TRABAJO DE GRADO
Opción Seminario.

Arquitectura Empresarial Aplicada a la Educación Superior

Corporación Universitaria Remington.
Nombre de la facultad: Ingenierías
Nombre del programa académico: Ingeniería de Sistemas

Nombres de los estudiantes autores del trabajo de grado.
Santiago Morales Florez
Carlos Andrés Oviedo Banquez

Jorge Leonardo Ramírez Restrepo - docente seminário.
Seminario

2026

Agradecimientos

Queremos expresar nuestro más sincero agradecimiento a la Corporación Universitaria Remington por brindarnos el espacio, los recursos y la excelencia académica necesarios para nuestra formación profesional integral y el desarrollo de este trabajo de grado.

De manera especial, extendemos nuestra profunda gratitud a nuestro docente del seminario, Jorge Leonardo Ramírez Restrepo, por su invaluable guía, su dedicación y por compartir su experiencia con nosotros. Sus orientaciones técnicas, retroalimentación constante y exigencia académica fueron fundamentales para estructurar, pulir y culminar con éxito este informe.

Tabla de Contenidos

Resumen

Se presentan los resultados de una evaluación diagnóstica de ciberseguridad y seguridad de la información realizada en la Universidad Innovar del Pacífico, una institución privada de educación superior la cual lleva más de veinte años de trayectoria y ha prestado sus servicios a una comunidad establecida por aproximadamente 8.500 estudiantes y 420 colaboradores. La organización ha desarrollado sus actividades mediante una infraestructura tecnológica integrada por 18 servidores virtualizados, una plataforma de gestión del aprendizaje (LMS), un sistema ERP administrativo, redes institucionales y diversos servicios digitales que dan soporte a sus procesos académicos y administrativos. Este análisis ha permitido identificar que el crecimiento de esta infraestructura ha carecido de políticas de seguridad explícitas y de controles técnicos y administrativos idóneos para la protección de la información y los datos.

El propósito de este informe consistió en la evaluación de las vulnerabilidades tecnológicas, operativas y humanas de la institución para fundamentar el diseño y desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI). Para ello, se evaluaron aspectos relacionados con el contexto organizacional, la problemática de seguridad, el gobierno de TI, la gestión de riesgos, el inventario y clasificación de activos de información, así como los controles existentes para la protección de la confidencialidad, integridad y disponibilidad de los datos institucionales.

Como resultado del diagnóstico, se evidenciaron deficiencias vistas en la gestión de accesos, la ausencia de procedimientos documentados para el tratamiento de incidentes, debilidades en la administración de usuarios y respaldos y una limitada cultura de seguridad frente a amenazas como la ingeniería social. Asimismo, se identificaron sistemas académicos y financieros los cuales se han detectado como activos críticos para la continuidad de las operaciones. Con base en lo anterior, se formularon recomendaciones orientadas al fortalecimiento del gobierno de seguridad, la implementación de políticas institucionales, la adopción de controles técnicos y administrativos, la capacitación permanente de los usuarios y el establecimiento de estrategias que contribuyan a mejorar la resiliencia digital y a la protección de la información institucional.

Palabras clave

Sistema de Gestión de Seguridad de la Información (SGSI), Gestión de riesgos, Vulnerabilidades tecnológicas, Cultura organizacional, Continuidad del negocio.

Marco conceptual y normativo

Conceptos fundamentales de ciberseguridad

La protección de la Universidad Innovar del Pacífico requiere articular la seguridad de la información y la ciberseguridad. La primera busca resguardar integralmente todos los recursos y datos de la organización (Voutssas, 2010, p. 131), mientras que la segunda se enfoca en la defensa específica de la infraestructura crítica frente a ataques digitales (Rodríguez Zambrano & Moreno Tamayo, 2024, p. 169). Esta base teórica es indispensable para asegurar los activos misionales de la institución, tales como el sistema LMS y el software ERP administrativo.

La operatividad técnica de estos recursos se fundamenta en los principios de la tríada CID: confidencialidad, integridad y disponibilidad (Mejía Medina, 2019, pp. 35-38). En el contexto de la institución analizada, aplicar estos principios implica garantizar que únicamente el personal autorizado acceda a los datos sensibles, prevenir alteraciones malintencionadas en los historiales académicos y evitar las constantes caídas del sistema de recaudo durante las temporadas críticas de matrículas.

Para mantener esta tríada inquebrantable, la universidad debe evaluar constantemente las amenazas y vulnerabilidades que propician los riesgos tecnológicos (Quiroz Zambrano & Macías Valencia, 2017, p. 684). La mitigación de estos riesgos, originados por debilidades operativas como la falta de control de accesos o la susceptibilidad a la ingeniería social, hace imperativa la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) y de controles rigurosos que aseguren la resiliencia institucional a largo plazo (Muñoz Campuzano, 2021, p. 12).

Marco normativo

Tabla 1. Normatividad aplicable.

Norma o estándar	***Propósito***	***Aplicabilidad en la organización***

ISO/IEC 27001	Definir los requisitos para la planificación, implementación, operación, monitoreo y mejora de un Sistema de Gestión de Seguridad de la Información (SGSI).	Proporciona la hoja de ruta estratégica para estructurar el gobierno de TI de la universidad garantizando el ciclo de mejora continua.
ISO/IEC 27002	Proporcionar directrices y recomendaciones internacionalmente aceptadas para realizar la gestión de la seguridad de la información mediante controles.	Permite implementar controles técnicos y administrativos específicos para proteger plataformas críticas como el LMS y el ERP.
ISO/IEC 17799	Ofrecer un punto de referencia para construir la seguridad de la información equilibrando los requisitos comerciales con la confidencialidad, integridad y disponibilidad	Brinda directrices sólidas previas para prevenir, detectar y contener las brechas de seguridad en las plataformas de la institución.
Ley 1273 de 2009	Tipificar delitos informáticos y obligar a preservar integralmente la información, los datos y los sistemas que utilizan tecnologías de la información.	Obliga legalmente a la universidad a blindar la confidencialidad de las bases de datos de sus 8.500 estudiantes y 420 colaboradores.
Ley 1341 de 2009	Determinar el marco general para la formulación de políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones (TIC).	Regula la responsabilidad de la administración respecto a la gestión, planeación y control eficiente de la infraestructura de redes institucionales.

La implementación de este marco normativo representa un pilar estratégico ineludible para la viabilidad operativa y la protección de los procesos misionales de la Universidad Innovar del Pacífico. A nivel internacional, la adopción de estándares como la ISO/IEC 27001 y su predecesora, la ISO/IEC 17799, proporciona una metodología comprobada para el análisis y evaluación de riesgos bajo el ciclo de mejora continua (PHVA), permitiendo así estructurar un Sistema de Gestión de Seguridad de la Información (SGSI) robusto (Solarte Solarte et al., 2015, p. 496).

Para materializar este sistema de manera efectiva, el diseño de políticas y de procedimientos basado en la ISO 27001 garantiza la estandarización y optimización directa de los servicios del área de Tecnologías de la Información de la Institución (Chavez Muñoz, 2026, p. 14). Como complemento operativo, la norma ISO/IEC 27002 facilita la aplicación práctica de estas directrices mediante la implementación de controles técnicos y administrativos específicos, los cuales optimizan la gestión de riesgos en plataformas críticas como el LMS y el ERP (Ferrari Fernández & Hilario Rivas, 2025, p. 2371).

En el ámbito del cumplimiento legal colombiano, la institución debe estar sujeta a normativas de carácter obligatorio que complementen estos estándares técnicos internacionales. La Ley 1273 de 2009 tipifica los delitos informáticos y crea un nuevo bien jurídico tutelado para la protección de la información y los datos, exigiendo legalmente a la universidad blindar sus bases de datos ante los constantes retos y amenazas de la criminalidad digital (Guerrero Pérez et al., 2026, p. 5). Simultáneamente, la Ley 1341 de 2009 establece el marco general del sector TIC, obligando a la administración a realizar una gestión eficiente y continua de su infraestructura de redes y reconociendo la conectividad como un medio indispensable para garantizar derechos fundamentales como la educación de su comunidad (Bocanegra Monroy et al., 2025, p. 150).

Marco contextual

Descripción de la organización

La Universidad Innovar del Pacífico es una institución de educación superior cuya principal actividad económica y misional se centra en la prestación de servicios académicos de pregrado, posgrado, investigación y extensión universitaria. En su contexto de operación, la entidad funciona como un eje fundamental para el desarrollo social, científico y tecnológico de su región, albergando una comunidad conformada por aproximadamente 8.500 estudiantes y 420 colaboradores, entre personal docente, administrativo y directivo.

A nivel estructural, la organización opera bajo un modelo jerárquico y departamentalizado, el cual está encabezado por la Rectoría, de la cual se desprenden tres áreas vitales: la Vicerrectoría Académica, encargada de coordinar las facultades, programas de estudio y el currículo; la Vicerrectoría Administrativa y Financiera, responsable de la optimización y manejo de los recursos físicos y monetarios; y la Dirección de Tecnologías de la Información (TI), la cual actúa como un departamento transversal encargado de garantizar la operatividad digital, el soporte técnico y el mantenimiento de la infraestructura de toda la institución.

Los procesos principales de la universidad son altamente dependientes de la tecnología e incluyen la gestión de admisiones y matrículas, la administración académica (control de calificaciones y asistencia), el recaudo financiero, el pago de nómina y el soporte a proyectos de investigación. Para respaldar este volumen transaccional, la institución posee un robusto inventario de recursos tecnológicos; su infraestructura centralizada está compuesta por 18 servidores virtualizados que alojan plataformas de misión crítica, destacando el Sistema de Gestión del Aprendizaje (LMS) para la educación virtual y presencial, el software de planificación de recursos empresariales (ERP) para las finanzas y las bases de datos de investigación. Asimismo, cuenta con una red física que da soporte a 440 equipos de cómputo distribuidos en laboratorios, áreas de trabajo y bibliotecas, los cuales se encuentran interconectados a través de la red inalámbrica institucional.

Problemática identificada

A pesar de que la institución cuenta con una infraestructura tecnológica robusta para operar diariamente, la Universidad Innovar del Pacífico enfrenta una problemática crítica caracterizada por la falta de un Sistema de Gestión de Seguridad de la Información (SGSI), sumado a una baja cultura de prevención en su personal. Esta carencia ha derivado en vulnerabilidades técnicas y procedimentales que exponen gravemente sus activos más valiosos.

En primer lugar, se han detectado deficiencias severas en el control de accesos lógicos. La institución carece de procedimientos documentados de desvinculación de personal, lo que ha permitido en primera instancia que exfuncionarios conserven sus credenciales activas, pudiendo acceder a plataformas sensibles desde el exterior. A esto se le suma la

proliferación del uso de dispositivos sin ningún tipo de monitoreo por parte de TI y el uso compartido de cuentas entre varios funcionarios administrativos, lo que anula por completo la trazabilidad y dificulta identificar quién realiza cambios en los historiales clínicos o académicos.

En segundo lugar, se presentan incidentes recurrentes en lo que respecta a la disponibilidad y confidencialidad del servicio. Durante las temporadas de matrículas, el sistema académico sufre caídas constantes por saturación, interrumpiendo las operaciones en su etapa de mayor criticidad comercial. Sumado a esto, a pesar de almacenar un volumen masivo de información financiera, académica y personal de sus estudiantes, la comunidad desconoce el tratamiento que se le da a esta información y la universidad no cuenta con canales o procedimientos que permitan solicitar la corrección, actualización o supresión de datos.

La situación observada justifica plenamente el desarrollo del presente informe técnico, dado el nivel extremo de exposición al riesgo operativo, legal y reputacional. Si estas vulnerabilidades continúan sin mitigarse, una amenaza —como un ataque de secuestro de datos, acceso fraudulento de exempleados o una caída prolongada del sistema— paralizaría por completo la misión educativa de la institución. Añadido a esto, la pérdida de confidencialidad de la información acarrearía severas sanciones económicas y penales para la organización por el incumplimiento de normativas vigentes, como la Ley 1273 de 2009 y la Ley 1581 de 2012. Por lo tanto, resulta imperativo diagnosticar la situación actual y diseñar controles estructurados que garanticen la resiliencia tecnológica de la institución.

Identificación y análisis de activos

Inventario de activos

Para garantizar la seguridad de la información, es indispensable la identificación de los recursos que sustentan la operatividad de la organización. Un activo de información no es solo el hardware; abarca cualquier elemento que, de ser comprometido, afectaría la continuidad, la reputación o la legalidad de la institución. A continuación, se presenta el inventario de activos críticos.

Tabla 2. Inventario de activos

Activo	***Tipo***	***Descripción***	***Criticidad***

Sistema académico y Sistema ERP	Activo lógico (Software)	Plataformas que procesan la matrícula, calificaciones, pagos y presupuestos de la institución.	Alta
Plataforma LMS	Activo lógico (Software)	Sistema de educación virtual que aloja aulas, contenidos y evaluaciones académicas.	Alta
Servidores virtualizados (18 equipos)	Activo físico (Hardware)	Infraestructura de hardware que centraliza y procesa todas las plataformas lógicas de la universidad.	Alta
Bases de datos de investigación	Activo de información	Repositorio que resguarda las publicaciones, proyectos y propiedad intelectual.	Alta
Personal de Tecnología (TI)	Activo humano	Director, administradores y desarrolladores con privilegios de configuración global.	Alta

Plataforma de copias de seguridad	Activo de información	Sistemas y servicios en la nube dedicados al respaldo de la información institucional.	Media
Computadores institucionales (440)	Activo físico (Hardware)	Equipos portátiles y de escritorio asignados al personal docente, administrativo e investigadores.	Media
Redes Wifi (Institucional y visitantes)	Activo físico (Hardware)	Infraestructura que provee conectividad a los sistemas a través de las instalaciones y laboratorios.	Media
Docentes, administrativos y estudiantes	Activo humano	Comunidad universitaria encargada de generar y operar la información diaria.	Media
Plataforma de gestión documental	Activo lógico (Software)	Repositorio auxiliar para el manejo de expedientes académicos, actas y certificados.	Baja

La identificación, clasificación y valoración de estos activos se fundamentan en el análisis detallado sobre su impacto directo en los procesos misionales de la universidad: gestión académica, educación virtual, investigación, gestión financiera, manejo documental y talento humano. Esta evaluación se realiza estrictamente bajo los criterios de la tríada de seguridad de la información: impacto sobre la confidencialidad, la integridad y la disponibilidad (CID).

Los activos clasificados con criticidad “Alta” (sistema académico institucional, plataforma LMS y sistema ERP) reciben este nivel porque superan cualquier umbral de tolerancia a fallos; es decir, su indisponibilidad genera un impacto crítico e inmediato en la viabilidad financiera y operativa de la institución. Se consideran el núcleo estratégico e irremplazable de la institución. Su vulneración detendría procesos ineludibles que van desde las matrículas y el dictado de clases virtuales, hasta los pagos de nómina.

El compromiso de estos activos afectaría severamente la confidencialidad (fuga de datos personales y financieros) y la integridad (alteración malintencionada de calificaciones, asistencias o nóminas). El caso de estudio documenta cómo, durante un periodo crítico de matrículas, la alta concurrencia provocó la caída del sistema académico, afectando de frente la disponibilidad y la operatividad de la universidad. Asimismo, las bases de datos de investigación requieren la máxima protección para resguardar la confidencialidad de la propiedad intelectual institucional.

En cuanto a los físicos, los 18 servidores virtualizados y el personal de tecnología reciben esta máxima criticidad debido a que su compromiso representa un punto único de fallo. Un ataque a la cimentación de hardware colapsaría la disponibilidad del ecosistema digital por completo. Además, el personal posee privilegios globales; un error humano previo ya ocasionó la eliminación accidental de documentos vitales, afectando la integridad de los datos.

Los activos de criticidad “Media” (plataformas de copias de seguridad en la nube) son catalogados en este nivel porque, si bien su interrupción a corto plazo no paraliza a toda la universidad, actúan como el principal vector de vulnerabilidad para el escalamiento de incidentes hacia los sistemas críticos. Son esenciales para la recuperación ante desastres; sin embargo, presentan un riesgo elevado al no contar con evidencias recientes de pruebas de restauración que garanticen su integridad.

Dentro de la categoría física, los 440 computadores y las redes Wifi se justifican en este nivel al ser la superficie de ataque más extensa y expuesta de la red. Proveen el acceso diario al personal y estudiantes. Aunque la falla de un solo equipo no paralizaría a la universidad, su falta de estandarización en actualizaciones los convierte en puerta de entrada para ciber amenazas. Esta debilidad se evidenció con el robo de un equipo portátil que contenía información sensible fuera de las instalaciones, vulnerando la confidencialidad.

De igual modo, el cuerpo docente, administrativo y estudiantil representa un activo humano de criticidad media al ser el eslabón de seguridad más impredecible. Al carecer de campañas de sensibilización, han desarrollado comportamientos de riesgo considerables. Estas malas prácticas los hacen altamente propensos a ataques de ingeniería social, como se demostró con un correo fraudulento que simulaba provenir de la rectoría.

Finalmente, los activos de criticidad “Baja” (plataforma de gestión documental) reciben esta calificación dado que el impacto sobre la tríada CID es mitigable a través de planes de contingencia inmediatos. Cumplen funciones de consulta administrativa. Su interrupción impacta levemente la disponibilidad y puede suplirse temporalmente mediante canales de contingencia o procesos manuales. No obstante, el SGSI debe asegurar estas herramientas para así evitar que los atacantes las utilicen como vectores de escalamiento de privilegios hacia sistemas más críticos.

Análisis de amenazas y vulnerabilidades

Tabla 3. Amenazas y vulnerabilidades

Activo	***Amenaza***	***Vulnerabilidad***
Sistema académico, Sistema ERP y Plataforma LMS	Accesos no autorizados, robo de información y suplantación de identidad.	Existencia de cuentas activas de exfuncionarios, mala configuración de permisos y estudiantes que comparten credenciales.
Sistema académico y Servidores virtualizados (18 equipos)	Indisponibilidad del servicio, interrupción operativa y colapso del sistema.	Incapacidad de procesamiento ante alta demanda de acceso simultáneo durante períodos críticos como las matrículas.
Docentes, administrativos, estudiantes y Personal de TI	Fuga de credenciales e infecciones masivas por ataques de ingeniería social o phishing.	Ausencia de campañas de sensibilización, resistencia a usar autenticación adicional y exceso de confianza en correos electrónicos.
Computadores institucionales (440) y Bases de datos de investigación	Robo, pérdida de dispositivos y extracción de propiedad intelectual.	Equipos sin las últimas actualizaciones de seguridad, falta de políticas de clasificación de datos y almacenamiento en dispositivos personales.
Plataforma de copias de seguridad	Pérdida definitiva o irrecuperable de información crítica (ransomware o borrado).	Ausencia de evidencias recientes y pruebas documentadas de restauración de los *backups*.

Al evaluar el panorama de seguridad de la Universidad Innovar del Pacífico, se evidencia que las situaciones de mayor riesgo provienen de vulnerabilidades operativas y de una marcada deficiencia en la cultura organizacional. Estas debilidades estructurales demuestran que la institución ha sufrido incidentes que podrían paralizar su misión educativa de manera inminente.

El riesgo más crítico radica en la gestión de identidades y el control de accesos lógicos. La persistencia de cuentas activas pertenecientes a exfuncionarios y la práctica estudiantil de compartir credenciales amenazan de frente al Sistema académico, el Sistema ERP y la Plataforma LMS. Esta vulnerabilidad ya se materializó cuando un estudiante logró acceder a información académica ajena a su programa debido a una mala configuración de permisos, vulnerando directamente la confidencialidad.

Esta deficiencia en el control de accesos se evidencia profundamente en los Docentes, administrativos, estudiantes y Personal de TI por la falta de campañas de sensibilización y capacitación. La comunidad universitaria ha desarrollado comportamientos de alto riesgo, priorizando la comodidad sobre la protección y asumiendo que la seguridad es responsabilidad exclusiva del área de tecnología. El evento documentado sobre la recepción de correos fraudulentos que simulaban provenir de la rectoría demuestra que los usuarios son el vector de ataque más vulnerable.

Otro escenario de altísimo riesgo para la continuidad institucional es la indisponibilidad de los servicios críticos por la falta de capacidad tecnológica. El colapso del sistema académico durante la temporada de matrículas revela una vulnerabilidad grave en la arquitectura de red y en los Servidores virtualizados (18 equipos). Esta incapacidad para soportar picos de demanda no solo paraliza los recaudos, sino que expone a la universidad a ataques de denegación de servicio (DDoS), los cuales podrían mantener en un estado de inactividad a la institución por días.

A nivel físico, la gestión deficiente de los Computadores institucionales (440) y las Bases de datos de investigación representa una amenaza constante y silenciosa. El robo del computador de un investigador evidencia la irresponsabilidad de almacenar propiedad intelectual en dispositivos locales sin protocolos de cifrado. Simultáneamente, la conexión frecuente de dispositivos personales a la red institucional sin controles previos facilita la introducción inadvertida de malware al ecosistema tecnológico.

Además, la ausencia de una política formal para la clasificación de la información agudiza el impacto de estas vulnerabilidades. Al no existir lineamientos unificados, diversas áreas manejan datos sensibles bajo criterios propios, fomentando el uso de cuentas y memorias externas personales por parte de los docentes. Esta fragmentación impide aplicar controles de seguridad proporcionales a la criticidad de la información.

Finalmente, la falta de pruebas de restauración en la Plataforma de copias de seguridad eleva exponencialmente el riesgo ante incidentes destructivos. Aunque la universidad

realice respaldos regulares, la falta de simulacros o pruebas genera una falsa sensación de protección. Ante un borrado accidental masivo, como el ya documentado en una plataforma colaborativa, la incapacidad de restaurar los datos operativos condenaría a la universidad a pérdidas irreparables.

Análisis y gestión de riesgos

Metodología de análisis

Para desarrollar la matriz de riesgos de la Universidad Innovar del Pacífico, se estructuró un modelo de evaluación fundamentado en los estándares internacionales para la gestión de la seguridad, específicamente las metodologías dictadas por las normas ISO 31000 e ISO/IEC 27005. La aplicación de estos marcos normativos resulta imperativa en el entorno de educación superior. Las instituciones universitarias modernas enfrentan un ecosistema digital complejo, por lo cual están llamadas a jugar un papel protagónico en la creación de un ciberespacio seguro, estableciendo en sí una cultura de ciberseguridad que proteja su infraestructura tecnológica frente a las constantes amenazas (Anchundia-Betancourt, 2017, p. 209).

El proceso para la gestión y estimación de estas amenazas exige determinar el nivel de criticidad de cada escenario adverso. Para lograrlo, el modelo metodológico establece que el nivel de riesgo debe calcularse evaluando dos variables fundamentales: la probabilidad de ocurrencia del evento malicioso y el impacto potencial que este generaría sobre los activos. Desde una perspectiva matemática y de gestión, el nivel de riesgo informático se define conceptualmente como el producto resultante entre la probabilidad de que una vulnerabilidad sea explotada y el impacto que causa dicho riesgo al materializarse (Arévalo et al., 2017, p. 33).

Para estructurar esta matriz de evaluación, la primera variable analizada fue el “impacto”. Este factor cualitativo mide la magnitud del daño operativo, financiero, legal o reputacional que sufrirá la institución si un actor malintencionado logra su objetivo. En el entorno de esta institución, el impacto se evaluó determinando la degradación que sufrirían los tres principios fundamentales de la información: la confidencialidad, la integridad y la disponibilidad de las plataformas críticas (Espinel Suancha, 2025, p. 65). Con base en esto, se definieron cuatro niveles de impacto: Bajo, Medio, Alto y Crítico.

La segunda variable analizada fue la “probabilidad”, la cual representa la frecuencia estimada o la viabilidad técnica de que una vulnerabilidad existente sea explotada por un atacante interno o externo. Esta probabilidad se determinó analizando los antecedentes, el entorno de control y las estadísticas de incidentes previos, estableciéndose tres niveles cualitativos: Baja (escenarios sin precedentes), Media (eventos factibles acordes con las vulnerabilidades) y Alta (amenazas inminentes con casos ya materializados). Al cruzar el impacto y la probabilidad dentro de la matriz, se obtiene el nivel de riesgo global.

Matriz de riesgos

Tabla 4. Matriz de riesgos

Riesgo	*Impacto*	*Probabilidad*	*Nivel*
Acceso no autorizado a sistemas mediante el uso de credenciales activas de exfuncionarios.	Alto	Alta	Extremo
Indisponibilidad del sistema académico institucional debido al colapso por saturación de tráfico.	Alto	Alta	Extremo
Pérdida definitiva de información crítica por incapacidad de restaurar las copias de seguridad.	Crítico	Baja	Alto
Infección de la infraestructura tecnológica y secuestro de datos a través de ataques de phishing.	Alto	Media	Alto
Pérdida de propiedad intelectual e investigaciones en desarrollo por el robo de dispositivos físicos.	Medio	Media	Medio

Una vez consolidada la valoración en la matriz de riesgos, el análisis profundo revela que la Universidad Innovar del Pacífico enfrenta debilidades operativas sistemáticas que requieren atención inmediata. La evaluación permitió identificar cinco escenarios críticos: dos se clasifican en un nivel de riesgo “Extremo”, dos en un nivel “Alto” y uno en un nivel “Medio”. Esta categorización es vital para que la alta dirección enfoque sus

inversiones tecnológicas en proteger los procesos misionales que sostienen a sus estudiantes y colaboradores.

El primer riesgo “Extremo” corresponde al acceso no autorizado mediante credenciales activas de exfuncionarios, agravado por la práctica de los estudiantes de compartir contraseñas. La probabilidad de ocurrencia se definió como “Alta”, puesto que la auditoría diagnóstica comprobó la existencia de cuentas activas de personal desvinculado, evidenciando una falla en los procedimientos. Su impacto se catalogó como “Alto”, ya que un atacante con estas credenciales legítimas puede evadir controles perimetrales para alterar historiales académicos en el ERP o extraer bases de datos de forma encubierta.

El segundo riesgo de prioridad “Extrema” se refiere a la indisponibilidad y el colapso del sistema académico central debido a la saturación de tráfico durante las temporadas de matrículas. La probabilidad de materialización es sumamente “Alta”, dado que ya existe un evento documentado en el que el sistema sufrió caídas y quedó inoperativo por la alta demanda. El impacto de esta amenaza es indiscutiblemente “Alto”, porque el colapso de esta plataforma detiene por completo el proceso de recaudo financiero y paraliza el registro de asignaturas institucionales.

El riesgo más alarmante de nivel “Alto” es la posible pérdida definitiva de información por la incapacidad de restaurar las copias de seguridad. Aunque la probabilidad de que ocurra un evento destructivo masivo (como un secuestro de datos con ransomware) se considera estadísticamente “Baja”, el impacto de este escenario es “Crítico”. El diagnóstico evidenció que, si bien la universidad cuenta con la automatización de respaldos en la nube, no existen evidencias de pruebas de restauración. Si un incidente llegara a ocurrir y los respaldos fallan, la pérdida sería irreversible.

El siguiente riesgo clasificado como de nivel “Alto” es la infección de la infraestructura tecnológica mediante tácticas de ingeniería social, centrándose en correos de phishing. Su probabilidad se establece como “Media”, sustentada en el hecho documentado de un correo fraudulento que circuló simulando provenir de la rectoría, lo cual demuestra una alta tendencia al incremento impulsada por la confianza excesiva del personal. Su impacto es valorado como “Alto”, ya que un solo colaborador engañado puede entregar sus credenciales administrativas, otorgando al ciberdelincuente la vía libre para encriptar los 18 servidores virtualizados de la organización.

Por otra parte, el riesgo asociado a la pérdida de propiedad intelectual por el robo de dispositivos físicos fue clasificado en un nivel “Medio”. El robo comprobado de un portátil a un docente investigador demuestra que la probabilidad es “Media”. Aunque su impacto no detiene las operaciones masivas de la universidad, la pérdida de investigaciones académicas sin cifrado representa una brecha significativa que el área de tecnología debe mitigar a mediano plazo para así consolidar la protección en todos sus frentes.

Políticas y controles de seguridad

Políticas propuestas

Tabla 5. Políticas de seguridad

Política	***Objetivo***	***Riesgo asociado***

Política de Control de Accesos y Gestión de Identidades	Garantizar que únicamente los usuarios legítimos puedan acceder a los sistemas, estableciendo normas para la asignación y revocación inmediata de permisos.	Acceso no autorizado mediante el uso de credenciales activas de exfuncionarios y contraseñas compartidas.
Política de Clasificación y Tratamiento de la Información	Categorizar los datos institucionales según su nivel de sensibilidad para exigir medidas de protección técnica proporcionales a su importancia estratégica.	Pérdida de propiedad intelectual e investigaciones en desarrollo por el robo de dispositivos físicos sin protección.
Política de Concientización y Cultura de Ciberseguridad	Educar y comprometer a toda la comunidad universitaria sobre las amenazas digitales actuales y el uso seguro de los recursos tecnológicos de la entidad.	Infección de la infraestructura tecnológica y secuestro de datos a través de ataques de ingeniería social o *phishing*.
Política de Gestión de Incidentes y Continuidad del Negocio	Establecer protocolos obligatorios de respuesta ante fallas sistémicas, garantizando la resiliencia de las plataformas críticas y la preservación de los registros.	Indisponibilidad del sistema académico institucional e incapacidad de restaurar las copias de seguridad.

Política de Uso Aceptable de Dispositivos (BYOD) y Actualizaciones	Regular estrictamente la conexión de equipos personales a la red institucional y obligar al parchado continuo del software de los computadores.	Fuga de información o introducción de *malware* a través de terminales de trabajo o memorias USB desactualizadas.

Controles propuestos

Tabla 6. Controles de seguridad

Riesgo	***Control***	***Justificación***

Acceso no autorizado mediante credenciales de exfuncionarios o contraseñas compartidas.	Implementación de Autenticación Multifactor (MFA) obligatoria y automatización del procedimiento de desvinculación o offboarding.	Bloquea el acceso a sistemas críticos, ya que un atacante o estudiante requerirá un dispositivo adicional validado, incluso si posee la contraseña legítima.
Indisponibilidad del sistema académico debido a la saturación de tráfico.	Implementación de balanceadores de carga en la red y despliegue de escalabilidad automática en los servidores virtualizados.	Distribuye inteligentemente el tráfico masivo de usuarios durante las jornadas de matrícula, evitando el colapso de la plataforma y garantizando el servicio.
Pérdida definitiva de información por incapacidad de restaurar copias de seguridad.	Ejecución de simulacros trimestrales y auditorías documentadas de restauración de los backups en entornos de prueba aislados.	Transforma el almacenamiento pasivo en una medida de aseguramiento activa, comprobando rutinariamente que los expedientes académicos pueden reconstruirse ante incidentes.
Infección de infraestructura por ataques de phishing.	Despliegue de campañas semestrales de simulación de engaños y capacitación en ciberseguridad para docentes y administrativos.	Modifica el comportamiento de riesgo de los usuarios, convirtiéndolos en una barrera preventiva capaz de reconocer y reportar correos electrónicos fraudulentos.
Pérdida de investigaciones por el robo de dispositivos físicos.	Implementación técnica de cifrado de disco duro (ej. BitLocker) en la totalidad de los 120 equipos portátiles institucionales asignados.	Asegura que la propiedad intelectual e información confidencial permanezca completamente ilegible para terceros en caso de hurto o extravío del hardware

La articulación entre las políticas normativas y los controles de seguridad propuestos constituye la estrategia fundamental para disminuir las vulnerabilidades operativas de la Universidad Innovar del Pacífico. Las políticas actúan como el cimiento de gobernanza que orienta el comportamiento diario de los usuarios, mientras que los controles técnicos materializan estas directrices en barreras preventivas, detectivas y correctivas, logrando una sinergia vital para blindar los procesos misionales y garantizar el derecho a la educación de la comunidad.

Para abordar el riesgo crítico de los accesos no autorizados, la Política de Control de Accesos elimina la ambigüedad en la administración de las credenciales institucionales. Al respaldarse operativamente con la implementación de la Autenticación Multifactor (MFA) y los protocolos formales de desvinculación, se cierra la brecha que permitía a los exfuncionarios ingresar a la red. Este control asegura que, aunque una contraseña sea compartida entre estudiantes o robada, el atacante fracasará al no contar con el segundo factor de validación.

En cuanto al riesgo extremo de indisponibilidad del sistema académico, la Política de Continuidad del Negocio proporciona el mandato formal para priorizar la resiliencia tecnológica institucional. Su control técnico asociado, enfocado en la utilización de balanceadores de carga y escalabilidad de servidores, ataca de raíz la vulnerabilidad evidenciada durante las temporadas críticas de inscripciones. Al distribuir el tráfico de la red de manera dinámica, se previene la saturación y se asegura que la prestación del servicio administrativo se mantenga estable frente a concurrencias masivas.

Para contrarrestar la amenaza de pérdida definitiva de información, esta misma directriz de continuidad exige la verificación rigurosa de la recuperabilidad de los datos. El control propuesto consiste en simulacros trimestrales de restauración de backups, lo cual transforma un respaldo inactivo en una garantía comprobable. Al validar rutinariamente que los históricos financieros y de investigación pueden ser reconstruidos, la institución reduce drásticamente su nivel de riesgo frente a eventos catastróficos o infecciones destructivas.

Frente a la vulnerabilidad provocada por el exceso de confianza de la comunidad ante el phishing, la Política de Concientización aborda directamente el factor humano. El desarrollo de simulaciones y capacitaciones funciona como un control administrativo indispensable para modificar las conductas imprudentes de los docentes y colaboradores, ya que, al instruir a los usuarios para que duden de enlaces sospechosos, disminuye la probabilidad de que sus perfiles sean comprometidos y utilizados como puente para inyectar un secuestro de datos en la red central.
Por su parte, la Política de Clasificación y Tratamiento resuelve la desorganización estructural al estandarizar cómo deben manejarse los proyectos confidenciales. Esta normativa, al integrarse con la Política de Uso Aceptable (BYOD), establece barreras claras sobre la exportación de la propiedad intelectual hacia memorias no autorizadas. En

la práctica operativa, estas políticas exigen la aplicación de controles de software altamente restrictivos, ordenando el cifrado obligatorio de los discos duros institucionales asignados a los investigadores.

La ejecución disciplinada de este modelo de cifrado frenaría el impacto provocado por el robo de dispositivos físicos, garantizando así que el conocimiento científico de la universidad se mantenga en absoluta reserva. El conjunto coordinado de estas iniciativas metodológicas permite que la Dirección de Tecnología abandone las respuestas reactivas para consolidar una postura preventiva superior, blindando la integridad del servicio y fortaleciendo la confiabilidad institucional ante su comunidad educativa.

Gestión de incidentes y continuidad del negocio

Tabla 7. Incidentes potenciales

Incidente	***Descripción***	***Impacto***

Caída del sistema académico por sobrecarga	Colapso y pérdida de disponibilidad de la plataforma central debido a un pico masivo de tráfico durante la temporada de matrículas.	Interrupción crítica de la gestión académica y financiera, impidiendo el registro de asignaturas y el recaudo de pagos institucionales.
Fuga de credenciales por ataques de phishing	Un funcionario o docente entrega sus datos de acceso tras ser engañado por un correo electrónico que suplanta la identidad de la rectoría.	Compromiso total de la red interna, facilitando el acceso a bases de datos sensibles o la inyección de un *ransomware* destructivo.
Robo de hardware con propiedad intelectual	Hurto de un equipo portátil institucional asignado a un docente investigador mientras se encontraba fuera del campus universitaria.	Exposición no autorizada de proyectos de investigación confidenciales y pérdida de los avances científicos no respaldados en la nube.
Eliminación masiva de información colaborativa	Borrado accidental o intencional de documentos alojados en una plataforma compartida debido a una falla en la configuración de permisos.	Pérdida de integridad y disponibilidad de expedientes documentales vitales para el funcionamiento administrativo de múltiples dependencias.
Acceso no autorizado a historiales ajenos	Un estudiante logra visualizar o modificar información académica que no corresponde a su programa mediante la explotación de una vulnerabilidad.	Violación flagrante del principio de confidencialidad y del derecho al *Habeas Data*, exponiendo a la universidad a severas sanciones legales.

Tabla 8. Plan básico de respuesta

Fase	***Acción***
Preparación	Establecer el Equipo de Respuesta ante Incidentes, definir canales de comunicación de crisis, automatizar copias de seguridad y capacitar a la comunidad.
Identificación	Monitorear continuamente la red para detectar anomalías, clasificar la severidad del evento y documentar los hallazgos técnicos iniciales.
Contención	Aislar inmediatamente los equipos infectados, bloquear cuentas comprometidas y mitigar el tráfico anómalo para evitar la propagación del daño al resto de la red.
Erradicación	Eliminar el código malicioso de los sistemas afectados, corregir las vulnerabilidades explotadas, reconfigurar los permisos y forzar el cambio de credenciales.
Recuperación	Restaurar las operaciones utilizando las copias de seguridad limpias, reconectar los sistemas de forma gradual y monitorizar el comportamiento de la red.
Lecciones aprendidas	Realizar una auditoría posterior al evento para documentar las fallas, evaluar la efectividad de la respuesta y actualizar los protocolos preventivos de seguridad.

Para garantizar la resiliencia tecnológica y administrativa frente a los incidentes descritos, la Universidad Innovar del Pacífico debe trascender la improvisación y adoptar una estrategia formal de continuidad. Esta capacidad de respuesta se fundamenta en la activación inmediata del Plan de Respuesta ante Incidentes y en la ejecución paralela del Plan de Continuidad del Negocio (BCP), los cuales garantizan que la misión educativa no se detenga ante una contingencia.

El primer pilar para mantener la continuidad operativa radica en la formalización de un Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT). Este comité, liderado por la Dirección de Tecnología y apoyado por las vicerrectorías, asume el control técnico ante cualquier crisis. Por ejemplo, ante una amenaza originada por un correo de phishing, el CSIRT ejecuta la fase de contención, aislando lógicamente los servidores virtualizados para así evitar que el ataque alcance el ERP financiero.

Cuando un incidente impacta directamente la disponibilidad de los servicios críticos, como la caída del sistema durante la temporada de matrículas, la organización debe activar su Plan de Recuperación ante Desastres (DRP). En este escenario, la universidad responderá redirigiendo el tráfico masivo mediante balanceadores de carga y habilitando servidores de respaldo en la nube. Esta redundancia técnica asegura que, mientras se estabiliza la plataforma principal, los estudiantes puedan continuar registrando sus pagos en un portal de contingencia.

En los escenarios donde la integridad de los datos se vea vulnerada, ya sea por el borrado accidental en plataformas colaborativas o por un secuestro de información, la continuidad dependerá exclusivamente de la estrategia de copias de seguridad. La organización responderá procediendo a la restauración de la información utilizando los respaldos inmutables almacenados en la nube. Para garantizar que esta acción sea inmediata, la institución habrá ejecutado pruebas de restauración previas de forma rutinaria.

La gestión de incidentes también contempla el manejo de violaciones a la confidencialidad, como el acceso no autorizado de estudiantes o el robo de un equipo a un investigador. La respuesta técnica consiste en revocar remotamente todas las sesiones activas, modificar las credenciales globales y ejecutar el borrado a distancia del disco duro del portátil robado mediante un software de gestión de dispositivos (MDM), protegiendo así la propiedad intelectual de inmediato.

De manera simultánea a las acciones técnicas, la continuidad exige una gestión de crisis comunicacional impecable. La universidad mantendrá informada a la comunidad académica a través de canales internos, como redes sociales o mensajes de texto, en caso de que el correo institucional falle. Si el incidente resulta en una filtración de datos personales, la organización cumplirá con su deber legal notificando a la Superintendencia de Industria y Comercio (SIC) y a los titulares afectados.

Como fase concluyente del ciclo, la organización garantizará su mejora continua mediante el análisis posterior a la crisis. Cada incidente superado generará un informe de lecciones aprendidas que detallará las brechas del esquema defensivo. Esta retroalimentación se utilizará para actualizar las políticas, endurecer los controles técnicos y rediseñar las campañas de capacitación, asegurando en sí que la universidad fortalezca de manera permanente su ecosistema digital.

Tabla 9. Hallazgos organizacionales

Situación observada	***Riesgo asociado***
Delegación de responsabilidad: Los usuarios asumen que la seguridad es una labor exclusiva del área de TI.	Apatía generalizada ante la protección de datos, lo que retrasa la detección y el reporte oportuno de amenazas por parte del usuario final.
Resistencia a controles: Existe oposición al uso de autenticación adicional y los docentes priorizan la comodidad de acceso.	Exposición de plataformas críticas al mantener accesos vulnerables, facilitando la intrusión de actores malintencionados con credenciales simples.
Comportamiento estudiantil riesgoso: Los estudiantes no protegen sus credenciales institucionales o las comparten.	Pérdida de confidencialidad y trazabilidad, permitiendo que atacantes accedan a la red asumiendo la identidad de usuarios legítimos.
Exceso de confianza digital: Alta vulnerabilidad y confianza desmedida en enlaces recibidos por correo electrónico.	Infección masiva de la red por malware e inyección de ransomware a través de ataques de ingeniería social o phishing
Ausencia normativa y formativa: La ciberseguridad no se aborda en inducciones y cada área maneja la información sin criterios comunes.	Manipulación inadecuada de datos sensibles y fuga de información debido al desconocimiento de los protocolos por parte de los empleados

Tabla 10. Recomendaciones de mejora

Hallazgo	***Recomendación***
Delegación de responsabilidad	Lanzar campañas de sensibilización que demuestren que la seguridad es una responsabilidad compartida, fomentando la cultura del "firewall humano".
Resistencia a controles	Implementar gradualmente el Múltiple Factor de Autenticación (MFA) acompañado de talleres prácticos que evidencien sus beneficios reales para el usuario.
Comportamiento estudiantil riesgoso	Incorporar un módulo de "Higiene Digital" obligatorio para los estudiantes al inicio de cada semestre, enfatizando el carácter intransferible de sus cuentas.
Exceso de confianza digital	Ejecutar simulacros controlados de phishing ético de manera sorpresiva, acompañados de retroalimentación inmediata para entrenar el escepticismo digital.
Ausencia normativa y formativa	Unificar la política de clasificación de información para toda la institución e incluirla obligatoriamente en todos los procesos de inducción del talento humano.

La cultura organizacional en ciberseguridad trasciende la mera implementación de software o herramientas tecnológicas. Esta representa el conjunto de valores, actitudes y comportamientos que los miembros de la Universidad Innovar del Pacífico adoptan frente a la protección de la información corporativa y personal. Las recomendaciones estructuradas en la tabla anterior tienen como propósito fundamental transformar el factor humano, pasando de ser considerado el eslabón más débil de la cadena tecnológica a convertirse en la primera y más sólida línea de defensa de la institución.

En primer lugar, abordar la creencia errónea de que la protección recae de manera exclusiva en la Dirección de Tecnología es el pilar indispensable de este cambio cultural. Mediante campañas de sensibilización continua, se busca implementar una mentalidad de corresponsabilidad; cuando un docente, estudiante o empleado administrativo comprende que un simple clic descuidado en un correo fraudulento tiene el potencial de comprometer los proyectos de investigación o los datos de toda la comunidad, se desarrolla una actitud proactiva orientada a la prevención y al reporte inmediato de anomalías.

En segundo lugar, las recomendaciones apuntan a disolver la resistencia al cambio, el cual se manifiesta como un fenómeno recurrente frente a los mecanismos adicionales de autenticación y la priorización de la comodidad sobre la prevención. La habilitación progresiva de controles como la Autenticación Multifactor (MFA), acompañada de un fuerte componente pedagógico, desmitifica la idea de que la seguridad es un obstáculo para la productividad. Esta estrategia educativa logra que la comunidad académica asimile los controles no como una imposición restrictiva, sino como un escudo indispensable que resguarda su propio trabajo.

Adicionalmente, enfrentar la confianza excesiva en enlaces web y la falta de recelo con las contraseñas estudiantiles mediante simulacros de phishing ético generaría un impacto de concientización sumamente efectivo. La experiencia práctica y el aprendizaje originado a través del error en un entorno controlado interiorizan el riesgo de una manera mucho más profunda que la capacitación teórica tradicional, agudizando el sentido crítico y la malicia digital frente a amenazas externas.

A modo de cierre, integrar los conceptos de ciberseguridad directamente en los procesos de inducción garantiza que el nuevo talento asimile los estándares de protección desde su primer día de vinculación. Al unificar los lineamientos operativos para el manejo de la información en todas las vicerrectorías y dependencias, se erradica por completo la fragmentación normativa. Mediante estas acciones, la Universidad Innovar del Pacífico logra consolidar una cultura organizacional madura, en la cual la seguridad de los datos pasa de ser una exigencia técnica para convertirse en un hábito natural e institucionalizado que garantice la continuidad de su misión educativa.

Conclusiones

A partir del diagnóstico de ciberseguridad y seguridad de la información realizado a la Universidad Innovar del Pacífico, se presentan cinco conclusiones fundamentales enfocadas estrictamente en los resultados operativos de la evaluación:

En primer lugar, se concluye que la ausencia de un Sistema de Gestión de Seguridad de la Información (SGSI) formal es el origen de las principales vulnerabilidades de la institución. El aprendizaje central es que la inversión en infraestructura robusta no garantiza la protección si se carece de un gobierno de TI estructurado que permita a la alta dirección alinear la tecnología con los objetivos misionales, demostrando que operar bajo una postura puramente reactiva es técnica y operativamente insostenible.

En segundo lugar, el análisis de la gestión de identidades demostró que las deficiencias en el control de accesos internos pueden anular cualquier defensa perimetral. El hallazgo de credenciales activas de exfuncionarios y el uso compartido de contraseñas evidencian una desconexión crítica entre los procesos administrativos y el área de tecnología. Como aprendizaje, se establece que la validación estricta de la identidad es el verdadero perímetro de seguridad institucional, lo que comprueba que los modelos tradicionales de acceso resultan insuficientes para frenar intrusiones internas.

En tercer lugar, se determina que la institución posee una falsa sensación de resiliencia operativa frente a la continuidad del negocio. El hallazgo de respaldos en la nube sin pruebas de restauración comprobables, sumado a las caídas del sistema académico, revela una fragilidad extrema. El aprendizaje es que un respaldo no verificado es apenas una esperanza técnica, inútil ante un desastre real, lo cual ratifica el riesgo inminente que corre la universidad al carecer de una arquitectura tecnológica orientada a la alta disponibilidad.

En cuarto lugar, el diagnóstico ratifica que el factor humano sigue siendo el vector de ataque más vulnerable y descuidado. La confianza desmedida en correos electrónicos sospechosos y la delegación absoluta de la ciberseguridad al departamento de TI muestran una apatía organizacional riesgosa. El aprendizaje derivado es que la tecnología más avanzada resulta inútil si el usuario final entrega sus accesos voluntariamente, confirmando que la falta de cultura preventiva en la comunidad universitaria representa un riesgo tan crítico como cualquier falla de software.

Como quinta deducción, se evidencia que la gestión inadecuada de los datos sensibles trasciende el riesgo operativo para convertirse en una amenaza legal y reputacional directa. La falta de lineamientos claros para el manejo de información confidencial y el uso de dispositivos físicos sin cifrar exponen a la universidad al incumplimiento de la normativa vigente sobre protección de datos. El aprendizaje fundamental de este ejercicio es que la ciberseguridad no solo protege infraestructura, sino que también salvaguarda el prestigio y el patrimonio intelectual, haciendo de la desorganización de la información institucional un riesgo corporativo inaceptable.

Referencias

Anchundia-Betancourt, C. E. (2017). Ciberseguridad en los sistemas de información de las universidades. Dominio de las Ciencias, 3(3), 200-217. https://dialnet.unirioja.es/servlet/articulo?codigo=6102849

Arévalo Moscoso, F. M., Cedillo Orellana, I. P., & Moscoso Bernal, S. A. (2017). Metodología ágil para la gestión de riesgos informáticos. Killkana Técnica, 1(3), 33-40. https://killkana.ucacue.edu.ec/index.php/killkana_tecnico/article/view/81/122

Bocanegra Monroy, I. L., Aragón Gil, L. V., Cortez Durán, M. C., & Solano de Jinete, N. (2025). Análisis de la protección del derecho al internet en el ordenamiento jurídico colombiano. Educación y Vida Sostenible, 3(3), 139-158. https://doi.org/10.57175/evsos.v3i3.249

Chávez Muñoz, H. J. (2026). Modelo de políticas y procedimientos basado en normas ISO/IEC 27001 para la estandarización y mejora de los servicios y procesos de tecnologías de la información en AW Faber-Castell Peruana SA [Trabajo de suficiencia profesional, Universidad San Ignacio de Loyola]. Repositorio Institucional USIL. https://hdl.handle.net/20.500.14005/17881

Espinel Suancha, L. T. (2025). Protección de datos sensibles en entornos digitales a partir de la implementación de los estándares ISO 27001 e ISO 27002 para la seguridad de la información [Trabajo de grado, Universidad Nacional Abierta y a Distancia]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/75515

Ferrari Fernández, F. E., & Hilario Rivas, J. L. (2025). Plan de Sistema de Gestión de Seguridad de la Información para mejorar la Administración de Riesgo. Revista Aula Virtual, 6(13), 2367-2382. https://doi.org/10.5281/zenodo.18076040

Guerrero Pérez, C., Toro Álvarez, M. G., & González Arcila, L. E. (2026). Ciberdelincuencia y criminalidad digital: retos del sistema penal colombiano. Universidad Libre. https://hdl.handle.net/10901/32341

Mejía Medina, M. (2019). Implementación de técnicas de seguridad informática para garantizar los principios de integridad, confidencialidad y disponibilidad de la información a un sistema de radiolocalización híbrido [Tesis de maestría, Escuela de Ingenierías]. Repositorio Institucional. http://hdl.handle.net/20.500.11912/4682

Muñoz Campuzano, P. S. (2021). Modelos de seguridad para prevenir riesgos de ataques Informáticos: Una revisión sistemática [Tesis de pregrado, Universidad Politécnica Salesiana]. Repositorio Institucional UPS. http://dspace.ups.edu.ec/handle/123456789/20932

Quiroz Zambrano, S. M., & Macías Valencia, D. G. (2017). Seguridad en informática: consideraciones. Dominio de las Ciencias, 3(3), 676-688. https://dialnet.unirioja.es/servlet/articulo?codigo=6137824

Rodríguez Zambrano, H. M., & Moreno Tamayo, C. H. (2024). Seguridad de la información y ciberseguridad: su importancia para los Estados, empresas y las personas, una revisión sistemática. Estudios y Perspectivas Revista Científica y Académica, 4(1), 159-178. https://doi.org/10.61384/r.c.a..v4i1.90

Solarte Solarte, F. N. J., Enriquez Rosero, E. R., & Benavides Ruano, M. C. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista Tecnológica ESPOL - RTE, 28(5), 492-507. https://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456

Voutssas, M. (2010). Preservación documental digital y seguridad informática. Investigación bibliotecológica, 24(50), 127-155. http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008&lng=es&tlng=es