicos y los manuales de procesos internos. Reducir las amenazas en un ecosistema tan complejo exige una visión global, que necesariamente debe arrancar con un análisis sincero sobre las vulnerabilidades de la institución para, a partir de ahí, aplicar controles que eviten problemas o permitan actuar de inmediato si algo sale mal (6).

Contextualización de la ciberseguridad en las empresas

Hoy la ciberseguridad se ha consolidado como un eje indispensable para resguardar la información y los sistemas tecnológicos dentro del mundo de los negocios. A medida que la digitalización de las empresas se acelera, las organizaciones tienen que lidiar con un incremento alarmante tanto en la cantidad como en la complejidad de las agresiones digitales. Estos peligros varían bastante en su forma, yendo desde el secuestro de archivos mediante ransomware para exigir un rescate económico, hasta la filtración de información confidencial provocada por trampas de ingeniería social como el phishing o por fallas de seguridad que quedan abiertas en sus propios sistemas operativos.

La ciberseguridad se define como el conjunto de prácticas, tecnologías y procesos que se implementan para proteger sistemas, redes y datos frente a accesos no autorizados, interrupciones o daños. Este ámbito no solo abarca la defensa contra atacantes externos, sino también la gestión de amenazas internas y la prevención de errores humanos.

De la misma forma, En el contexto empresarial, la ciberseguridad se enfrenta a retos complejos y en constante evolución (6), entre los que destacan:

Adopción de nuevas tecnologías

La transformación digital ha acelerado la adopción de servicios en la nube, dispositivos IoT y plataformas de colaboración remota. Si bien es cierto que estas innovaciones mejoran la eficiencia en el trabajo y agilizan la comunicación, la realidad es que también abren una ventana mucho más grande a los riesgos informáticos en las empresas. Las bandas cibernéticas aprovechan constantemente el más mínimo fallo en estas plataformas digitales para coordinar ataques dirigidos, robar propiedad intelectual o paralizar operaciones comerciales que son críticas. Un caso muy común ocurre cuando hay un descuido en la separación de las redes que conectan los dispositivos del Internet de las Cosas (IoT); esta falta de control hace posible que un intruso termine metiéndose en los servidores corporativos más privados, usando como trampolín un aparato de oficina que parecía del todo inofensivo.

Cumplimiento normativo

Leyes internacionales como el RGPD, las normativas destinadas a blindar las Infraestructuras Críticas y las reglas particulares de industrias como la banca o la salud imponen estándares de seguridad sumamente estrictos a la hora de manejar información digital. Ignorar estas exigencias jurídicas no solo conlleva multas económicas muy pesadas, sino que además destruye por completo la credibilidad de la empresa ante sus clientes, proveedores y aliados comerciales.

Por esta razón, las instituciones se ven obligadas a desarrollar modelos de gobernanza sólidos y globales. Estos sistemas de gestión tienen que sostenerse en auditorías técnicas constantes, análisis detallados sobre cómo se verían afectadas las operaciones ante un incidente, y una política de supervisión totalmente clara en lo que respecta al manejo y uso de los datos en el día a día.

Concienciación del personal

Dentro de cualquier empresa, el personal representa normalmente la parte más débil de toda la estrategia de defensa. Tácticas como el robo de identidad por correo y la ingeniería social consiguen resultados muy efectivos precisamente por el desconocimiento de los empleados y por esas pequeñas desatenciones del día a día causadas por la prisa del trabajo.

Si se quiere reducir este riesgo, es fundamental diseñar talleres continuos de capacitación en seguridad digital. Estas jornadas formativas tienen que trascender las típicas explicaciones teóricas y aburridas; lo ideal es incluir simulacros de ataques reales, dar instrucciones sencillas sobre cómo tratar los datos confidenciales y ofrecer canales directos para avisar sobre cualquier sospecha, creando un ambiente seguro donde la gente pueda alertar de un error sin miedo a ser castigada o señalada. Además, la capacitación debe estar adaptada a los diferentes roles dentro de la organización, asegurando que todos comprenden las amenazas específicas que enfrentan (6).

A manera de resumen, los retos de seguridad se puedan apreciar en la Figura 1.

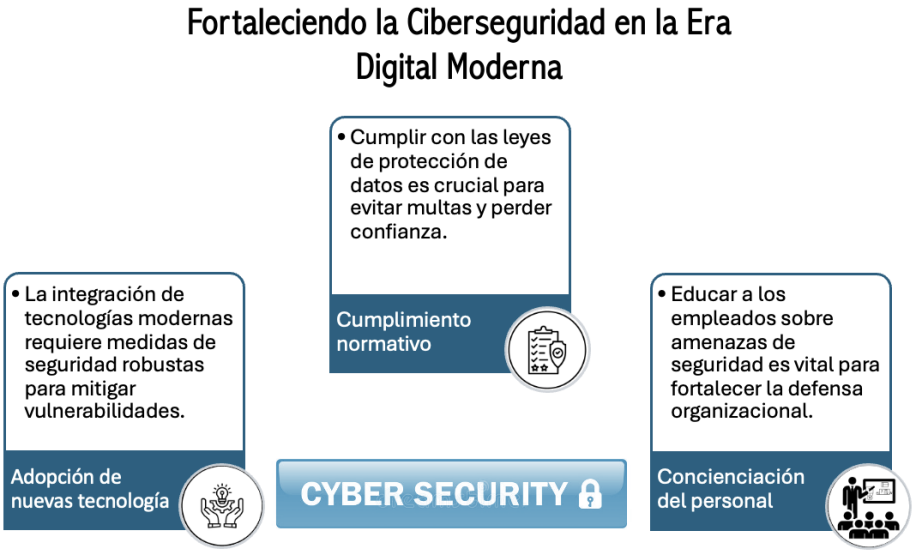

Figura 1. Retos de la ciberseguridad en el contexto empresarial.

Las estrategias modernas de ciberseguridad incluyen el uso de herramientas avanzadas como sistemas de detección de intrusos, firewalls de próxima generación y soluciones de inteligencia artificial que detectan patrones de comportamiento anómalos. Además, se fomenta la implementación de principios como "cero confianza" (Zero Trust), que limitan el acceso de los usuarios y dispositivos únicamente a los recursos estrictamente necesarios.

¿Qué es la tríada CID?

La tríada CID es un acrónimo de confidencialidad, integridad, disponibilidad que es la estructura principal de la toda empresa en relación a la seguridad de la información (7). Si la infraestructura tecnológica, aplicaciones, bases de datos o sitios web han sido vulnerados, o incluso si hay una

fuga importante de información confidencial (contraseñas, datos personales, copias de seguridad, etc.), significa que se ha violentado al menos una de las tres dimensiones de la tríada (8).

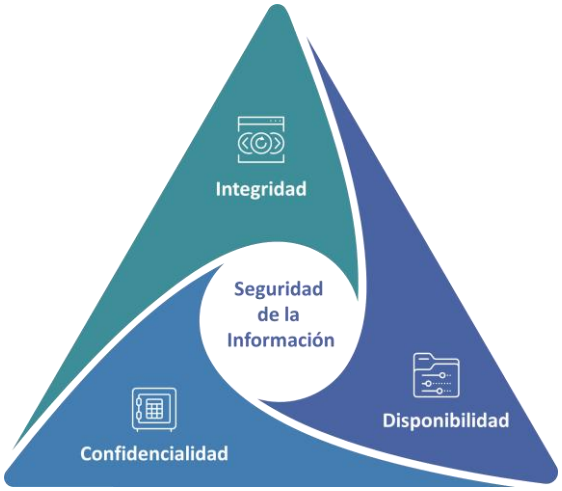

Figura 2. Principios de la seguridad de la información.

A continuación, se presentan los conceptos relacionados a la triada CID:

Confidencialidad

La confidencialidad de la información significa que se deben tomar medidas para protegerla del acceso no autorizado. Una forma de lograrlo es imponiendo diferentes niveles de acceso a la información según quién necesita acceso y qué tan confidencial es la información. Algunos medios para gestionar la confidencialidad incluyen cifrado de archivos y volúmenes, listas de control de acceso y permisos de archivos.

Integridad

La integridad de los datos es una parte integral de la tríada de seguridad de la información, cuyo objetivo es proteger los datos de modificaciones o eliminaciones no autorizadas. Esto también implica garantizar que los cambios o eliminaciones no autorizados realizados en los datos puedan deshacerse.

Disponibilidad

La disponibilidad tiene como objetivo garantizar que los datos sean accesibles para quienes los necesitan cuando sea necesario. Algunos de los riesgos de seguridad de la información relacionados con la disponibilidad incluyen sabotaje, corrupción del hardware, fallas de la red y cortes de energía. Estos tres componentes de la seguridad de la información funcionan de la mano y no es posible concentrarse en uno de ellos a expensas de los demás (9).

La gestión del riesgo

El riesgo es el resultado de la incertidumbre sobre los objetivos. Se trata, en esencia, de casos o eventos adversos que impiden el normal desarrollo de las actividades de una empresa y que, por lo general, tienen incidencias económicas para las organizaciones (10).

De manera simple, podemos definir el riesgo como la combinación de la probabilidad de ocurrencia de un evento y sus consecuencias (11).

Para el negocio en general, el riesgo está relacionado a la incertidumbre de los probables daños de un evento inesperado sobre el logro de los objetivos establecidos (12).

Por otra parte, se manifiesta que el Riesgo de seguridad es una combinación de amenazas, vulnerabilidades e impactos. Las amenazas son eventos que aprovechan las vulnerabilidades (debilidades) y pueden causar daños. El impacto es el resultado de una vulnerabilidad al ser explotada por una amenaza (13).

En cuanto a la gestión del riesgo, algunas definiciones se consideran importantes y se presentan a continuación:

- La gestión del riesgo incluye todas las medidas adoptadas para controlar los riesgos en una organización, incluyendo el análisis/ evaluación, el tratamiento, la aceptación y la comunicación de los riesgos.
- El análisis de riesgos identifica y estima los riesgos, teniendo en cuenta el uso sistemático de la información. Abarca el análisis de las amenazas, vulnerabilidades e impactos y se considera el punto clave de la política de seguridad de la información de una organización.
- La evaluación del riesgo compara el riesgo estimado en el análisis con los criterios predefinidos con el fin de identificar la importancia de cada riesgo para la organización.
- Aceptación de riesgos incluye la identificación del nivel aceptable de riesgos para una organización en función de sus necesidades específicas de negocio y seguridad.
- El tratamiento del riesgo corresponde a la selección y la aplicación de medidas para modificar un determinado riesgo.

La comunicación de riesgos involucra iniciativas para mostrar los riesgos a los empleados, directivos y terceros (estos últimos, cuando sea apropiado y necesario).

Como se puede apreciar se consideran los términos que están asociados a la seguridad de la información y el tratamiento del riego: Las vulnerabilidades y amenazar, misma que se tratan a continuación.

Vulnerabilidades y amenazas

Después de identificar los activos que deben ser protegidos en la organización, se deben considerar las probabilidades de cada activo de ser vulnerable a las amenazas. Para ello, hay que prestar atención a la información que pueda quedar comprometida, creando listas de prioridades, por ejemplo; y los servicios de seguridad que puedan verse comprometidos, tal como la confidencialidad, integridad y disponibilidad.

Ejemplos de amenazas típicas:

- Amenazas provocadas por la naturaleza.
- Cortes de electricidad.
- Interrupciones por fallas de hardware.
- Interrupciones por fallas de software.
- Robo.
- Fraudes.
- Errores de la personas (dolosas o culposas).

A continuación, se presentan algunas de las amenazas típicas en entornos de las TI:

- Los desastres naturales que afectan a la instalación física de la organización. Durante el desastre, los controles de acceso físico pueden verse comprometidos y algunos recursos con información sensible se pueden violar con facilidad.
- Las fallas en el suministro eléctrico, que afectan a la parte de hardware de la organización. Con el hardware dañado, los servicios no estén disponibles.
- Amenazas programadas tales como virus y bombas lógicas que afectan software. Por lo tanto, los códigos no autorizados pueden revelar la información confidencial al mundo exterior, tal como contraseñas.
- Las fallas de hardware. De este modo, la máquina comprometida puede ser enviada a mantenimiento sin el previo cuidado de borrar la información confidencial contenida en los mismos. » Las fallas de software, corrompiendo lo datos.
- Los errores humanos que afectan a cualquier sistema de la organización, permitiendo así la revelación de información confidencial; por ejemplo, imprimir información confidencial en una impresora pública.

El análisis de riesgos debe medir las amenazas, las vulnerabilidades y los impactos de modo que el resultado pueda servir como guía para la adopción de medidas de seguridad adecuadas a los requisitos de negocio de la organización, teniendo en cuenta, por lo tanto, costos asociados, nivel de protección requerido por los activos y facilidad de uso.

En particular, se puede considerar el análisis de riesgos en términos cualitativos, con el fin de cumplir con los requerimientos del negocio, o en términos cuantitativos, con el fin de asegurar que los costos de las medidas preventivas, correctivas e ilustrativas no superen el valor del activo en cuestión, en lo que se refiere al patrimonio de la organización y también a la continuidad del negocio (13).

MATERIALES Y MÉTODOS

Métodos de análisis de riesgos

Existen tres métodos utilizados para determinar el nivel o magnitud del riesgo (14). Estos son cualitativos, cuantitativos y semicuantitativos, a efectos del tratamiento del presente trabajo, abordaremos 2 de ellos:

Métodos cualitativos

Este método de análisis de riesgos es el más usado. Se aplica una valoración realizada a través de las características de un escenario de amenazas sobre los activos, y generalmente está asociado a una ponderación de los riesgos que utiliza como parámetros cualidades como alto, medio o bajo (14).

Debido a que cada persona posee un concepto específico de lo que representa una característica «alta, media o baja», como una manera de clasificación, la evaluación cualitativa puede convertirse en un elemento subjetivo, por lo que es importante definir criterios precisos de lo que cada categoría representa (14).

Para determinar el nivel de riesgo (alto, medio o bajo) aplicando el método cualitativo, podemos valernos de una o varias de las siguientes actividades: Lluvia de ideas (brainstorming), juicio de los auditores, cuestionario y entrevistas estructuradas, evaluación para grupos multidisciplinarios (14).

Métodos Cuantitativos

La evaluación cuantitativa tiene como propósito asignar valores numéricos a riesgos específicos, por lo que tiene como punto de partida en este trabajo de fin de cursos, la determinación de calificaciones asociadas a la materialización de una o más amenazas (14).

Generalmente, resulta necesaria llevar a cabo una evaluación cuantitativa (si se compara con una cualitativa), entre otras razones, porque esta evaluación considera un conjunto de variables a las cuales se les debe asignar un valor numérico que permita obtener resultados con mayor precisión y que esté apegado a la realidad de los riesgos de la información y activos de la empresa (14).

El uso de modelos matemáticos y estadísticos como el cálculo de niveles de confianza y de riesgos, frecuencias, porcentajes, entre otros, agregan objetividad a los resultados de la evaluación, ya que, con los mismos valores utilizados durante el cálculo, se obtienen resultados consistentes (14).

Población de estudio y muestra

Entendiendo que el colectivo politécnico que hacen uso y gestionan los laboratorios de cómputo de la Facultad de Administración de Empresas, está integrado por: Docentes, estudiantes y personal técnico y administrativo, se consideró a los grupos mencionados como la población de estudio.

Según los datos proporcionados por la administración del centro de cómputo, los grupos de estudio se componen de la siguiente manera:

Tabla 1. Composición de los grupos de estudio.

Grupo	N° de personas
Personal técnico - administrativo	1
Docentes	18
Estudiantes	1450

Fuente: Marco Ortiz. Técnico responsable del centro de cómputo.

En consideración al tamaño de los grupos poblacionales, se considera aplicar el muestreo únicamente a los estudiantes que hacen uso de los laboratorios.

Para ello, se utilizará la fórmula para el cálculo de la muestra para poblaciones finitas:

$$n = \frac{N * Z^2 * p * q}{e^2 * (N-1) + Z^2 * p * q}$$

En donde:

N	Población	1450
Z	Nivel de confianza	1,96
p	Probabilidad de ocurrencia	0,5
q	Probabilidad de no ocurrencia	0,5
e	Margen de error	10%
n	Muestra	A calcular

Reemplazando los datos en la fórmula, se obtiene los siguientes resultados:

$$n = \frac{1450 * 1{,}96^2 * 0{,}5 * q0{,}5}{0{,}10^2 * (1450-1) + 1{,}96^2 * 0{,}5 * 0{,}5}$$

$$n = 304 \text{ estudiantes}$$

Técnicas e instrumentos

Se considera la utilización de las siguientes técnicas por grupo de estudio:

Tabla 2. Técnicas e instrumentos.

Grupo	Técnica	Instrumento
Personal administrativo	Entrevista	Guía de entrevista
	Cuestionario de control	Cuestionario
Docentes	Encuesta	Cuestionario

Estudiantes	Encuesta	Cuestionario

Realizado por: Los autores

RESULTADOS Y DISCUSIÓN

1. Análisis cuestionario de control aplicado al personal administrativo

Tabla 3. Cuestionario de control (CID) Personal técnico – administrativo.

CID	N°	PREGUNTAS	SI	NO	POND.	CALIF.	OBSERVACIÓN
CONFIDENCIALIDAD	P1	Los accesos a los laboratorios de cómputo están controlados adecuadamente para evitar el ingreso de personas no autorizadas. (Confidencialidad)	X		10	**7**	Si, pero únicamente con responsabilidad del docente. Solo si está el docente presente, los estudiantes pueden ingresar
	p2	Existen políticas claras sobre el uso de cuentas, contraseñas y perfiles de usuario en los equipos del laboratorio. (Confidencialidad)		X	10	**5**	No, los equipos se utilizan sin autenticación. Para la red Wifi, cada usuario ingresa con credenciales individuales.
INTEGRIDAD	P3	Los sistemas y equipos del laboratorio cuentan con mecanismos que evitan la alteración no autorizada de la información. (Integridad)	X		10	**3**	A pesar de que se realizan mantenimientos, los usuarios podrían guardar, borra las aplicaciones e información de los equipos informáticos.
	P4	Se realizan copias de seguridad (Backus) de la información crítica del laboratorio. (Integridad)		X	10	**3**	No, más bien en los mantenimientos una de las tareas consiste en la eliminación de archivos generades por las actividades docentes.
DISPONIBILIDAD	P5	Los equipos y servicios del laboratorio están disponibles cuando se los requiere para actividades académicas o administrativas. (Disponibilidad)	X		10	**10**	Si, conforme la planificación docente y curricular.
	P6	Existe un plan o procedimiento para responder ante incidentes de seguridad informática. (Disponibilidad)	X		10	**5**	Existe un plan de contingencias pero no está socializado a los diferentes usuarios.
	P7	Los equipos del centro de cómputo se encuentran actualizados o con vigencia tecnológica (Disponibilidad)		x	10	**3**	De las 140 computadoras 65 están en operación desde 10 a 17 años.
		PONDERACIÓN TOTAL			70		
		CALIFICACIÓN TOTAL			36		

Fuente: Ortiz, Marco – Responsable técnico – administrativo del centro de cómputo

A continuación, procedemos al cálculo de los niveles de confianza y de riesgo sobre el cumplimiento de los controles aplicados por el técnico responsable del centro de cómputo de la FADE; para ello, se utiliza la fórmula para al cálculo del nivel de confianza o cumplimiento:

Tabla 4. Cálculo del nivel de cumplimiento y riesgo de la seguridad informativa (CID).

NIVELES	FÓRMULA	EN DONDE:			RESPUESTA
CONFIANZA	$NC = \frac{CT}{PT} * 100$	CT PT NC	Calificación Total Ponderación Total Nivel de confianza	33 60 .?	$NC = \frac{36}{70} * 100$ $\boldsymbol{NC = 51\%}$
RIESGO	$NR = 100\% - NC$	NC NR	Nivel de confianza. Nivel de riesgo.	51% .?	$NC = \frac{36}{70} * 100$ $\boldsymbol{NR = 49\%}$

Realizado por: Los autores.

Si ubicamos los valores cuantitativos, en la matriz de riesgo y confianza que usualmente se utiliza en los proseos de auditoría, tenemos la valoración cualitativa:

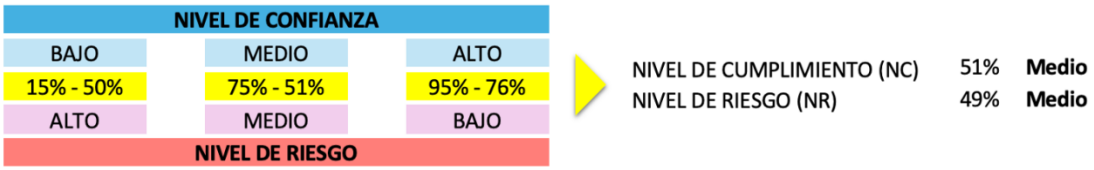

Figura 3. Determinación cualitativa del nivel de confianza y riesgo seguridad informativa (CID)

Realizado por: Los autores

Los aspectos más relevantes que se pueden mencionar sobre los resultados de la aplicación del cuestionario de control son:

- No existen políticas claras sobre el uso de cuentas, contraseñas y perfiles de usuario en los equipos (P2). El personal técnico califica este control con un 50%, indicando una debilidad crítica en la autenticación y el control de acceso lógico.
- Los sistemas de información, no evitan la manipulación y alteración no autorizada de la información (P3, Nivel de cumplimiento 30%). Los usuarios pueden guardar, eliminar aplicaciones e información. No se realizan copias de seguridad de la información crítica (P4, Nivel de cumplimiento 30%).
- Existiendo un plan de contingencias, este, no está socializado a los usuarios de la FADE (P6).

Es importante considerar la obsolescencia de equipos informático (computadoras) del centro del cómputo (P7), se desarrolla el indicador de obsolescencia:

Tabla 5. Cálculo del nivel de cumplimiento y riesgo de la seguridad informativa (CID).

INDICADOR	DESCRIPCIÓN	FÓRMULA	CÁLCULO	ANÁLISIS
Obsolescencia computadoras	Establecer e novel de equipos que están en estado de obsolescencia	# de computadoras obsoletas/Total de computadoras*100	$= \frac{65}{140} * 100$ $= 46\%$	Existe un % alto de equipos obsoletos, que afectan a la disponibilidad e integridad

Realizado por: Los autores

2. Análisis de la aplicación de la encuesta aplicada a docentes

Tabla 6. Evaluación Confidencialidad, integridad y disponibilidad – Docentes.

RESULTADO DE ENCUESTA APLICADA A DOCENTES

CID	N°	PREGUNTAS	SIEMPRE		A VECES		NUNCA	
			F	%	F	%	F	%
CONFIDENCIALIDAD	P1_Doc.	Considera que la información académica manejada en los laboratorios se mantiene protegida contra accesos no autorizados. (Confidencialidad)	6	33%	3	17%	9	50%
	P2_Doc.	El acceso a los equipos y sistemas del laboratorio es otorgado únicamente a usuarios autorizados. (Confidencialidad)	6	33%	9	50%	3	17%
INTEGRIDAD	P3_Doc.	La información y los trabajos académicos almacenados en los equipos no se alteran sin autorización. (Integridad)	9	50%	9	50%	0	0%
	P4_Doc.	Los sistemas del laboratorio funcionan de manera confiable durante las actividades docentes. (Integridad)	3	17%	15	83%	0	0%
DISPONIBILIDAD	P5_Doc.	Los laboratorios de cómputo están disponibles en los horarios planificados para la docencia. (Disponibilidad)	9	50%	9	50%	0	0%
	P6_Doc.	Cuando ocurre un problema técnico o de seguridad, este se soluciona oportunamente. (Disponibilidad)	0	0%	15	83%	3	17%

Fuente: Encuesta realizada a docentes

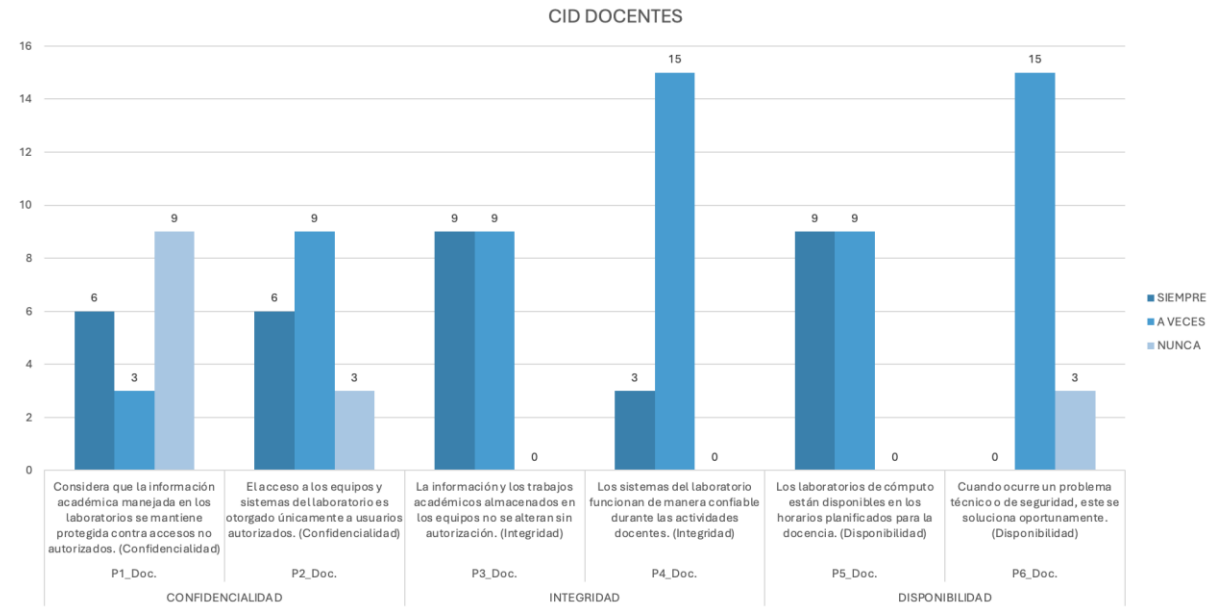

Figura 4. Evaluación Confidencialidad, integridad y disponibilidad - Docentes

Fuente: Encuesta realizada a docentes - FADE

El 50% de los docentes considera que la información académica nunca está protegida (P1_Doc). El 50% a veces o el 17% nunca considera que el acceso es solo para usuarios autorizados (P2_Doc). Por otro lado, el 83% de los docentes considera que los sistemas a veces o nunca cuentan con mecanismos que eviten la alteración no autorizada de la información (P4_Doc). Finalmente, el 83% de los docentes considera que el laboratorio a veces o nunca ofrece una solución oportuna ante problemas técnicos o de seguridad (P6_Doc).

3. Análisis de la aplicación de la encuesta aplicada a estudiantes

Tabla 7. Evaluación Confidencialidad, integridad y disponibilidad – Estudiantes.

RESULTADO DE ENCUESTA APLICADA A ESTUDIANTES

CID	N°	PREGUNTAS	SIEMPRE		A VECES		NUNCA	
			F	%	F	%	F	%
CONFIDENCIALIDAD	P1_Est.	Mis datos personales y trabajos académicos están protegidos cuando utilizo los equipos del laboratorio. (Confidencialidad)	194	64%	103	34%	7	2%
	P2_Est.	Se solicita algún tipo de identificación o credencial para utilizar los equipos del laboratorio. (Confidencialidad)	93	31%	63	21%	148	49%
INTEGRIDAD	P3_Est.	La información almacenada en los equipos se mantiene íntegra durante el uso del laboratorio. (Integridad)	194	64%	100	33%	10	3%
	P4_Est.	Los equipos del laboratorio funcionan correctamente y sin fallas frecuentes. (Integridad)	142	47%	158	52%	4	1%
DISPONIBILIDAD	P5_Est.	Puedo acceder a los equipos del laboratorio cuando los necesito para mis actividades académicas. (Disponibilidad)	141	46%	136	45%	27	9%
	P6_Est.	El laboratorio cuenta con soporte técnico disponible cuando se presentan problemas. (Disponibilidad)	193	63%	96	32%	15	5%

Fuente: Encuesta realizada a estudiantes

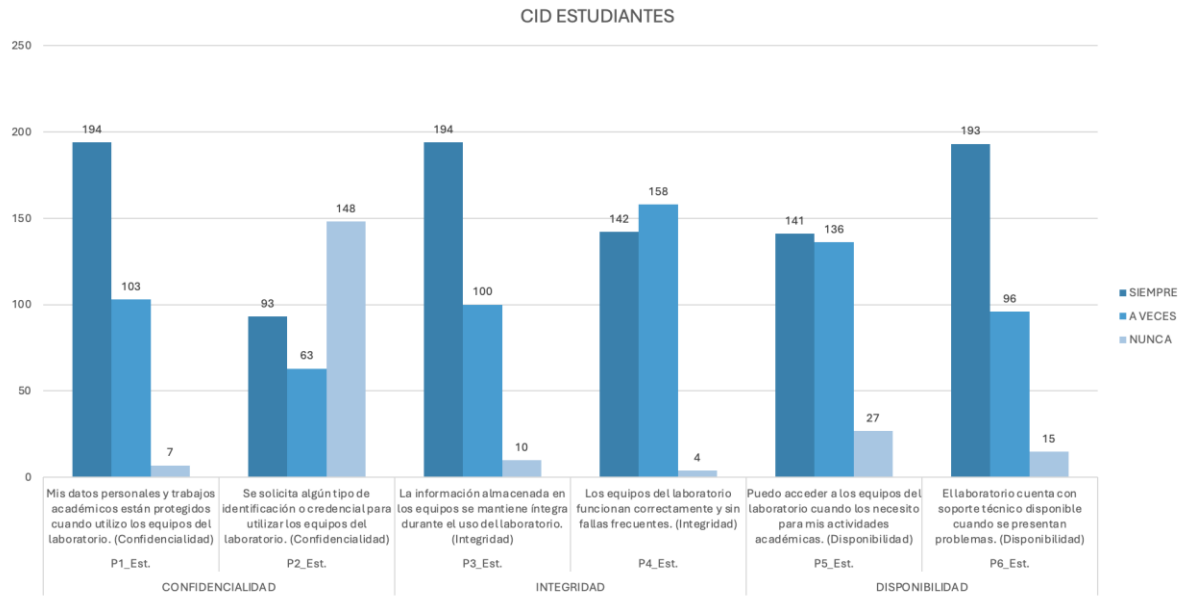

Figura 5. Evaluación Confidencialidad, integridad y disponibilidad - Estudiantes

Fuente: Encuesta realizada a estudiantes - FADE

El 49% nunca o el 2l% a veces tiene una forma de identificación o credencial para usar los equipos (P2_Est), lo que sugiere un control de acceso débil. Sin embargo, el 52% a veces o el l% nunca percibe que los equipos funcionan correctamente y sin fallas (P4_Est), lo que podría afectar la integridad de los datos por fallos de hardware o software. Finalmente, el 45% a veces o el 9%

nunca puede acceder a los equipos cuando los necesita (P5_Est), lo que indica problemas de disponibilidad de recursos.

4. Evaluación de BRECHAS DE SEGURIDAD (riesgos)

Se plantea el proceso en el que se identifican, cuantifican y priorizan los riesgos con base en criterios de tratamiento de estos. Los resultados de esta evaluación deben determinar la acción apropiada los responsables de la administración del centro de cómputo de la FADE, gestiones y establezcan controles apropiados.

Análisis de brechas de seguridad (riesgos)

El propósito del análisis de las brechas de seguridad tiene una relación directa con la identificación del riesgo, reconocer y describir estos riesgos que podrían impedir que el centro de cómputo de la FADE logre sus objetivos primarios y relacionados con las actividades de apoyo hacia docentes y estudiantes para el desarrollo de la función académica. Para la identificación de la brechas, es importante contar con información pertinente, apropiada y actualizada.

Se utiliza dos técnicas (cuestionarios de control y encuestas) para identificar las brechas que podrían afectar a uno o varios objetivos. De los análisis realizados a las personas involucradas en el uso (docentes y estudiantes) y administración del centro de cómputo (técnico responsable), se puede determinar los siguientes brechas o riesgos:

1. Ausencia de políticas de seguridad de la información.
2. Ausencia de autenticación en los equipos.
3. Inexistencia de respaldos de la información.
4. Dependencia de controles de los docentes para la seguridad física.
5. Interrupción de servicios en el centro de cómputo.
6. Inexistencia en buenas prácticas en Ciberseguridad.

5. Vulnerabilidades y amenazas

Tabla 8. Análisis de vulnerabilidades y amenazas.

RIESGOS (BRECHAS DE SEGURIDAD)	VULNERABILIDAD	AMENAZA	TIPO AMENAZA
1. Ausencia de políticas de seguridad de la información	Falta de un marco normativo y directrices claras para el manejo de la información y los sistemas. Desconocimiento por parte del personal y usuarios sobre sus responsabilidades de seguridad.	Errores de los usuarios del centro de cómputo, negligencia y/o mal uso de recursos). Acciones por parte de los usuarios generado por la ausencia de políticas de seguridad.	Humana
2. Ausencia de autenticación en los equipos	Acceso no autorizado a los sistemas y datos por cualquier persona con acceso físico o de red al equipo.	Robo, modificación, duplicación o eliminación de datos por usuarios que no están autorizados para ocupar el centro de cómputo. Instalación de aplicaciones o software malicioso en general.	Humana

	Falta de trazabilidad y rendición de cuentas de las acciones realizadas en los equipos.		
3. Inexistencia de respaldos de la información	Pérdida total e irrecuperable de datos críticos ante cualquier evento adverso. Alto tiempo de recuperación (RTO) o imposibilidad de reanudar las operaciones.	Fallo de hardware o software. Desastres naturales (incendio, inundación). Errores de las personas (borrado accidental). Ataques de ransomware o malware destructivo.	Humana
4. controles que dependen de los docentes para el acceso al centro de cómputo	Acceso no controlado en las horas fuera de la jornada académica.	Robo de equipos o partes y piezas de computadoras. Alteración de configuración de equipos. Daños de infraestructura (Edificios, sistema eléctrico, cableado de red, etc.)	Humana
5. Limitación o Interrupción de servicios académicos en el centro de cómputo	Sistemas eléctrico y de transmisión de datos expuestos a los usuarios del centro de cómputo	Fallo de suministro eléctrico. Fallo de componentes críticos de red o servidores. Mantenimiento no planificado.	Humana
6. Falta en buenas prácticas en Seguridad de la información (Ciberseguridad)	Uso inadecuado de equipos y aplicaciones. Falta de procedimientos para generación de claves de usuarios.	Pérdida o modificación de datos y de aplicaciones instaladas en los equipos. Infección virus o por malware. Ataques de ingeniería social (phishing).	Humana

Realizado por: Los autores

6. Análisis de los riesgos, criterios valoración de la probabilidad e impacto.

El criterio es una descripción que nos permite ser más específicos y consistentes en la asignación de cada clasificación según corresponda.

Tabla 9. Criterios de valoración para análisis de riesgos.

PROBABILIDAD	**CRITERIO**
BAJA	Es poco probable que ocurra. Podría ocurrir una vez en el año.
MEDIA	Es probable que ocurra. Podría ocurrir mensualmente.
ALTA	Es muy probable que ocurra. Podría ocurrir diariamente.
IMPACTO	**CRITERIO**
BAJA	Eventos que no afectan las actividades del centro de cómputo.
MEDIA	Eventos que podrían afectar las actividades del centro de cómputo y/o provocar pérdidas de información o recursos informáticos.
ALTA	Eventos que podrían afectar las actividades del centro de cómputo, provocar pérdidas y afectación a la planificación académica.

Fuente: Amarante (2022).

7. Determinación de la probabilidad y el impacto de cada uno de los riesgos

El propósito de la valoración del riesgo es apoyar la toma de decisiones en la empresa. Esta valoración implica comparar los resultados del análisis del riesgo con los criterios establecidos para determinar cuándo se requiere una acción para mitigarlos (10).

Tabla 10. Determinación de la probabilidad e impacto de los riesgos – centro de cómputo FADE.

N°	RIESGO	PROBABILIDAD	IMPACTO
1	Ausencia de políticas de seguridad de la información.	ALTA	ALTO
2	Ausencia de autenticación en los equipos.	ALTA	ALTO
3	Inexistencia de respaldos de la información.	MEDIA	MEDIO
4	Dependencia de controles de los docentes para la seguridad física.	MEDIA	MEDIO
5	Interrupción de servicios en el centro de cómputo.	ALTA	ALTO
6	Inexistencia en buenas prácticas en Ciberseguridad.	MEDIA	ALTO

Realizado por: Los autores

8. Nivel de riesgo resultante de la probabilidad y el impacto

Vamos a utilizar la siguiente matriz estándar (15):

Tabla 11. Matriz para la determinación del nivel de riesgo.

NIVEL DE RIESGO				
PROBABILIDAD	**ALTO**	MEDIO	ALTO	ALTO
	MEDIO	BAJO	MEDIO	ALTO
	BAJO	BAJO	BAJO	MEDIO
		BAJO	**MEDIO**	**ALTO**
		IMPACTO		

Fuente: Amarante (2022)

El nivel de riesgo será el resultado del cruce del valor de la probabilidad (filas de la matriz) y el impacto (columnas de la matriz) (15). Nuestra evaluación cualitativa quedaría de esta forma:

Tabla 12. Determinación de los niveles de riesgo – centro de cómputo FADE

N°	BRECHA DE SEGURIDAD (RIESGO)	PROBABILIDAD	IMPACTO	NIVEL RIESGO
1	Ausencia de políticas de seguridad de la información.	ALTA	ALTO	ALTO
2	Ausencia de autenticación en los equipos de cómputo. Accesos no autorizado.	ALTA	ALTO	ALTO
3	Inexistencia de respaldos de la información.	MEDIA	MEDIO	MEDIO
4	Dependencia de controles de los docentes para la seguridad física.	MEDIA	MEDIO	MEDIO
5	Interrupción de servicios en el centro de cómputo.	ALTA	ALTO	ALTO
6	Inexistencia en buenas prácticas en Ciberseguridad.	MEDIA	ALTO	MEDIO

Realizado por: Los autores

Una vez realizada la valoración cualitativa del nivel de probabilidad y el nivel de impacto podemos determinar que existen 3 brechas de seguridad (riesgos) que se presentan con Nivel Alto: Ausencia de políticas de seguridad de la información, Ausencia de autenticación en los equipos de cómputo. Accesos no autorizado, y , Interrupción de servicios en el centro de cómputo; lo que implica que son los aspectos que merecen mayor tención y que serán abordados más adelante. Así mismo, existen 3 brechas de seguridad que se presentan con valoración Medía: Inexistencia de respaldos de la información, Dependencia de controles de los docentes para la seguridad física, y, Inexistencia en buenas prácticas en Ciberseguridad. Los mismos que también requieren atención y se incluyen en el plan de mejora.

9. Evaluación de la cultura de seguridad

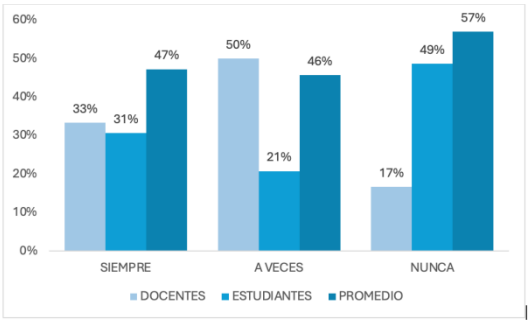

Figura 6. Política de seguridad

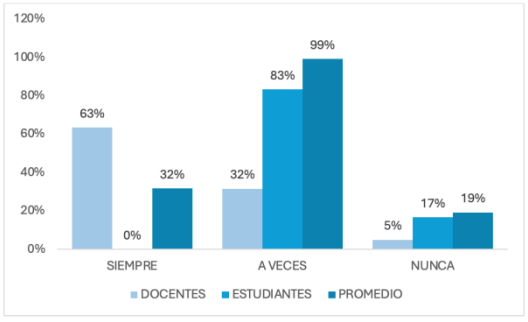

Figura 7. Normativa: Plan de contingencias

En la evaluación de la cultura de seguridad, se analizan dos criterios que consideramos relevantes: 1. La política de seguridad, y 2. Las normas de control relacionada la existencia e implementación del Plan de contingencias.

Se evalúa, si, el acceso a los equipos y sistemas del laboratorio es otorgado únicamente a usuarios autorizados, y, si, se solicita algún tipo de identificación o credencial para utilizar los equipos del laboratorio, determinar que los niveles brechas son moderados, el 57% en promedio responden que nunca se implementan políticas de seguridad relacionados con la confidencialidad, esto quiere decir que no existe una política de autenticación para el uso de los equipos informáticos en el centro de cómputo de la FADE.

En lo relacionado al cumplimiento de las normas de control interno, con respecto a la existencia de un plan de contingencias, a pesar de que el técnico del centro de cómputo manifiesta que si existe este instrumento, el 99% de encuestado manifiestan tener respuesta ante: la disponibilidad de soporte técnico disponible cuando se presentan problemas, y, a la solución oportuna de asistencia técnica o de seguridad cuando ocurre un problema, concluyendo que, no se conoce de los procedimientos determinados en el plan de contingencias, o que el personal responsable no tienen la capacidad técnica para actuar frente a eventualidades que afectan el normal desarrollo de la operatividad del centro de cómputo.

10. Plan de mejora

El plan de mejora constituye la herramienta necesaria para transformar la situación actual que atraviesa el centro de cómputo de la FADE. Para ello, se plantea una propuesta de actividades por cada componente relacionada con las dimensiones de la seguridad de la información (Confidencialidad, integridad y disponibilidad).

Tabla 13. Plan de mejora para el centro de cómputo de la FADE.

CID	OBJETIVO	ACTIVIDADES	INDICADOR	RESPONSABLE	TIEMPO
CONFIDENCIALIDAD	Implementar políticas de seguridad de la información.	Elaborar y socializar políticas de seguridad de la información.	Una política de seguridad de la información diseñada y aprobada	Decano FADE	Febrero 2026
		Implementar autenticación básica en los equipos.	# de equipos con sistema de autenticación/Total de equipos	Técnico del centro de cómputo	Febrero a marzo 2026
INTEGRIDAD	Mantener la integridad de la información a fin de salvaguardar los datos.	Implementar un sistema de copias de seguridad.	# de copias de seguridad realizadas/copias de seguridad panificadas	Técnico del centro de cómputo	1 vez por mes Año 2026
		Implementar un sistema de control de acceso físico.	# de laboratorios don sistemas de control de acceso.	Decano FADE Técnico del centro de cómputo	Febrero 2026
DISPONIBILIDAD	Evaluar y poner en conocimiento de los usuarios el	Socializar y probar el plan de contingencia.	Usuarios socializados/Total de usuarios	Técnico del centro de cómputo	Marzo a mayo 2026

	plan de contingencias.	Capacitar a docentes y estudiantes en buenas prácticas de ciberseguridad.	Docentes y estudiantes capacitados/Total de docentes y estudiantes	Técnico del centro de cómputo	Febrero 2016

Realizado por: Los autores

CONCLUSIONES

La implementación de políticas de ciberseguridad en las empresas es necesaria para velar por el uso adecuado de los recursos tecnológicos, y, garantizar se cumplan con eficiencia y eficacia las dimensiones de la seguridad de la información: confidencialidad, integridad y disponibilidad de la información.

A pesar de que se presenta una discrepancia en la percepción entre estudiantes y docentes, se evidencia la ausencia de una política de seguridad, afectando directamente la confidencialidad de la información; al mismo tiempo, la integridad de la información se encuentra vulnerada, básicamente por la falta de mecanismos de protección de datos, equipos y la ausencia de procesos de copias de seguridad; la falta de socialización del plan de contingencias y su aplicación, comprometen la disponibilidad, estudiantes y docentes perciben que la operatividad ante una crisis es cuestionable.

Se detectaron 3 brechas de seguridad (riesgos) que se presentan con Nivel Alto: Ausencia de políticas de seguridad de la información, inexistencia en prácticas de autenticación en los equipos de cómputo, e, interrupción de servicios en el centro de cómputo, aspectos que requieren una atención prioritaria, ya que inciden directamente sobre las dimensiones de la ciberseguridad, frente a ello, se establece un plan de mejora, que para abordar la problemática, establece acciones e indicadores para evaluar y minimizar los riesgos, contribuyendo a la toma de decisiones y cumplimento de los objetivos del centro de cómputo de la FADE.

AGRADECIMIENTOS

Al Centro de cómputo de la Facultad de Administración de Empresas - ESPOCH.

DECLARACIÓN DE INTERÉS

Los autores declaran no tener conflicto de intereses.

REFERENCIAS BIBLIOGRÁFICAS

1. Universidad Internacional de Valencia. Ciencia y Tecnología. Ciberseguridad en Ecuador. [Online].; 2025. Acceso 12 de 03 de 2025. Disponible en: https://www.universidadviu.com/ec/actualidad/nuestros-expertos/ciberseguridad-en-ecuador#la.

2. Towhidi G, Pridmore J. Journal of Information Systems Education. [Online]; 2023. Disponible en: https://aisel.aisnet.org/jise/vol34/iss1/6.
3. Orosco J. Ciberseguridad en educación superior: una revisión bibliométrica. Revista Digital de Investigación en Docencia Universitaria. [Online].; 2024. Acceso 21 de 03 de 2026. Disponible en: https://doi.org/10.19083/ridu.2024.1933.
4. Escuela Superior Politécnica (ESPOCH). Escuela Superior Politécnica. [Online]; 2025. Disponible en: https://www.espoch.edu.ec/mision-vision/.
5. Escuela Superior Politécnica de Chimborazo. ESPOCH. [Online]; 2025. Disponible en: https://www.espoch.edu.ec/2025-2/.
6. Palacios P. Universidad Autónoma de los Andes (UNIANDES). [Online].; 2023.. Disponible en: https://dspace.uniandes.edu.ec/bitstream/123456789/8158/1/PIUASIS011-2018.pdf.
7. Pérez M. Elibro. [Online].; 2025.. Disponible en: https://elibro-net.proxy.espoch.edu.ec/es/ereader/espoch/283847?page=10.
8. Mata A. Elibro. [Online]. Madrid; 2024.. Disponible en: https://elibro-net.proxy.espoch.edu.ec/es/ereader/espoch/273939?page=18.
9. IAPLIKADA. IAPLIKADA. Soluciones Seguridad Informática. [Online]; 2025. Disponible en: https://www.iaplikada.com/soluciones-seguridad-informatica/.
10. Holloway D. SGSI.online. [Online].; 2025.. Disponible en: https://es.isms.online/iso-27002/.
11. International Organization for Standardization. ISO 31000: Risk management — Guidelines. ISO.; 2018.
12. ISOTools Excelence. ISOTOOLS. [Online].; 2025.. Disponible en: https://d3g4v0cf6ioz32.cloudfront.net/uneg/BibliotecaGrupos/44822132_32dc_48e2_995b_c5c973f2dbac.pdf.
13. Secretaría Central de ISO. Universidad Juárez del Estado de Durango (UJED). [Online].; 2018.. Disponible en: https://forestales.ujed.mx/succi/recursos/documento_29.pdf.
14. RED CEDIA. Gestión de la Seguridad de la Información Bogotá: RENATA; 2018.
15. Mendoza M. ¿Evaluación de riesgos cualitativa o cuantitativa? [Online].; 2018. Acceso 16 de 03 de 2026. Disponible en: https://www.welivesecurity.com/la-es/2015/03/23/evaluacion-de-riesgos-cualitativa-o-cuantitativa/.
16. Amarante D. Auditoría de Sistemas de Información. Una guía práctica para aprender auditoría incluso si sólo cuentas con conocimientos básicos de informática. San Francisco California; 2022..
17. Sudha S, Javaid A, Niyaz Q, Yang X. ASEE Annual Conference and Exposition, Conference Proceedings, Baltimore. [Online]; 2023. Disponible en: https://acortar.link/M6lvzj.