

APUNTES PEDAGÓGICOS:

HACIA UN HÁBITAT DIGITAL QUE HUMANIZA

6

PROPUESTA DE EVALUACIÓN
AUTÉNTICA DIGITAL PARA LA
CARRERA DE INGENIERÍA EN
CIBERSEGURIDAD Y GESTIÓN DE
TECNOLOGÍAS DE LA INFORMACIÓN
DE LA PUCE

Por:

MSc. Damián Nicolalde
PhD. Ricardo Orellana



Este artículo propone un modelo de mejora para la evaluación de la carrera de Ingeniería en Ciberseguridad y Gestión de Tecnologías de la Información de la Pontificia Universidad Católica del Ecuador (PUCE), a partir del análisis documental de los anexos curriculares, la malla académica y artículos sobre evaluación auténtica, educación en línea, inteligencia artificial generativa e integridad académica. El diagnóstico muestra que la carrera posee una orientación metodológica pertinente, basada en aprendizaje por proyectos y retos, WebLabs, entornos virtuales de aprendizaje y formación ética; sin embargo, la evaluación se formula de manera general mediante cuestionarios, tareas prácticas, proyectos y criterios claros, sin una matriz operacional que vincule resultados de aprendizaje, evidencias, rúbricas, retroalimentación y mecanismos de verificación de autoría. Se propone un modelo de evaluación auténtica digital para ciberseguridad compuesto por seis principios: desempeño técnico verificable, alineación curricular, retroalimentación sostenible, Sustentación Técnica Sincrónica, uso responsable de inteligencia artificial y trazabilidad de evidencias. El artículo plantea una matriz de instrumentos evaluativos, una distribución referencial de ponderaciones y una ruta de implementación por niveles, con el propósito de fortalecer la validez, pertinencia profesional e integridad académica de la evaluación en modalidad en línea.

Términos índice—Ciberseguridad, educación en línea, evaluación auténtica, evaluación digital, inteligencia artificial generativa, PUCE.

1. Introducción

La carrera de Ingeniería en Ciberseguridad y Gestión de Tecnologías de la Información de la PUCE se plantea como una respuesta académica a la necesidad de formar profesionales capaces de diseñar, implementar y administrar sistemas seguros y eficientes de información y comunicaciones. Los documentos curriculares describen una propuesta en modalidad en línea, con sede en Quito, duración de ocho niveles, cuarenta y ocho asignaturas, ciento veinte créditos y cinco mil setecientos sesenta horas de formación. La malla curricular integra fundamentos matemáticos y computacionales, programación, redes, sistemas operativos, bases de datos, criptografía, seguridad en aplicaciones, auditoría, seguridad en la nube, análisis forense, respuesta a incidentes, gestión de identidad, seguridad en industria 4.0 e integración curricular [1], [2].

El diseño académico declara un modelo de aprendizaje basado en proyectos y retos, apoyado por aulas virtuales, videoconferencias, foros, recursos digitales, actividades prácticas y WebLabs [3], [4]. Esta orientación es adecuada para una carrera de ciberseguridad, pues el desempeño profesional no se reduce al recuerdo conceptual: exige diagnosticar vulnerabilidades, proponer controles, configurar entornos, interpretar evidencia técnica, comunicar riesgos y tomar decisiones éticas bajo restricciones reales. Por ello, la evaluación debe comprobar no solo conocimiento declarativo, sino desempeño

situado y verificable.

El análisis de los documentos muestra que la evaluación está presente como intención, pero todavía no como sistema. La justificación de modalidad en línea indica que se diseñarán actividades como cuestionarios, tareas prácticas y proyectos dentro de la plataforma de aprendizaje, con criterios claros de evaluación [5]. El anexo de plataforma tecnológica describe foros, cuestionarios, talleres, encuestas, juegos, proyectos, retos, presentación del trabajo y retroalimentación [3]. No obstante, los documentos no desarrollan una arquitectura evaluativa completa que precise evidencias por competencia, rúbricas, ponderaciones, trazabilidad del trabajo, Sustentación Técnica Sincrónica, coevaluación, autoevaluación y mecanismos de uso responsable de inteligencia artificial.

En este contexto, el objetivo del artículo es proponer una mejora de la evaluación de la carrera mediante un modelo de evaluación auténtica digital. La propuesta busca fortalecer la coherencia entre perfil de egreso, resultados de aprendizaje, metodología en línea y exigencias propias del campo de la ciberseguridad.

2. Fuentes y método de análisis

El artículo se elaboró mediante análisis documental de tres conjuntos de fuentes. El primer conjunto corresponde a los documentos de carrera: anexo de pertinencia, infraestructura, plataforma tecnológica, profesores, docencia, investigación, vinculación, formato de oferta académica, formulario RANT, informe académico, justificación de modalidad en línea y malla curricular [1]-[11]. El segundo conjunto corresponde a cuatro artículos: una propuesta sobre evaluación auténtica, transformación digital e inteligencia artificial [12]; una revisión de alcance sobre diseño de evaluación auténtica [13]; un estudio sobre presentaciones grupales sincrónicas en cursos en línea para adultos [14]; y una guía aplicada sobre evaluación auténtica en programas en línea [15].

El tercer conjunto incorpora tres documentos institucionales de PUCE Virtual: el Informe de acompañamiento pedagógico docente de las carreras y programas de la modalidad en línea, el apunte sobre el modelo TPACK y la formación del docente virtual, y el apunte sobre pedagogía digital situada [16]–[18]. Estas fuentes se utilizaron para contrastar la propuesta con hallazgos institucionales sobre evaluación, verificación del aprendizaje, uso de herramientas digitales, aula virtual, presencia docente y accesibilidad.

El procedimiento consistió en identificar: a) el perfil de formación y resultados de aprendizaje declarados por la carrera; b) la estructura de horas, créditos y asignaturas de la malla; c) la metodología de enseñanza-aprendizaje prevista; d) la forma en que los documentos describen evaluación; y e) los principios de evaluación auténtica y evaluación en línea

derivados de los artículos. A partir de ese contraste se definieron brechas y se construyó una propuesta de mejora.

3. Diagnóstico de la evaluación inicial

La carrera presenta fortalezas importantes para construir un sistema de evaluación robusto. En primer lugar, el perfil de egreso declara capacidades vinculadas con programación, algoritmos, selección de tecnologías, inteligencia artificial, evaluación crítica de soluciones, resolución de problemas de seguridad, diseño de soluciones empresariales, tendencias de ciberseguridad, análisis forense, respuesta a incidentes, ética y responsabilidad social [6]. En segundo lugar, la malla curricular incorpora asignaturas que permiten evaluar progresivamente competencias técnicas y de gestión, desde fundamentos de programación hasta análisis forense, auditoría, seguridad en la nube y gestión de identidad [1]. En tercer lugar, la modalidad en línea cuenta con una justificación basada en entornos virtuales, WebLabs, comunicación sincrónica y asincrónica, recursos digitales, tutoría y seguimiento [3]-[5].

La debilidad principal no está en la orientación pedagógica, sino en el nivel de operacionalización evaluativa. La evaluación se menciona como una actividad asociada a cuestionarios, tareas prácticas y proyectos, pero no se presenta como un sistema integrado. Tampoco se observa una matriz que vincule resultados de aprendizaje con evidencias concretas, criterios, instrumentos, porcentajes, momentos de retroalimentación y herramientas tecnológicas. Esta ausencia puede afectar la validez de la evaluación, especialmente en una carrera en línea donde la integridad académica, la autoría de productos y la demostración del desempeño técnico requieren evidencias más fuertes que una entrega escrita (véase tabla I).

TABLA I

DIAGNÓSTICO SINTÉTICO DE LA EVALUACIÓN PLANTEADA

Aspecto	Estado observado	Riesgo	Mejora requerida
Enfoque metodológico	Aprendizaje basado en proyectos y retos; aula invertida; recursos virtuales y WebLabs.	Que el modelo quede como declaración pedagógica sin instrumentos evaluativos consistentes.	Convertir proyectos y retos en evidencias evaluables con rúbricas, entregables y Sustentación Técnica Sincrónica.
Instrumentos	Se mencionan cuestionarios, tareas prácticas, proyectos, foros y presentaciones.	Uso de instrumentos genéricos aplicables a cualquier carrera en línea.	Diseñar instrumentos específicos de ciberseguridad: laboratorios, reportes técnicos, bitácoras, análisis forense y planes de respuesta.

Alineación	Existen resultados de aprendizaje de carrera y asignaturas técnicas en la malla.	Falta trazabilidad explícita entre resultado, evidencia e instrumento.	Implementar matriz resultado-evidencia-rubrica-herramienta.
Integridad académica	Se reconoce evaluación en línea, pero no se detalla verificación de autoría.	Dependencia excesiva de entregas escritas vulnerables al uso no declarado de IA.	Agregar Sustentación Técnica Sincrónica, bitácora, evidencias de proceso y declaración de uso de IA.
Retroalimentación	Se menciona retroalimentación docente en proyectos y modalidad en línea.	Retroalimentación no estructurada ni sostenible.	Definir hitos formativos: propuesta, avance, prueba técnica, entrega y reflexión final.

4. Fundamento conceptual: Evaluación auténtica digital

Los artículos revisados coinciden en que la evaluación en educación superior debe evolucionar desde pruebas centradas en el recuerdo hacia tareas que demanden aplicación, juicio, colaboración y reflexión. Perla y Vinci sostienen que la transformación digital y la inteligencia artificial han impulsado la diversificación de herramientas de evaluación, la analítica de aprendizaje y la necesidad de equilibrar enfoques tecnocráticos con una mirada humanista [12]. Para esta carrera, el punto central es que la tecnología no debe utilizarse solamente para trasladar exámenes al entorno virtual, sino para enriquecer la evidencia del aprendizaje mediante procesos continuos, datos de participación, retroalimentación y apoyo al estudiante.

La revisión de Zhan, Boud y Du es especialmente relevante porque caracteriza la evaluación auténtica mediante dimensiones de autenticidad, desafío cognitivo, criterios, retroalimentación, agencia estudiantil y colaboración social [13]. Esta perspectiva permite evaluar una carrera de ciberseguridad desde un marco más completo: no basta con que la tarea se parezca al trabajo profesional; debe ser cognitivamente exigente, tener criterios transparentes, involucrar al estudiante como agente de su aprendizaje, ofrecer retroalimentación transferible y reconocer la dimensión colaborativa y social de la seguridad digital.

El estudio de Viswanathan y Ng aporta evidencia aplicable a la modalidad en línea. Al sustituir tareas escritas por presentaciones grupales sincrónicas, el estudio encontró mejoras en colaboración, interacción, comprensión de contenidos y confianza para presentar ideas, además de un efecto positivo frente a problemas de integridad académica asociados con inteligencia artificial generativa [14]. Aunque se trata de un estudio de escala limitada y de otra disciplina, su utilidad para ciberseguridad es directa: una Sustentación Técnica Sincrónica de un laboratorio o proyecto obliga al estudiante a explicar decisiones, responder preguntas, justificar técnicamente su práctica y demostrar dominio situado.

Aziz y Gasevic proponen revisar la autenticidad de las evaluaciones considerando alineación con resultados de aprendizaje, estándares de habilidades, racionalidad evaluativa, pertinencia del método, autenticidad profesional, desarrollo de habilidades y contexto [15]. Su aporte práctico es entender la autenticidad como un continuo. Esto es importante para la carrera: no se requiere eliminar los instrumentos actuales, sino rediseñarlos para que se acerquen progresivamente a tareas profesionales verificables.

5. Propuesta de modelo

Se propone un Modelo de Evaluación Auténtica Digital para Ciberseguridad, orientado a transformar la evaluación de la carrera desde una lógica de actividades aisladas hacia un sistema de evidencias integradas. El modelo se compone de seis principios (véase tabla II).

- **Desempeño técnico verificable.** Cada asignatura técnica debe incluir al menos una evidencia en la que el estudiante produzca, configure, analice, defienda o documente una solución. En ciberseguridad, la evidencia puede ser un entorno endurecido, un reporte de vulnerabilidades, una arquitectura segura, un script, una política de acceso, un análisis de logs, una cadena de custodia simulada o un plan de continuidad.
- **Alineación curricular explícita.** Toda evaluación relevante debe declarar el resultado de aprendizaje que mide, la competencia profesional asociada, el instrumento, los criterios de logro y la herramienta utilizada. Esta alineación reduce la distancia entre perfil de egreso y actividades de aula.
- **Retroalimentación sostenible.** Los proyectos y laboratorios deben evaluarse en hitos: planteamiento del problema, diseño de solución, implementación o análisis, validación técnica, comunicación de resultados y reflexión. La retroalimentación no debe limitarse a justificar una nota; debe ayudar al estudiante a transferir criterios de calidad a situaciones futuras.
- **Sustentación Técnica Sincrónica.** En asignaturas clave, la entrega de productos debe complementarse con una Sustentación Técnica Sincrónica. Esta instancia puede ser individual o grupal, pero debe incluir preguntas técnicas, explicación de decisiones, revisión de evidencias y justificación profesional de la práctica realizada. Su propósito es que el estudiante brinde el sustento profesional de su trabajo de ciberseguridad, demuestre autoría y haga explícito el razonamiento técnico que sustenta sus decisiones en modalidad en línea y frente al uso de inteligencia artificial generativa. Los parámetros operativos mínimos de esta instancia se presentan en el Anexo I, Protocolo de STS (Sustentación Técnica Sincrónica).

- **Uso responsable de inteligencia artificial.** La carrera no debería tratar la IA solo como amenaza. En un campo tecnológico, es más pertinente exigir declaración de uso, trazabilidad de prompts o herramientas cuando corresponda, comparación crítica de respuestas generadas, validación técnica independiente y responsabilidad final del estudiante sobre el producto entregado.
- **Trazabilidad de evidencias.** Cada evaluación práctica debe dejar rastros mínimos: bitácora, capturas, repositorio, archivo de configuración, reporte, video corto, registro de pruebas, historial de cambios o registro o acta de Sustentación Técnica Sincrónica. La trazabilidad fortalece la integridad académica y mejora la capacidad del docente para valorar proceso y producto.

TABLA II

MATRIZ PROPUESTA DE INSTRUMENTOS DE EVALUACIÓN AUTÉNTICA DIGITAL

Instrumento	Evidencia esperada	Criterios principales	Aplicación sugerida
Laboratorio técnico en WebLab	Configuraciones, capturas, comandos, resultados de pruebas y breve reporte.	Corrección técnica, reproducibilidad, análisis de riesgos, documentación.	Redes, sistemas operativos, criptografía, seguridad web, nube, forense.
Reto o caso aplicado	Solución a un escenario realista con restricciones técnicas y organizacionales.	Pertinencia de la solución, argumentación, priorización, impacto.	Gestión de riesgos, continuidad, auditoría, seguridad empresarial.
Reporte profesional	Informe ejecutivo y técnico con hallazgos, evidencias y recomendaciones.	Claridad, rigor, trazabilidad, lenguaje profesional, ética.	Auditoría, vulnerabilidades, respuesta a incidentes, seguridad legal.
Bitácora de proceso	Registro de decisiones, pruebas, errores, ajustes y uso de herramientas.	Reflexión, honestidad metodológica, aprendizaje de errores, secuencia lógica.	Proyectos, laboratorios extensos, integración curricular.
Sustentación Técnica Sincrónica	Presentación y respuesta a preguntas técnicas.	Dominio conceptual, explicación de decisiones, comunicación, autoría.	Asignaturas de quinto a octavo nivel y proyectos integradores.
Coevaluación y autoevaluación	Valoración individual y grupal con criterios definidos.	Responsabilidad, colaboración, juicio evaluativo, contribución individual.	Proyectos grupales, presentaciones, retos interdisciplinarios.

6. Distribución referencial de ponderaciones

Como referencia para asignaturas técnicas, se propone una estructura flexible que cada docente pueda ajustar según los resultados de aprendizaje. Los laboratorios técnicos deberían representar entre 25% y 35% de la calificación; el proyecto o reto aplicado, entre 20% y 30%; las evaluaciones conceptuales o cuestionarios, entre 10% y 20%; los reportes

técnicos, entre 10% y 15%; la Sustentación Técnica Sincrónica, entre 10% y 15%; y la participación, autoevaluación o coevaluación, entre 5% y 10%. Esta distribución evita que el curso dependa de un examen final y preserva un espacio para verificar fundamentos conceptuales.

Para asignaturas de formación humanística, gestión o investigación, el mismo modelo puede adaptarse mediante estudios de caso, análisis ético, diseño de políticas, informes de investigación, debates sincrónicos, portafolios y proyectos de vinculación. La evaluación auténtica no exige que todas las asignaturas tengan laboratorios técnicos; exige que cada asignatura produzca evidencias coherentes con su contribución al perfil de egreso.

7. Implementación por niveles

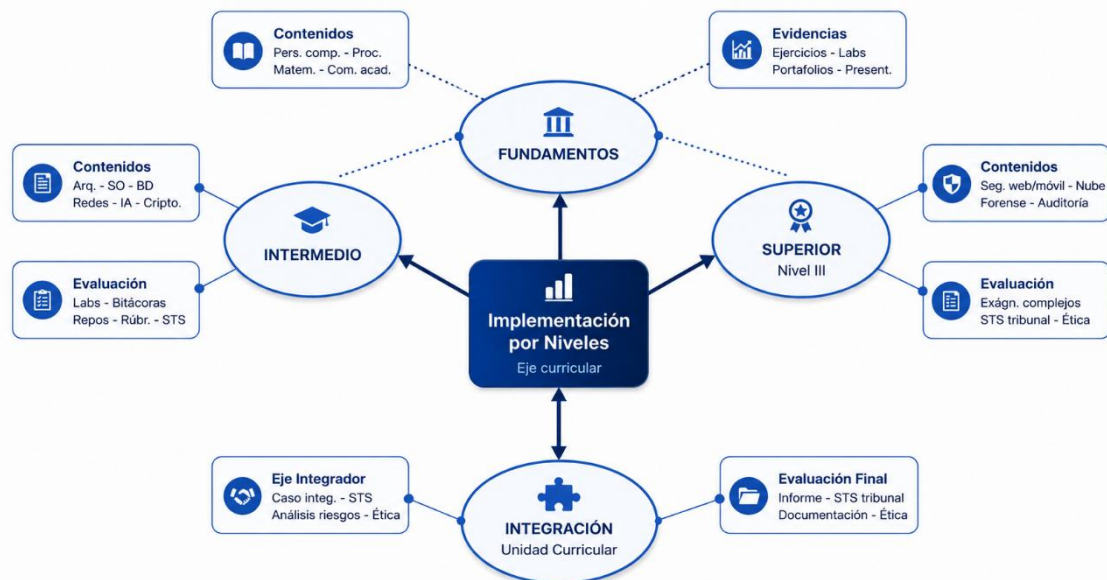
La malla curricular permite una implementación progresiva. En los primeros niveles, la evaluación debe concentrarse en fundamentos, resolución de problemas, pensamiento computacional, programación inicial, matemáticas y comunicación académica. Las evidencias pueden incluir ejercicios aplicados, pequeños laboratorios, portafolios de código, explicación de algoritmos y presentaciones breves.

En los niveles intermedios, donde aparecen arquitectura de computadoras, sistemas operativos, bases de datos, redes, desarrollo en plataformas, inteligencia artificial y criptografía, la evaluación debe aumentar el componente de laboratorio y reto. En esta etapa conviene introducir bitácoras, repositorios, rúbricas técnicas y Sustentación Técnica Sincrónica de prácticas seleccionadas.

En los niveles superiores, la evaluación debe acercarse al desempeño profesional. Auditoria, seguridad web y móvil, nube, gestión de identidad, análisis de amenazas, forense, respuesta a incidentes, seguridad industrial e integración curricular requieren escenarios complejos, informes profesionales, trabajo colaborativo, Sustentación Técnica Sincrónica y criterios de ética, legalidad y responsabilidad social. En estas asignaturas, las STS se aplicarán según el Protocolo de STS (Anexo I) y podrán realizarse con codocencia o tribunal académico en los hitos integradores.

La Unidad de Integración Curricular puede convertirse en el eje de validación del modelo. Tanto el trabajo de integración curricular como el examen complejo deberían incorporar evidencias de desempeño: resolución de un caso integrador, Sustentación Técnica Sincrónica, análisis de riesgos, documentación profesional y reflexión ética. De esta forma, la titulación mediría la capacidad del estudiante para integrar conocimientos y no solo para reproducir contenidos (véase figura 1).

Figura 1. Implementación por niveles



8. Condiciones institucionales

La propuesta requiere condiciones institucionales razonables y compatibles con los documentos existentes. La carrera ya declara uso de Moodle, aulas virtuales, videoconferencia, foros, recursos digitales, WebLabs, personal de diseño instruccional, equipo multimedia y soporte de planificación [3], [4]. Sobre esa base, la mejora evaluativa puede implementarse sin cambiar la naturaleza de la modalidad en línea.

No obstante, sí se requieren productos académicos adicionales: banco de rúbricas por tipo de instrumento, guía de evaluación auténtica digital, protocolo de Sustentación Técnica Sincrónica, formato de declaración de uso de IA, plantilla de bitácora, criterios de coevaluación, criterios de retroalimentación y matriz de trazabilidad por asignatura. Estos instrumentos permitirían que la evaluación sea consistente entre paralelos y docentes, especialmente cuando existan actividades grupales o proyectos de varias semanas.

Para evitar que la Sustentación Técnica Sincrónica (STS) genere una sobrecarga de trabajo en asignaturas con alta matrícula, su aplicación debe planificarse con criterios de escalabilidad. Se recomienda realizar STS obligatorias en laboratorios, retos, proyectos integradores o entregas de mayor ponderación, y utilizar muestreo académico para actividades de menor peso, con selección aleatoria, por riesgo o por desempeño. También pueden organizarse sesiones breves por equipos, complementadas con preguntas individuales rotativas; distribuir las sustentaciones en ventanas programadas durante el

período; y apoyarse en rúbricas analíticas, agenda previa, evidencias asincrónicas y grabación institucional cuando la normativa aplicable lo permita.

La codocencia constituye una alternativa viable y coherente con el modelo propuesto. Dos docentes que imparten la asignatura pueden compartir la preparación, observación y calificación de las STS; para hitos integradores, ambos docentes pueden conformar, junto con la coordinación de la carrera, un tribunal académico. Esta modalidad debe reservarse para proyectos de alta complejidad o asignaturas estratégicas, contar con una rúbrica común y roles definidos —moderación, preguntas técnicas, registro y consolidación de calificaciones—, y programarse con antelación. Así, la participación colegiada fortalece la consistencia y legitimidad de la valoración, sin convertir cada actividad ordinaria en un tribunal.

9. Discusión

La propuesta responde a una tensión central del expediente curricular. Por un lado, la carrera declara una metodología activa, práctica y orientada a proyectos. Por otro lado, la evaluación aparece todavía como una lista general de recursos de plataforma. Los artículos muestran que esta tensión es común en educación superior en línea: digitalizar la evaluación no garantiza autenticidad, integridad ni pertinencia profesional [12]-[15].

En ciberseguridad, la evaluación auténtica tiene un valor adicional. La profesión exige actuar con evidencia, justificar decisiones y respetar límites éticos y legales. Por ello, una evaluación basada en laboratorios, reportes, bitácoras y las sustentaciones técnicas sincrónicas no solo mejoran la medición del aprendizaje; también modelan prácticas profesionales. El estudiante aprende que una afirmación técnica debe sustentarse con pruebas, que un hallazgo debe documentarse, que una recomendación debe priorizar riesgos y que el uso de herramientas automatizadas no reemplaza el juicio profesional.

La propuesta también permite enfrentar el uso de inteligencia artificial generativa de forma más madura. En lugar de intentar prohibiciones difíciles de controlar, el modelo exige evidencias de proceso y Sustentación Técnica Sincrónica. Si un estudiante utiliza IA para apoyar redacción, generación de ideas o revisión de código, debe declararlo y demostrar que comprende, valida y asume responsabilidad sobre el resultado. Este enfoque es coherente con una carrera tecnológica y con la necesidad de formar criterio profesional.

10. Conclusión

La evaluación planteada actualmente en los documentos de la carrera de Ingeniería en Ciberseguridad y Gestión de Tecnologías de la Información de la PUCE posee una orientación adecuada, porque reconoce la modalidad en línea, los proyectos, los retos, las

tareas prácticas, los cuestionarios, los foros y la retroalimentación. Sin embargo, requiere una formulación más específica para el campo de la ciberseguridad. La mejora principal consiste en pasar de una evaluación descrita por tipos generales de actividad a un sistema de evaluación auténtica digital basado en evidencias verificables de desempeño.

El modelo propuesto articula desempeño técnico, alineación curricular, retroalimentación sostenible, Sustentación Técnica Sincrónica, uso responsable de inteligencia artificial y trazabilidad. Su aplicación permitiría fortalecer la validez de la evaluación, mejorar la integridad académica en modalidad en línea y demostrar con mayor claridad que los estudiantes pueden diagnosticar, configurar, analizar, defender, documentar y justificar soluciones de ciberseguridad. En consecuencia, la propuesta no reemplaza el diseño curricular existente; lo completa y lo vuelve más defendible académica y profesionalmente.

ANEXO I. PROTOCOLO DE STS (SUSTENTACIÓN TÉCNICA SINCRÓNICA)

Tabla A1. Guía operativa para la planificación, desarrollo y valoración de la STS.

Componente	Orientación operativa
Propósito	Verificar que el estudiante explique, justifique y sustente profesionalmente las decisiones, procedimientos, evidencias y resultados de una práctica de ciberseguridad. La STS valora razonamiento técnico, autoría, trazabilidad y responsabilidad ética.
Cuándo aplicar	Prioritariamente en laboratorios complejos, retos, proyectos integradores, auditorías, análisis forense, respuesta a incidentes y configuraciones de seguridad. La guía de la asignatura debe comunicar previamente producto, rúbrica, modalidad y fecha.
Duración sugerida	Individual: 10–15 minutos, incluidos 3–5 minutos de preguntas. Grupal: 20–30 minutos por equipo, más una ronda individual de 3–5 minutos por integrante. Puede realizarse por videoconferencia institucional con apoyo de WebLab, repositorio, bitácora, capturas, logs o reporte técnico.
Secuencia	1) identificación y encuadre del caso; 2) síntesis o demostración de la evidencia; 3) explicación de decisiones, riesgos y controles; 4) preguntas; 5) retroalimentación breve y registro de resultados.
Tipos de preguntas	Fundamento: conceptos, estándares y criterios. Decisión técnica: herramientas, configuraciones, prioridades y alternativas. Evidencia: comandos, logs, pruebas y hallazgos. Transferencia: respuesta ante cambios de escenario o amenazas. Ética y legalidad: autorización, datos y límites profesionales. En trabajos grupales se incluyen preguntas individuales.
Criterios de evaluación	Dominio técnico y conceptual (30%); calidad y pertinencia de la evidencia (20%); justificación profesional de decisiones, riesgos y controles (20%); trazabilidad, documentación y reproducibilidad (15%); comunicación técnica y respuesta a preguntas (10%); ética, legalidad y uso declarado de IA, cuando corresponda (5%). Cada criterio se operacionaliza con rúbrica analítica y niveles de logro.
Escalabilidad en alta matrícula	Aplicar STS obligatorias en evidencias de alta ponderación; usar muestreo académico en actividades menores; organizar franjas horarias y sesiones por equipos con preguntas individuales rotativas; solicitar evidencias asincrónicas previas; y utilizar rúbricas, agenda y registro común. Esto focaliza el tiempo docente sin perder verificación de autoría.
Codocencia y tribunal	En proyectos integradores o asignaturas estratégicas, dos docentes que imparten la asignatura pueden compartir moderación, preguntas y calificación. Junto con la coordinación de carrera pueden conformar un tribunal académico. Deben definirse roles, rúbrica compartida, agenda y mecanismo de consolidación de calificaciones. No se recomienda aplicar este formato a todas las actividades ordinarias.
Registro y retroalimentación	Conservar una ficha con fecha, participantes, evidencia revisada, preguntas relevantes, nivel alcanzado y retroalimentación. La grabación se realizará solo con fines académicos e institucionales, conforme a la normativa de protección de datos y disposiciones de la PUCE.

Referencias

- [1] Pontificia Universidad Católica del Ecuador, "MallaCurricularV6-18ABRIL2023-DGACiberseguridad," documento local de carrera, 2023.
- [2] Pontificia Universidad Católica del Ecuador, "Informe académico - RRA 2022_grado VF," documento local de carrera.
- [3] Pontificia Universidad Católica del Ecuador, "Anexo C criterio 2 Plataforma tecnológica," documento local de carrera.
- [4] Pontificia Universidad Católica del Ecuador, "Anexo A criterio 2 Infraestructura aulas, laboratorio y talleres," documento local de carrera.
- [5] Pontificia Universidad Católica del Ecuador, "Justificación modalidad en línea," documento local de carrera.
- [6] Pontificia Universidad Católica del Ecuador, "Anexo Criterio 4 DocenciaCiberseguridad," documento local de carrera.
- [7] Pontificia Universidad Católica del Ecuador, "Anexo del Criterio 1 Pertinencia_GradoCiber," documento local de carrera.
- [8] Pontificia Universidad Católica del Ecuador, "Anexo Criterio 3 Profesores_PROPUEST," documento local de carrera.
- [9] Pontificia Universidad Católica del Ecuador, "Anexo Criterio 5 Investigación - Ing. Ciberseguridad y Gestión de Tecnologías de la Información," documento local de carrera, 2023.
- [10] Pontificia Universidad Católica del Ecuador, "Anexo Criterio 6 Vinculación Ciberseguridad," documento local de carrera.
- [11] Pontificia Universidad Católica del Ecuador, "Formato diseño de oferta académica RRA 2022" y "Formulario justificación creación carrera y titulación_Anexo III RANT," documentos locales de carrera.
- [12] L. Perla and V. Vinci, "Enhancing authentic assessment in higher education: Leveraging digital transformation and artificial intelligence," artículo local en PDF.
- [13] Y. Zhan, D. Boud, and Z. Du, "Designing for authentic assessment: A scoping review," Higher Education, artículo local en PDF, 2025.

- [14] G. Viswanathan and B.-Y. Ng, "Rethinking online assessments for adult learners: Exploring synchronous group presentations," *Journal of Applied Learning & Teaching*, vol. 8, Special Issue no. 2, artículo local en PDF, 2025.
- [15] Z. Aziz and D. Gasevic, "Unlocking education opportunities: Authentic assessments in online programs," artículo local en PDF, 2024.
- [16] R. Orellana, "Informe de acompañamiento pedagógico docente de las carreras y programas de la modalidad en línea de PUCE Virtual", PUCE Virtual, informe institucional, 12 feb. 2026.
- [17] J. Balladares, "El modelo TPACK y la formación del docente virtual", *Apuntes pedagógicos: Hacia un hábitat digital que humaniza*, no. 4, PUCE Virtual, abr. 2026.
- [18] R. Orellana, "Hacia una pedagogía digital situada", *Apuntes pedagógicos: Hacia un hábitat digital que humaniza*, no. 5, PUCE Virtual, mayo 2026.

PUCE irtual

Dirección: PhD. Jorge Balladares

Diseño: Jessika Chicango

Agosto 2026

La excelencia no se improvisa

síguenos

