GRUPO BLR

TOMO II

GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN: UNA PERSPECTIVA DEL CONTROL INTERNO EN EL SECTOR PÚBLICO

Raquel Virginia Colcha Ortiz
Byron Napoleón Cadena Oleas
Michael Adrián Erazo Granizo
Alfredo Rodrigo Colcha Ortiz

Desarrollo operativo, evaluación, implementación y aplicación práctica del control interno de tecnologías de la información.

ISBN: 978-9907-0-0580-6

Año: 2025

TOMO II GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN: UNA PERSPECTIVA DEL CONTROL INTERNO EN EL SECTOR PÚBLICO

AUTORES

RAQUEL VIRGINIA COLCHA ORTIZ

BYRON NAPOLEÓN CADENA OLEAS

MICHAEL ADRIÁN ERAZO GRANIZO

ALFREDO RODRIGO COLCHA ORTIZ

GRUPO BLR

Este libro ha sido debidamente examinado y valorado en la modalidad doble par ciego con fin de garantizar la calidad científica.

©Grupo Editorial BLR
Riobamba – Ecuador
Correo: publicaciones@grupoblr.com
https://grupoblr.com/libros-investigo
REPOSITORIO

Colcha, R.,Cadena, B., Erazo, M., Colcha,A. (2025) Tomo II Gestión de tecnologías de la información: una perspectiva del control interno en el sector público. Grupo Editorial BLR.

ISBN:
978-9907-0-0580-6

FILIACIONES DE LOS AUTORES

Raquel Virginia Colcha Ortiz
Escuela Superior Politécnica de Chimborazo
Correo Electrónico: raquel.colcha@espoch.edu.ec.
ORCID: https://orcid.org/0000-0002-3252-9158

Byron Napoleón Cadena Oleas
Escuela Superior Politécnica de Chimborazo
Correo Electrónico: bcadena@espoch.edu.ec
ORCID: https://orcid.org/0000-0002-4535-5265

Michael Adrián Erazo Granizo
Universidad Nacional de Chimborazo
Correo Electrónico: michael.erazo@unach.edu.ec
ORCID: https://orcid.org/0000-0003-0247-1394

Alfredo Rodrigo Colcha Ortiz
Universidad Nacional de Chimborazo
Correo Electrónico: alfredo.colcha@unach.edu.ec
ORCID: https://orcid.org/0009-0005-2280-5189

GRUPO BLR

PRÓLOGO

La transformación digital del ámbito público ha dejado de ser una variable opcional para convertirse en un imperativo de operatividad y sostenibilidad institucional. En un ecosistema donde la información se ha posicionado como el recurso estratégico por antonomasia, las tecnologías de la información se constituyen en la espina dorsal que articula la eficiencia pública, la transparencia pública y la resiliencia de los servicios públicos. Sin embargo, para extraer este valor es preciso implementar una arquitectura de control interno sólida, caracterizada por los procesos estandarizados y la gobernanza que se alinean con la variabilidad de los riesgos actuales; esta es la necesidad que el Tomo II sistematiza.

La obra representa una intersección multidisciplinaria entre ingeniería, auditoría forense y gestión estratégica que pone a nuestra disposición un *framework* metodológico que transita entre la teoría y su ejecución factual. La auditoría tecnológica se reconfigura no como un tipo de revisión retrospectiva (post-mortem), sino como un sistema para el aseguramiento continuado de calidad y la mitigación proactiva de los riesgos en tiempo real.

El profesional se encontrará en estas páginas con una instrumentación técnica avanzada: indicadores de desempeño verificables (KPI), matrices de cumplimiento, taxonomías de riesgos y modelos de madurez ajustados a estándares internacionales. Cada capítulo ha sido diseñado con un rigor ingenieril que permite a auditoras y CIOs el poder de aplicar mecanismos de control medibles y replicables en las organizaciones.

En definitiva, este volumen pone de relieve que la madurez tecnológica no se decreta, se construye mediante la ingeniería de procesos y la evidencia empírica. Se trata de un tratado que no solo establece la codificación de la normativa, sino que operacionaliza su propósito dotando a las organizaciones de las herramientas necesarias para alcanzar la excelencia operativa y cimentar una gobernanza en tecnología de alto nivel.

ÍNDICE

PRÓLOGO ..... **i**
ÍNDICE……..... **iii**
INTRODUCCIÓN ..... **xi**
CAPÍTULO I **15**
1 INSTRUMENTOS DE EVALUACIÓN DEL SUBGRUPO 410
INTRODUCCIÓN **15**
1.1 Norma 410-01 02 organización de la unidad TI 16
1.2 Objetivo metodológico 16
1.3 Indicadores sugeridos 17
1.4 Evidencias obligatorias 18
1.5 Lista de verificación (checklist) 19
1.6 Matriz de cumplimiento 20
1.7 Riesgos por incumplimiento 21
1.8 Buenas prácticas 22
1.9 Norma 410-02 comité de tecnologías de la información y comunicaciones 23
1.9.1 Finalidad del instrumento 23
1.9.2 Indicadores 23
1.9.3 Documentos de soporte 24
1.9.4 Lista de verificación 25
1.9.5 Matriz de cumplimiento 25
1.9.6 Evidencias de funcionamiento del CTIC 26
1.9.7 Recomendaciones 27
1.10 Norma 410-03 segregación de funciones 27
1.10.1 MatrizRACIe incompatibilidades 28
1.10.2 Indicadores verificables 29

1.10.3 Evidencias requeridas 29
1.10.4 Checklistpor procesos 30
1.10.5 Hallazgosmás comunes 31
1.10.6 Acciones preventivas 31
1.11 Norma 410-04 planificación estratégica y operativa de TI 32
1.11.1 Indicadores deplanificación 33
1.11.2 EvidenciasdelPETIy POA-TI 33
1.11.3 Matriz dealineación institucional 34
1.11.4 Seguimiento y evaluación 34
1.11.5 Hallazgos frecuentes 34
1.12 Norma 410-05 políticas y procedimientos de TI 35
1.12.1 Lista de políticas mínimas requeridas 35
1.12.2 Indicadores verificables 36
1.12.3 Evidencias documentales 37
1.12.4 Calificación del nivel de madurez 37
1.12.5 Observaciones recurrentes 38
1.13 Norma 410-06 clasificación y arquitectura de la información 39
1.13.1 Indicadores de clasificación 39
1.13.2 Arquitectura institucional de datos 40
1.13.3 Instrumentos de documentación 40
1.13.4 Lista de verificación 40
1.13.5 Métodos de validación de integridad 41
1.13.6 Riesgos y controles sugeridos 41
1.14 Norma 410-07 administración de proyectos tecnológicos 43
1.14.1 Indicadores por fase del proyecto 43
1.14.2 Evidencias de gestión (actas, planes, entregables) 44

1.14.3 Matriz de riesgos del proyecto 45
1.14.4 Plantilla de seguimiento 46
1.14.5 Estándares y buenas prácticas 46
1.15 Norma 410-08 desarrollo, mantenimiento y adquisición de softwar 48
1.15.1 Matriz de controles por fase de desarrollo 48
1.15.2 Indicadores técnicos 50
1.15.3 Evidencias requeridas 51
1.15.4 Lista de verificación 51
1.15.5 Riesgos de desarrollos no controlados 52
1.15.6 Trazabilidad de cambios 52
1.16 Norma 410-09 adquisición de infraestructura tecnológica 53
1.16.1 Indicadores de adquisición 53
1.16.2 Evidencias y documentación soporte 54
1.16.3 Lista de verificación técnica 55
1.16.4 Estándares mínimos de equipos 56
1.16.5 Matriz de control de adquisiciones 56
1.17 Norma 410-10 mantenimiento y control de infraestructura tecnológica 58
1.17.1 Indicadores de mantenimiento 58
1.17.2 Registro técnico obligatorio 59
1.17.3 Matriz de seguimiento 59
1.17.4 Inventario tecnológico 61
1.17.5 Riesgos por falta de mantenimiento 62
1.18 Norma 410-11 seguridad de tecnologías de información 63
1.18.1 Indicadores de seguridad 63
1.18.2 Evidencias del SGSI institucional 64

1.18.3 Checklist de controles mínimos 65
1.18.4 Matriz de riesgos de seguridad 65
1.18.5 Auditoría interna de seguridad 67
1.19 Norma 410-12 contingencia y continuidad operativa 68
1.19.1 Indicadores de continuidad 68
1.19.2 Matriz de impacto al negocio 69
1.19.3 Plan de contingencias 71
1.19.4 Evidencias de pruebas y simulacros 71
1.19.5 Lista de verificación técnica 72
1.20 Norma 410-13 administración del soporte tecnológico 73
1.20.1 Indicadores del servicio 73
1.20.2 Gestión de tickets 74
1.20.3 Matriz de tiempos de respuesta 74
1.20.4 Evidencias del soporte 76
1.20.5 Evaluación del servicio 77
1.21 Norma 410-14 monitoreo y evaluación de servicios tecnológicos 77
1.21.1 Indicadores operativos 78
1.21.2 Modelo de monitoreo continuo 78
1.21.3 Evidencias de trazabilidad 79
1.21.4 Herramientas de monitoreo 79
1.21.5 Matriz de debilidades frecuentes 80
1.22 Norma 410-15 portal web, intranet y servicios telemáticos 82
1.22.1 Indicadores de gestión del portal 82
1.22.2 Estándares de accesibilidad 83
1.22.3 Evidencias obligatorias 84
1.22.4 Lista de verificación de contenido 85

1.22.5 Riesgos operativos 86
1.23 Norma 410-16 capacitación en tecnologías de la información……87
1.23.1 Indicadores de capacitación 88
1.23.2 Matriz de necesidades 88
1.23.3 Evidencias de capacitación 90
1.23.4 Evaluación de competencias digitales 91
1.23.5 Seguimiento del desarrollo del personal 91
1.24 Norma 410-17 firmas electrónicas en la administración pública……....92
1.24.1 Indicadores de uso 92
1.24.2 Evidencias de implementación 93
1.24.3 Lista de control 93
1.24.4 Verificación de certificados 94
1.24.5 Riesgos del uso incorrecto 95
CAPÍTULO II 99
2 ETAPA 3: EVALUACIÓN Y CALIFICACIÓN DEL CUMPLIMIENTO 99
2.1 Evaluación norma por norma 100
2.2 Tabla de cumplimiento general 101
2.3 Identificación de desviaciones 104
2.4 Priorización de debilidades 105
2.5 Validación técnica de hallazgos 106
CAPÍTULO III 107
3 ETAPA 4: IDENTIFICACIÓN Y CLASIFICACIÓN DE HALLAZGOS 107
3.1 Tipos de hallazgos 108

1. Riesgo inherente y residual: 110
3.2 Matriz "Hallazgo – Evidencia – Riesgo – Recomendación"……...112
3.3 Hallazgos transversales 113
3.4 Hallazgos específicos por norma 114
3.4.1 Dominio: Seguridad de la información (ISO/IEC 27001 & Ley 29733): 114
3.4.2 Dominio: Continuidad del negocio (ISO 22301) 116
3.4.3 Dominio: Gestión de servicios (ISO/IEC 20000) 118
CAPÍTULO IV 121
4 ETAPA 5: DISEÑO DEL PLAN DE MEJORAS 121
4.1 Criterios de priorización 122
4.2 Acciones correctivas 123
4.2.1 Eje tecnológico (infraestructura y software) 124
4.2.2 Eje de gobernanza (políticas y procesos) 126
4.2.3 Eje de capital humano (cultura y capacitación) 129
4.3 Cronograma y responsables 131
4.3.1 Fase 1: Saneamiento inmediato (0 - 3 meses): 131
4.3.2 Fase 2: Estandarización y formalización (3 - 12 meses):.. ……133
4.3.3 Fase 3: Optimización y transformación (12 - 24 meses):.. ……134
4.4 Matriz de seguimiento 136
4.4.1 Componentes de la matriz: 136
4.5 Indicadores de mejora continua 137
CAPÍTULO V 139

5 APLICACIÓN PRÁCTICA DE LA METODOLOGÍA (TRES CASOS DE ESTUDIO)..... 139
5.1 Caso 1: Institución educativa pública 140
5.1.1 Contextualización y diagnóstico inicial (el problema)..... 140
5.1.2 Aplicación metodológica (intervención)..... 141
5.1.3 Resultados y evidencia de mejora 141
5.2 Caso 2: Gobierno autónomo descentralizado..... 142
5.2.1 Contextualización y diagnóstico inicial (el problema)..... 142
5.2.2 Aplicación metodológica (intervención)..... 142
5.2.3 Resultados y evidencia de mejora 143
5.3 Caso 3: Agencia pública reguladora..... 143
5.3.1 Contextualización y diagnóstico inicial (el problema)..... 143
5.3.2 Aplicación metodológica (intervención)..... 144
5.3.3 Resultados y evidencia de mejora 144
5.3.4 Patrones de Hallazgos Comunes 145
5.3.5 Conclusión de la Validación..... 145
CAPÍTULO VI..... 147
6 RESULTADOS, IMPACTO Y NIVEL DE MADUREZ INSTITUCIONAL 147
6.1 Nivel de cumplimiento por norma 148
6.1.1 Evolución en seguridad de la información (ISO/IEC 27001)……...148
6.1.2 Evolución en continuidad del negocio (ISO 22301) 149
6.1.3 Evolución en gestión de servicios (ISO/IEC 20000 / ITIL)……151
6.2 Indicadores institucionales posteriores a la intervención..... 152
6.2.1 Indicadores de Eficiencia Operativa (KPIs Técnicos) 152

6.2.2 Indicadores de Percepción de Calidad (NPS y SERVQUAL)…….....154
6.2.3 Net Promoter Score (NPS) Tecnológico 155
6.2.4 Dimensión de tangibilidad 156
6.2.5 La Brecha de Talento Digital (Human Capital Gap)..... 157
6.2.6 La rigidez del sistema nacional de presupuesto 158
6.2.7 Silos de información y cultura organizacional..... 159
6.3 Lecciones aprendidas 159
CONCLUSIONES DEL TOMO II..... 161
GLOSARIO..... 163
BIBLIOGRAFÍA 172

INTRODUCCIÓN

La segunda parte de "*Gestión de Tecnologías de la Información: Una Perspectiva del Control Interno en el Sector Público*" representa la transición crítica desde la norma establecida en el volumen anterior hasta la ejecución y validación empírica; el primer convenció la norma del Subgrupo 410, pero el presente los procedimientos de control y de justificación en las TI como ejes centrales de los procedimientos de la administración pública.

Acorde con lo anterior, este volumen se configura a partir de una lógica de ingeniería de procesos, la lógica que permite proporcionar procedimientos estandarizados y métricas de evaluación y de control. Este trabajo presenta una metodología de trabajo integral, desde el diagnóstico hasta los planes de remediación y el impacto.

La parte técnica del texto presenta los instrumentos de evaluación del Subgrupo 410 mediante matrices de cumplimiento, los indicadores clave (KPIs) y las taxonomías de riesgos, alineando la gobernanza tecnológica de dentro del país con normas como ISO 27001, ISO 20000, ISO 22301, COBIT 2019 o PMBOK. Esta triangularización de normas permite al auditor y al gestor de TI justificar el nivel de madurez tecnológica, en referencia a las definiciones de cada punto del proceso de control.

Finalmente, la obra hace valer la teoría con tres casos de uso reales, validando la aplicabilidad del modelo en entornos muy complejos, con una ideación continua y de resiliencia operativa; y no se entiende como un mero texto de consulta sino como una herramienta obligada para justificar la transparencia, la eficiencia y el valor público desde la TI.

CAPÍTULO I

1 INSTRUMENTOS DE EVALUACIÓN DEL SUBGRUPO 410 INTRODUCCIÓN

La auditoría de Tecnologías de la Información (TI) dentro de las entidades de la administración pública ha ido consolidándose como un mecanismo fundamental para garantizar eficiencia, transparencia y cumplimiento normativo en la administración de recursos estatales. En el caso ecuatoriano, el Acuerdo N.º 004-CG-2023 de la Contraloría General del Estado, Normas de Control Interno (NCI), desarrolla la regulación de los instrumentos de Control Interno reconociendo la necesidad de adecuar el manejo de las tecnologías de la información con las metas institucionales (Contraloría General del Estado GCE, 2023) y estipulando que una auditoría de TI que resulte efectiva no solo genere la mitigación de los riesgos y la prevención del fraude, sino que establece un marco para que la gobernanza de TI gestione de una manera efectiva la verificación de que las inversiones en TI generen un valor público real (Calle García y otros, 2023).

El Subgrupo 410: Tecnología de la Información del Acuerdo impone las normas y requisitos más estrictos sobre la estructura, planificación y seguridad de los activos informáticos. En este caso, la evaluación de la organización de la unidad de TI no es solo la observación administrativa, sino que resulta del análisis de la segregación de las funciones y de la independencia operativa, elementos básicos para evitar conflictos de intereses y para garantizar un control interno robusto (DNV, 2017). El presente capítulo muestra los instrumentos metodológicos para auditar

la Norma 410-01, en su vertiente de proporcionar soporte técnico para validar el cumplimiento de la efectividad de dicha norma.

1.1 Norma 410-01 02 organización de la unidad TI

La primera norma del subgrupo de tecnologías de la información, la norma internacional ISO 38500, establece las bases sobre las que ha de operar la gestión tecnológica en el ámbito del sector público. Su evaluación no determina solamente la gestión administrativa, sino que ayuda a determinar que la tecnología opere como habilitador estratégico, bajo un marco de control potente y transparente.

1.2 Objetivo metodológico

El principal objetivo de la evaluación de la norma 410-01 es comprobar que la entidad fiscalizada tiene una estructura organizacional de TI formalmente constituida, lo que permite verificar la adecuada separación de funciones y la posición estratégica de la unidad, al tiempo que puede asesorar a la alta dirección. Según normativa, las actividades tecnológicas deben estar centralizadas en torno a una unidad que regula y estandariza los procesos, evitando que las actividades operativas deduzcan sus informes de conformidad con las actividades que pueden acabar evaluando. Esto es necesario para evitar que los departamentos operativos evalúen el trabajo que han ejecutado, o para que los mismos departamentos imponen criterios sin supervisión (Contraloría General del Estado GCE, 2023).

A partir de la buena práctica internacional, el auditor debe determinar que la estructura implementada propicia que la gobernanza de TI es el

marco en el que se asegura que la tecnología soporte las estrategias del negocio. Los auditores en este contexto deben definir si la unidad pertenece plenamente a la toma de decisiones institucionales, en la que se puede ejecutar cambios de mejora, tal como lo sugieren los principios de estándares como ISO/IEC 38500 van encaminados a propiciar el uso de TI de forma eficiente y aceptable a través de un sistema de dirección fuerte, claro y monitoreado (Business Beam s.f, 2019). La forma en la que se lleva a cabo la metodología de evaluación busca evidencias que vayan en la línea de que la unidad no es un simple ejecutante de soporte, sino un socio estratégico con autoridad.

1.3 Indicadores sugeridos

Con el objetivo de poder evaluar de una manera objetiva el cumplimiento de esta norma, se sugieren unos indicadores de gestión (los conocidos como KPIs, del inglés Key Performance Indicators) que están concebidos para que esta pueda ser evaluada cuantitativamente, esto es, en términos de la madurez organizativa o del alineamiento estratégico. Por tanto, gracias a esta propuesta de indicadores, el auditor podrá basarse menos en valoraciones subjetivas y más en determinados datos que parecen ser verificables sobre lo eficiente y lo transparente en el ámbito de la gestión pública (Checklist Fácil, 2023).

- **Índice de Independencia Estructural (IIE):** Este índice nos mide hasta qué nivel jerárquico tiene la unidad de TI (tecnología de la información).

Formula: $\frac{\text{Nivel Jerárquico de TI}}{\text{Nivel Jerárquico de áreas Usuarias Máximas}}\ x\ 100$

Interpretación: Un IIE superior o igual a 100 indica que TI reporta al mismo nivel que el área a la que sirve (por ejemplo: la dirección financiera), garantizando esta forma la autonomía (GCE, 2023).

- **Tasa de Segregación de Roles Críticos (TSRC):** Este índice mide la separación de los deberes incompatibles con los que mantiene la unidad de TI (por ejemplo: conciliación y procesamiento contable).

Formula: $\frac{\text{N\# de Roles con Conflictos de Segregación Identificados}}{\text{Total de Roles Evaluados}}\ x\ 100$

Meta: 0%. La norma establece que deben separarse funciones como desarrollo, operación y seguridad que prevengan el fraude y los errores descubribles (DNV, 2017).

- **Cobertura de Estructura Mínima (CEM):** Verifica la existencia de las funciones obligatorias.

Criterio: cumplimiento binario (1/0) sobre la existencia formal de cuatro funciones: 1) Proyectos, 2) Infraestructura, 3) Soporte, 4) Seguridad de la Información (GCE, 2023).

1.4 Evidencias obligatorias

La prueba del cumplimiento de la norma necesita que el auditor verifique la existencia de documentación específica que pruebe la implantación de los controles. La evidencia tiene que ser suficiente, competente y pertinente en el sentido de que la estructura no solo existe

en papel, sino que funciona tal como se describe en el acuerdo 004-CG-2023 (GCE, 2023).

El auditor debe obligatorio pedir:

- **Estatuto orgánico o manual de funciones aprobado:** Donde se visualice la unidad de TI en un nivel asesor o de apoyo directivo, separado de las unidades usuarias.
- **Actas de comité de dirección:** Que verifiquen la participación del responsable de TI en decisiones estratégicas de la entidad.
- **Manual de perfiles de puesto:** Que describa y confirme la existencia de funciones separadas, donde no existan roles que combinen, por ejemplo, programación de software con administración de bases de datos en producción.
- **Designación del oficial de seguridad de la información (CISO):** Es el acto administrativo donde se nombre al responsable de seguridad y, además, que queda explícito que su independencia jerárquica respecto de la jefatura de TI es prueba del "control por oposición" (EY Switzerland, 2025).

1.5 Lista de verificación (checklist)

En esta sección se detallan los puntos de control críticos a validar por parte del auditor, de tal modo que proceda a comprobar el cumplimiento de la norma.

- El primer punto de control consiste en comprobar que la unidad de TI tenga un nivel jerárquico suficiente para asesorar a la alta dirección que a la vez se contrasta con el organigrama institucional

vigente a fin de comprobar que el responsable de TI se encuentre en relación de jerarquía directa con la máxima autoridad (GCE, 2023).

- El segundo punto de control implica validar la independencia funcional de la unidad de TI respecto de las áreas usuarias. En este caso, el auditor debe comprobar que la unidad de TI no esté subordinada a las áreas del Financiero o del Administrativo ya que afectaría el control y la estrategia (GCE, 2023).
- El tercer aspecto por revisar sería la estructura interna que revisaría la existencia de las áreas Proyectos, Infraestructura, Soporte y Seguridad explícitamente. Se aporta verosimilitud mediante la distribución de recursos humanos y la asignación efectiva de los roles (GCE, 2023).
- Finalmente, es importante validar la posición y la designación del Oficial de Seguridad de la Información: el auditor debe verificar que exista el rol y que sea independiente de la Jefatura de TI, garantizando así la eficacia del esquema de control por oposición (EY Switzerland, 2025).

1.6 Matriz de cumplimiento

A fin de evaluar la madurez en la implementación de la norma, se describen los distintos niveles de desarrollo que puede mostrar la entidad:

- En la madurez en desarrollo o "Definido" la entidad cuenta con la unidad de TI oficialmente reconocida y con políticas aprobadas.

En este momento, la unidad tiene la potestad para regular elementos tecnológicos, aunque tiene un poder de regulación limitado de no verificar el cumplimiento en todas las áreas (CGE, 2023).

- El nivel intermedio o "Gestionado" se alcanza cuando la unidad de TI participa activamente en la planificación estratégica de la institución. La tecnología deja de verse únicamente como soporte, transformándose en un socio del negocio y existen métricas al respecto alineadas con los objetivos organizacionales (Business Beam s.f, 2019).

- El nivel óptimo o "Optimizado" se caracteriza por una independencia absoluta en la función de seguridad. En este nivel, el Oficial de Seguridad de la Información (CISO) informa directamente a la Máxima Autoridad o lo hace ante un Comité de Riesgos, y existen auditorías de seguridad continuas y automatizadas. Este nivel supone el cumplimiento más elevado de la norma, en el cual el control interno forma parte de la cultura organizacional (EY Switzerland, 2025).

1.7 Riesgos por incumplimiento

Al no observar las directrices de la Norma 410-01, se presentan a la entidad riesgos estratégicos y operacionales acentuados. Ciertamente, el mayor riesgo se presenta a raíz del conflicto de interés en la gestión de la seguridad, ya que, si el oficial de seguridad no es independiente, la probabilidad de ocultar la vulnerabilidad y el incidente es alta a fin de

no atenerse a la sanción, lo cual pone en riesgo la integridad de la información pública (EY Switzerland, 2025).

La inobservancia de una adecuada segregación de funciones dentro de la unidad de TI también conlleva al riesgo del fraude interno. Si el personal tiene exceso de permisos que combinan desarrollo y operación con la posibilidad de no ser supervisados, entonces la manipulación de datos y activos financieros se hace simple (DNV, 2017). Así mismo, la baja jerarquía de la unidad de TI suele llevar a obsolescencia tecnológica, ya que la inversión realizada no acompaña una visión estratégica de la entidad ni la necesaria a partir de la ciudadanía (Calle García y otros, 2023).

1.8 Buenas prácticas

Para garantizar la adecuada observancia de esta norma, se recomienda observar marcos de referencia de tipo internacional como lo son COBIT 2019 o ISO/IEC 38500. Una buena práctica es la creación de un Comité de Estrategia de TI que contenga miembros de alta dirección, de forma tal que la estructura organizacional adapte la evolución de la misma conforme a los riesgos y retos del mundo digital (CIO Index s.f, 2025).

En cuanto al tema de la seguridad se recomienda seguir el modelo de las "Tres Líneas de Defensa", en el cual se debe colocar al Oficial de Seguridad en la segunda línea, ya que él podrá cuestionar y auditar las prácticas operativas de la primera línea (unidad de TI) al mismo tiempo que pertenece al Comité de Auditoría. Esta manera de posicionarse es como se considera en el modelo de la norma la mejor manera de

gobernar la seguridad para así evitar los conflictos de interés (EY Switzerland, 2025).

1.9 Norma 410-02 comité de tecnologías de la información y comunicaciones

El contenido de esta norma describe un mecanismo de gobernanza colegiada, cuyo objetivo es que las decisiones tecnológicas tomadas en la institución no se realicen de manera aislada, sino que se produce un proceso de consenso de estas a partir de la estrategia institucional.

1.9.1 Finalidad del instrumento

El objetivo de auditar la Norma 410-02 acabo de exponerlo. El propósito auditado sería verificar la existencia real y operativa de una entidad de gobierno (Comité de TI) responsable de la aprobación y priorización de inversiones y proyectos tecnológicos. La responsabilidad del mismo no es de tipo técnica-operativa, sino que debe ser de carácter estratégico por cuanto debe garantizar que la iniciativa de TI se encuentra alineada a un objetivo del negocio, generando valor público, tal y como se puede apuntar desde la evaluación realizada por última vez. La evaluación auditada tendría por finalidad confirmar que dicho comité actúa como un filtro de alineación estratégica, no dejando opción a la "informática oculta" o a la adquisición no planificada (Contraloría General del Estado GCE, 2023).

1.9.2 Indicadores

Los indicadores que se proponen para tener constancia de la eficacia de este órgano de dirección son:

- **Índice de Ejecución de Resoluciones (IER):** Porcentaje de acuerdos del comité, con relación a aquellos que se han ejecutado en el plazo dispuesto. Si el porcentaje es bajo el comité pierde su autoridad real, pasando a ser considerado sólo "de papel".
- **Frecuencia de Sesiones (FS):** Total de sesiones ordinarias realizadas en relación con las que existían planificadas al año. La inactividad es uno de los hallazgos de auditoría en este control

- **Nivel de Asistencia de Alta Gerencia (NAAG):** Porcentaje de asistencia de la Máxima Autoridad (o su delegado oficial) en las sesiones. Si existe ausencia de los responsables, se diluye el poder de decisión del comité (CGE, 2023).

1.9.3 Documentos de soporte

El auditor deberá solicitar acceso irrestricto a los siguientes documentos para tener evidencia de la conformación del cumplimiento:

- **Acto administrativo de conformación:** Resolución o Acuerdo firmado por la Alta Autoridad cuya firma les da existencia a los miembros del comité y aquellos que son permanentes (talento humano, planificación, jurídica, TI, etc).
- **Reglamento de funcionamiento del comité:** Documento que norma con respecto a la periodicidad de reuniones, quórum y procedimiento para toma de decisiones (por unanimidad, consenso, etc.)

- **Actas de sesiones (cronológico):** Registro oficial de las temáticas tratadas, discusión en la que queda reflejado el resultado de las resoluciones numeradas y firmadas por todos los asistentes.
- **Plan estratégico de TI (PETI) aprobado:** Evidencia física de que el PETI ha sido revisado y aprobado formalmente en una sesión de este comité (Arcotel, 2023).

1.9.4 Lista de verificación

Se evalúa el control a través de los siguientes verificadores de puntos críticos:

- ¿Hay resolución formal de creación del Comité de TI vigente y socializada?
- ¿El comité está presidido por la Máxima Autoridad o siendo delegada con poder de decisión financiero y administrativo?
- ¿El comité se integra por la persona responsable de Planificación, Jurídica y Talento Humano, ¿además de la persona responsable de TI?
- ¿Se reúnen siguiendo la frecuencia establecida en el reglamento interno?
- ¿Existen actas firmadas que evidencien la aprobación del Plan Operativo Anual de TI y del presupuesto tecnológico?
- ¿El Comité monitorea el avance de los proyectos de TI y toman acciones correctivas cuando hay desviaciones?

1.9.5 Matriz de cumplimiento

El nivel de madurez del Comité de TI se clasifica de acuerdo con la documentación hallada en los siguientes niveles:

- **Nivel 0 (inexistente):** No existe un comité constituido. Las decisiones son administradas de forma unilateral por el director de TI o la responsabilidad financiera.
- **Nivel 1 (inicial):** Existe un comité designado de forma administrativa pero no se reúne o no deja documentación (actas) de decisiones de este.
- **Nivel 3 (definido):** El comité se reúne y tiene un reglamento operativo y formaliza la aprobación del plan de TI. Existe representación de todas las áreas claves.
- **Nivel 5 (optimizado):** El comité utiliza tableros de control (dashboards) para monitorizar los riesgos y los beneficios en tiempo real. Sus decisiones conducen a la innovación y a la transformación digital institucional de forma proactiva (Auditool, 2025).

1.9.6 Evidencias de funcionamiento del CTIC

No es suficiente con tener el acta de constitución; la operatividad se demuestra a través de:

- **Convocatorias formales:** Correos u oficios con convocatoria a sesión y un claro orden del día.
- **Matriz de seguimiento de acuerdos:** Herramienta visual donde se muestre el estado (Abierto, En Proceso, Cerrado) de cada resolución acordada en sesiones anteriores.

- **Informes de gestión presentados al comité:** Presentaciones o informes ejecutivos que el área de TI comparte con los miembros para justificar el gasto o para informar del progreso.

1.9.7 Recomendaciones

Para liberar la gobernanza tecnológica a través del comité se sugieren:

- **Formalizar el estatuto:** Se sugiere poder asegurar que el reglamento interno del comité presente claramente la responsabilidad de cada miembro, evitando que las personas asistentes se conviertan en delegados sin voz ni voto.
- **Integrar la gestión de riesgos:** Incorporar como un punto fijo el riesgo de ciberseguridad y continuidad de negocio que se revisa de forma sistemática en el orden del día y no solamente la compra de los equipos.
- **Una secretaría técnica fuerte:** Para poder conseguir que el director de TI esté como secretario técnico (probablemente con voz pero sin voto) que asegure las actas y que la documentación técnica sea precisa y que sea tratada como el Ministerio del Trabajo da poder custodiarla para su finalización correcta (Ministerio del Trabajo, 2024).

1.10 Norma 410-03 segregación de funciones

La segregación de funciones (SoD por sus siglas en inglés) es uno de los conceptos más relevantes en relación con el control interno que pretende evitar fraudes y errores mediante la separación de tareas críticas entre las diferentes personas que forman parte de la organización. La Norma

410-03 impone a las organizaciones la obligación de contar con funciones de los usuarios y del personal de tecnología de la información (TI) bien definidas y comunicadas, de modo que nadie pueda tener el control absoluto de una transacción de forma continua (es decir, desde que empieza hasta que finaliza). La literatura académica asegura que una clara y adecuada separación de funciones disminuye considerablemente el riesgo de que las personas se apropien de los datos u otras personas sean las responsables de la detección de las acciones que no deberían ser ejecutadas a través de los sistemas de información (Whittington & Pany, 2005).

1.10.1 Matriz RACI e incompatibilidades

Para auditar el grado de cumplimiento de esta norma hay que estudiar la distribución de las funciones utilizando una estructura lógica, que puede ser representada generalmente a través de la matriz RACI (responsable, Aprobador, Consultado e Informado).Dentro del marco de la norma 410-03, el auditor debe comprobar que los papeles de "Ejecución" y "Autorización" no pueden recaer en la misma persona. Un ejemplo podría ser que realizar un código de software (la persona responsable de ejecución) no podrá ser el mismo que quien aprueba su paso a producción (Aprobador), dejando a la vista un claro conflicto de interés directo y comprometiendo la integridad del sistema. Las incompatibilidades más importantes que deben identificarse son la combinación de las funciones de administración de seguridad y operación de los sistemas, o permitir que el programador acceda y modifique datos reales en producción. La norma es muy clara e indica que deben evitarse las funciones incompatibles y facilitar el cambio

periódico de las personas en las áreas implicadas en los procesos críticos con la intención de reducir la dependencia de personas claves y de disminuir la oportunidad de ocultar irregularidades que se perpetúan en el tiempo.

1.10.2 Indicadores verificables

La efectividad de la segregación de funciones puede medirse mediante la definición de un determinado indicador. Un primer indicador puede ser el Percentil de Conflictos por Segregación de Funciones (PCSF), el porcentaje de usuarios que tienen permisos tóxicos (combinaciones de accesos incompatibles) respecto del total de usuarios del sistema. En este indicador, un valor distinto de cero debe ser justificado con documentación adicional y controles compensatorios a corto plazo (ISACA, 2019).

Un segundo indicador, también interesante para valorar la efectividad del control de la segregación de funciones es la Tasa de Rotación en Puestos Críticos (TRPC), indicador que muestra la frecuencia con la que cambian los responsables de tareas críticas como la administración de bases de datos o la gestión de claves criptográficas, tal y como realiza la norma a manera de control preventivo; de no existir rotación en un largo periodo de tiempo puede corresponder a un estancamiento que favorezca la ocultación de errores o fraudes operativos.

1.10.3 Evidencias requeridas

Con el fin de dar sustento al cumplimiento, el auditor deberá recabar documentos formales aprobados. La evidencia básica es: el Manual de

Descripción de Puestos, el cual deberá concretar la descripción de las competencias y responsabilidades que se asignen a cada puesto de trabajo en tal sentido se velará por que no existan traslapes teóricos de funciones incompatibles y, además que dichos documentos estén actualizados y firmados por la unidad de Talento Humano y jefatura de TI.

Adicionalmente, se requiere la Matriz de Accesos y Privilegios que debe ser obtenida directamente de los sistemas, que evidencie que los permisos administrados en la práctica se ajustan a los roles definidos en el papel. También se pedirán los reportes de auditoría interna o externa anteriores en los cuales se da cuenta de la revisión periódica de dichos accesos, por otro lado, se tendrán que solicitar las bitácoras que reflejan la supervisión de las actividades realizadas por usuarios con privilegios elevados.

1.10.4 Checklist por procesos

La verificación de este control se realizará a través de un conjunto de comprobaciones secuenciales. En primer lugar, es necesario corroborar si las funciones de arranque, aprobación, registro y revisión de las transacciones están delegadas en personas diferentes. En segundo lugar, es preciso comprobar que el personal de desarrollo de software no tenga acceso de escritura o modificación en el entorno de producción, una de las desviaciones más graves y comunes de la separación de funciones.

A continuación, es preciso constatar la existencia de un proceso formal de revisión periódica de derechos de acceso, que asegure que los permisos se revoquen o ajusten cuando un funcionario cambia de puesto

o bien cuando el funcionario abandona la entidad. Finalmente, hay que comprobar si existen controles compensatorios (por ejemplo, un control intensivo de logs) en aquellas situaciones demás que, por limitaciones en el número de personas, no permita establecer de forma adecuada la separación de funciones

1.10.5 Hallazgos más comunes

En las auditorías que se ejecutan al sector público se constatan los casos en los cuales el personal de soporte técnico accede a credenciales de nivel de "administrador" ("superuser"), quedando habilitado para cambiar información de una forma que no deja un rastro auditoria claro, justificándolo mediante el concepto de "agilidad operativa". Este hallazgo incumple sin duda estrictamente con la exigencia de definir los roles y responsabilidades claramente, de manera que se cuente con suficiente autoridad y respaldo.

Otro hallazgo recurrente es la obsolescencia de los manuales de funciones y donde las responsabilidades que se han infectado no son coincidentes con las actividades que ejecuta el personal. En la realidad muchas veces se determina una dependencia de personal clave ("búsquedas de héroes"), donde una persona centraliza el conocimiento y los accesos de forma crítica sin la documentación ni procedimientos que permitan la instauración y/o supervisión, violando de esta forma la cláusula de "no depender del personal clave".

1.10.6 Acciones preventivas

Para mitigar los riesgos expuestos se debe cuando menos hacer aparecer un sistema de Gestión de Identidades y Accesos (IAM) basado en roles (RBAC) que haga la asignación de permisos en función del perfil del puesto y donde por defecto aparezcan denegados los accesos incompatibles. Dicho esto, se debe tener como un objetivo automatizado del principio por el cual sólo se debe conseguir el mínimo privilegio en donde las personas obtengan sólo los accesos necesarios para poder realizar sus funciones.

Finalmente, es imprescindible establecer un calendario anual de revisión de accesos que se encuentre validado por los dueños de los procesos de negocio y no solamente por TI. La formación continua acerca de la importancia de la Seguridad y la ética del manejo de la información es también una barrera preventiva, en cuanto se favorece una cultura de control donde los mismos funcionarios comprenden y respetan los límites de sus atribuciones.

1.11 Norma 410-04 planificación estratégica y operativa de TI

La Norma 410-04 manifiesta que la gestión de las TI debe ser planificada, es decir, no es una mera respuesta a contingencias; Más aún, la unidad de TI tiene la obligación de formular e implementar un Plan Estratégico de Tecnologías de la Información (PETI) que cumpla con una serie de prescripciones, ya establecidas en el Plan Estratégico Institucional y con planos del Plan Nacional de Desarrollo. Detalles que el cuerpo de estudios publicado en TI Governance ha puesto de manifiesto, quedando plasmado, ya que indica que la alineación estratégica es el componente que facilita en mayor medida el que las TI

generen valor público, dado que es la responsable de ganar la obligación de un gasto surgido de un centro de costes a un socio estratégico (Weill & Ross, 2005).

1.11.1 Indicadores de planificación

La planificación, autocomunicada por el área de TI, se mide por la ejecución de indicadores que miden el cumplimiento y la gestión financiera. El Índice de Ejecución del PETI mide la cantidad de proyectos tecnológicos ejecutados con respecto a los programados, permitiendo determinar el grado de ejecución real de la estrategia. La Desviación Presupuestaria de TI también compara la asignación de recursos en el Plan Operativo Anual (POA) con los recursos realmente ejecutados; desviaciones significativas que no cuenten con respaldos técnicos que las justifiquen sugieren deficiencias en el proceso de estimación de costos, las cuales además contravienen el imperativo de contar con la correspondiente aprobación presupuestaria por parte del máximo responsable de la entidad.

1.11.2 Evidencias del PETI y POA-TI

El principal documento de la auditoría es el Plan Estratégico de TI (PETI), que, debiendo estar legalizado, además obligatoriamente debe contener el análisis de la situación actual, las propuestas de mejora, el análisis de los riesgos y el cronograma de inversiones presentado en los POA. De forma complementaria, hay que auditar los Planes Operativos Anuales (POA), los cuales presentan el portafolio de proyectos y servicios concretos para el ejercicio fiscal, incluyéndose las estrategias para evitar el envejecimiento tecnológico.

1.11.3 Matriz de alineación institucional

La auditoría debería también determinar la trazabilidad entre objetivos tecnológicos y objetivos misionales. Se verifica que cada proyecto recogido en el PETI exhiba una justificación de los objetivos estratégicos de la organización, que TI colaboró con la misión institucional. De igual forma, el análisis debería verificar que la planificación tecnológica considera partícipes a las políticas públicas de los gobiernos y el Plan Nacional de Desarrollo, entrelazando la gestión institucional en el marco macro situacional.

1.11.4 Seguimiento y evaluación

La normativa establece que ni los planes estratégicos ni los operativos pueden considerarse documentos estáticos, sino que deben ser objeto de seguimiento, evaluación y actualización con periodicidad. El auditor debería buscar informes de gestión entregados a la alta dirección que dan cuenta del grado de ejecución y las medidas correctivas llevadas a cabo en un caso de desviaciones. La literatura académica sobre COBIT 2019 refuerza que la evaluación continua del desempeño es una práctica fundamental para readaptar las estrategias mediante cambios de entorno tecnológico o normativo (ISACA, 2019).

1.11.5 Hallazgos frecuentes

Un hallazgo habitual son adquisiciones de hardware o software que no se encuentran en el plan estratégico aprobado, situación no permitida salvo en casos de emergencia con autorización previa. También se detectan planes estratégicos desactualizados, que no reflejan la realidad

operativa de la entidad, que no contienen un análisis de riesgos, convirtiéndose en documentos de cumplimiento formal sin utilidad alguna para la toma de decisiones.

1.12 Norma 410-05 políticas y procedimientos de TI

La Norma 410-05 recoge el marco regulador interno que rige el modo de obrar y gestionar la tecnología en el seno de la organización. Esta norma obliga a la unidad de TI a no regirse por criterios discrecionales, sino a fijar, documentar y dar a conocer indicaciones y procedimientos normalizados a los cuales debe dar consentimiento la autoridad máxima. La normativa especializada entiende a las políticas de seguridad como la expresión formal de las reglas que han de seguir las personas que acceden a la tecnología y a la información de la organización y que constituyen la base legal y administrativa para cualquier acción de control o sanción (Whitman & Mattord, 2021).

1.12.1 Lista de políticas mínimas requeridas

Para dar cumplimiento a esta norma, la entidad tiene que disponer de un cuerpo documental que contemple los dominios críticos de la gestión de TI. Conforme al Acuerdo 004-CG-2023, las políticas mínimas de obligado cumplimiento son: gestión de inventario tanto de hardware como de software, clasificación de la información, generación de respaldos (backups) y pruebas de recuperación, así como la gestión de incidentes y de continuidad de operaciones. Este conjunto de normas siempre ha sido contemporáneo a los controles, como se evidencia en el anexo A de la norma ISO/IEC 27001, en virtud de la cual, como respuesta a esta cuestión, se estructura la seguridad en dominios

prácticamente idénticos para alcanzar la finalidad de asegurar la confidencialidad, la integridad y la disponibilidad (International Organization for Standardization ISO, 2022).

Además, la norma ISO/IEC 270017241 demanda específicamente la existencia de procedimientos para el control de acceso lógico (altas, bajas y modificaciones de los usuarios), protección frente a la llegada de software malicioso, logging (registro) de logs de auditoría y gestión de cambios en la configuración. A su vez, en el actual momento, se ha hecho también necesario incluir también políticas sobre teletrabajo, sobre seguridad en dispositivos móviles y sobre la gestión de servicios en la nube, de modo que el marco normativo institucional sea capaz de adaptarse a la velocidad de las nuevas modalidades de trabajo o de amenazas cibernéticas (Contraloría General del Estado GCE, 2023).

1.12.2 Indicadores verificables

La eficacia de las políticas se puede medir de la vigencia de éstas y su penetración en la cultura organizativa. Un indicador clave lo constituye la Tasa de Actualización Recordada, que calcula el porcentaje de políticas en la organización que han sido revisadas y aprobadas en los últimos 12 meses frente al total de políticas existentes. Las políticas obsoletas representan un peligro latente, en tanto que éstas pueden prescribir controles para tecnologías que la organización ya no está usando o ignorar nuevas vulnerabilidades (ISACA, 2019).

Un segundo indicador de relevancia es el Nivel de Difusión y Aceptación, obtenido como porcentaje de empleados que han firmado formalmente (en físico o digitalmente) la aceptación de las políticas de

seguridad de la información. Este indicador es fundamental desde una perspectiva jurídica, puesto que una política no comunicada es inaplicable administrativamente. Un escaso nivel de aceptación propone que las normas son "letra muerta" y que no están involucradas en la rutina cotidiana de la institución (Peltier, 2026).

1.12.3 Evidencias documentales

El auditor debe solicitar el Manual de Políticas y Procedimientos en TI en vigor, comprobando que cada uno de sus documentos tenga la firma de la máxima autoridad o del Comité de TI, como exige la normativa de control interno (CGE, 2023). No es suficiente con presentar borradores o cualquier documentación en trámite de revisión, la evidencia debe mostrar que la norma es oficial y de cumplimiento obligatorio.

Adicionalmente al manual, es probable que se presente la evidencia socializadora, para la cual se podrá recurrir a los registros de asistencia a capacitaciones, los correos masivos de difusión, las capturas de pantalla de la intranet donde se socializan las normas, etc.; resulta necesario auditar los registros de operación que evidencien el cumplimiento del procedimiento, tales como los formularios de solicitud de accesos firmados, las bitácoras de incidentes y los reportes de inventario que se encuentren actualizados, cotejando lo que dice el papel con lo que se está haciendo (CGE, 2023).

1.12.4 Calificación del nivel de madurez

La calificación del nivel de madurez que tiene la gestión de las políticas irá aumentando poco a poco. En un nivel Inicial, las políticas forman

parte del funcionamiento informal o ad hoc, sin ser aprobadas, y son conocidas únicamente por el personal técnico.

Un nivel Definido implica que las políticas son documentadas, aprobadas y estandarizadas, cumpliendo con los mínimos establecidos por la CGE aunque sean revisadas de forma reactiva. Para alcanzar el nivel Optimizado, se establece un ciclo de mejora continua para la revisión de las políticas y se automatiza su cumplimiento mediante herramientas tecnológicas (ejemplo: políticas de contraseñas forzadas por el directorio activo o bloqueo de puertos USB por software). En este nivel, las políticas se adecuan de forma dinámica a los objetivos de negocio y a estándares internacionales, como pueden ser la ISO 27001 o el estándar NIST (ISO, 2022).

1.12.5 Observaciones recurrentes

Una observación habitual de las auditorías es la existencia de políticas que son copias literales de plantillas que se encuentran en Internet o de otras instituciones, incorporando cargos o tecnologías que no están presentes en la entidad auditada, lo que denota un escaso análisis y adaptación a la realidad institucional convirtiendo el cumplimiento en un mero ritual burocrático sin valor de control real (CGE, 2023).

Otro hallazgo habitual es la falta de consistencia entre la política y la configuración técnica: por ejemplo, la política documental establece el requerimiento de contraseñas de 12 caracteres que deben rotar cada 90 días, a la vez que el sistema permite claves de 4 caracteres que no caducan; esta disparidad entre la norma escrita y la configuración del

sistema evidencian la falta de supervisión y ejecución de los procedimientos establecidos (Whitman & Mattord, 2021).

1.13 Norma 410-06 clasificación y arquitectura de la información

Para gestionar adecuadamente la información es necesario un esquema de gobierno donde garantizar la disponibilidad, la integridad y la confidencialidad de los datos a partir de la forma en que la información es clasificada y además de contar con políticas de clasificación (DAMA International, 2017).

1.13.1 Indicadores de clasificación

Los indicadores de clasificación permiten clasificar la información a partir de su valor legal, de su nivel de sensibilidad y de su criticidad para la organización. Tal como indica la norma ISO/IEC 27001, los datos de información tienen que ser clasificados o etiquetados para garantizar que reciban el nivel de protección correspondiente (International Organization for Standardization ISO, 2022).

- **Niveles de clasificación:** Se suelen aplicar estructuras típicas de clasificación jerárquicas; son utilizados los niveles de neutral, uso interno, confidencial y secreto (Whitman & Mattord, 2021).
- **Etiquetado:** El etiquetado (labeling) como control físico o lógico que vincula los atributos de seguridad con el objeto de datos, permite el manejo automatizado de la información (Stallings & Brown, Computer Security: Principles and Practice, 2018).

1.13.2 Arquitectura institucional de datos

La arquitectura de datos describe los modelos, las reglas y los estándares responsables de definir qué datos se recogen y cómo se almacenan, integran y utilizan en la institución (Laudon & Traver, 2021).

- Modelado de datos que se presenta en tres niveles de abstracción:
- **Modelo conceptual:** Representación de nivel alto de las entidades de negocio y sus relaciones.
- **Modelo lógico:** Una descripción de los atributos de las entidades que no incluye la tecnología.
- **Modelo físico:** Traduce el diseño lógico a un sistema de gestión de bases de datos concreto (DAMA International, 2017).

1.13.3 Instrumentos de documentación

La documentación técnica es clave para la continuidad del sistema y la auditoría. ISACA (2019) manifiesta que la no existencia de una documentación actualizada es una vulnerabilidad una debilidad que tiene lugar en la gobernanza TI.

- **Diccionario de datos:** Repositorio centralizado que contiene metadatos sobre la característica de los datos, así como el formato, definición y uso (Connolly & Begg, 2015).
- **Inventario de activos:** Es una lista que identifica al propietario (*Data Owner*) y su localización física o lógica de la información (ISO, 2022).

1.13.4 Lista de verificación

Las listas de verificación son herramientas de control interno que se utilizan para garantizar el cumplimiento de los procedimientos de seguridad y arquitectura antes de la puesta en producción de los sistemas.

- **Aplicación:** Según el Instituto Nacional de Estándares y Tecnología (NIST), estas listas de verificación deben contemplar las configuraciones de seguridad, parches aplicados y validación de privilegios de usuario de acuerdo con Souppaya & Scarfone, (2018).
- **Elementos clave:** Verificaciones de backups, confirmar propietarios de datos y testeos de recuperación ante desastres.

1.13.5 Métodos de validación de integridad

La integridad presenta la información no ha sido modificada de forma no autorizada, y los métodos criptográficos son el estándar para este tipo de validaciones.

- **Funciones hash:** Algoritmos matemáticos (sha-256), que producen una cadena de caracteres única para un archivo, y con cualquier cambio que se produzca con el archivo, el hash resultante resulta profundamente alterado (Stallings, 2017).
- **Sumas de verificación (checksums):** Técnicas utilizadas para detectar errores introducidos ya sea en la transmisión o almacenamiento de datos (Tanenbaum & Wetherall, 2011).

1.13.6 Riesgos y controles sugeridos

La gestión de riesgos es la práctica que consiste en identificar posibles amenazas existentes a los activos de información e implantar controles que minimicen los riesgos a un nivel aceptable.

La Tabla 1 de "Riesgos identificados y su control sugerido" representa de manera precisa los principales riesgos que se derivan de la gestión de la información en entornos tecnológicos y al mismo tiempo informa de los controles que se sugieren desde el propio NIST (2020) para su control, de manera que sirve para orientar e informar de una manera comparativa y natural a fin de aumentar la identificación de las amenazas más importantes y la selección de mecanismos de protección y gestión que sean adecuados para garantizar la seguridad de los vínculos de interés para los activos de la información.

Tabla 1. Riesgos identificados y su control sugerido

Riesgo identificado	**Control sugerido (NIST, 2020)**
Fuga de datos (Data Leakage)	Implementación de sistemas DLP (*Data Loss Prevention*) y cifrado de datos en reposo y tránsito.
Acceso no autorizado	Principio de menor privilegio y autenticación multifactor (MFA).
Inconsistencia de datos	Reglas de integridad referencial en bases de datos y validación de entrada.

Fuente: NIST, (2020)

Nota: Riesgos identificados y su control sugerido

La Tabla 1, pone de relieve una relación directa que existe entre los riesgos que resultan ser más relevantes e importantes para la gestión de la información y los controles que se sugieren desde el NIST (2020), lo que pone de manifiesto una propuesta completa que busca dotar de mayor seguridad a la organización. La fuga de información queda controlada mediante DLP y cifrado, lo cual permite aumentar la confidencialidad; el acceso no autorizado queda parcialmente controlado aplicando el principio del mínimo privilegio y la autenticación multifactor, combinación que permite disminuir considerablemente la posibilidad de intrusiones; y la inconsistencia de los datos queda minimizada mediante reglas de integridad referencial y validaciones de entrada que permiten asegurar la calidad y la coherencia de la información. En definitiva, los controles que se proponen permiten gestionar los riesgos de forma correcta gracias a que se alinean con buenas prácticas internacionales y que aportan estabilidad y resiliencia a los sistemas de información.

1.14 Norma 410-07 administración de proyectos tecnológicos

La gestión de los proyectos de TI consiste en la aplicación de un conjunto de conocimientos, habilidades, herramientas y técnicas a las actividades del proyecto con el objetivo de cumplir sus requisitos. En el marco de la auditoría se desea que el proyecto cumpla con los requisitos de ámbito, tiempo, costes y calidad (Project Management Institute, 2021).

1.14.1 Indicadores por fase del proyecto

Los KPIs permiten comprobar la salud del proyecto. Según Kerzner (2022), no deben ser medidos exclusivamente al término del proyecto sino también a la finalización de cada fase de ciclo de vida.

Fase de inicio y planificación:

- Varianza de estimación de costos: Diferencia entre el presupuesto apropiado y el presupuesto base aprobado.
- Calidad de los requisitos: Proporción de requisitos que han sido verificados y aprobados por los interesados antes del desarrollo (Schwalbe, 2019).

Fase de ejecución y monitoreo (Gestión del Valor Ganado - EVM):

- SPI (Schedule Performance Index): Para cuantificar la eficiencia del cronograma. Un SPI < 1.0 provoca retraso.
- CPI (Cost Performance Index): Para evaluar la eficiencia del coste. Un CPI < 1.0 modifica la sobrecarga.

Fase de cierre:

- **Satisfacción del cliente/usuario:** Medida mediante encuestas tras la implementación.
- **Deuda técnica acumulada:** Cantidad trabajo necesario para hacer sobre la re-factoring aplazado debido a la entrega (Fowler, 2019).

1.14.2 Evidencias de gestión (actas, planes, entregables)

En una auditoría, "lo que no está escrito, no puede darse". La documentación proporciona la trazabilidad de las decisiones llevadas a cabo.

- **Acta de constitución (Project Charter):** Documento que da por formalmente autorizado el proyecto entregando el proyecto a la persona que le dirige (PMI, 2021).

- **EDT/WBS (Estructura de Desglose del Trabajo):** Descomposición del alcance total del trabajo en un esquema jerárquico.
- **Actas de Reunión (Meeting Minutes):** Registro de discusiones, decisiones y asignación de tareas. Son pruebas en el ámbito judicial de cada una de las disputas contractuales.
- **Actas de Aceptación de Usuario (UAT Sign-off):** Acta firmada en la que el usuario final acredita que el sistema cumple con lo requerido en la especificación de requisitos funcionales (Heldman, 2021).

1.14.3 Matriz de riesgos del proyecto

El proceso de gestión de riesgos es proactivo, no reactivo. Es una herramienta gráfica que clasifica los riesgos según su probabilidad e impacto.

- **Estructura:** Normalmente es una matriz de 5x5 (Probabilidad vs. Impacto)
- **Cálculo:** $\text{Riesgo} = \text{Probabilidad x Impacto}$

Estrategias de respuesta: Para cada riesgo alto se debe definir una respuesta a tal: mitigar, transferir (ej. pólizas de seguros), aceptar o evitar (NIST, 2020).

1.14.4 Plantilla de seguimiento

El seguimiento del proyecto se realiza mediante Status Reports (informes de estado). Se debe utilizar una plantilla ejecutiva, directa y concisa.Elementos clave de una hoja de seguimiento (Meredith y otros, 2017):

1. **Semáforo del proyecto (RAG status):** Rojo (Crítico), Ámbar (En Peligro), Verde (En Progreso).
2. **Hitos alcanzados (periodo actual):** Objetivos alcanzados en esta semana/mes.
3. **Hitos planificados (próximo periodo):** Objetivos a completar la semana que viene.
4. **Bloqueos e impedimentos:** Problemas que requieren la atención de la alta dirección.
5. **Control de cambios:** Listado de solicitudes de cambio aprobadas o rechazadas del alcance.

1.14.5 Estándares y buenas prácticas

Existen marcos de referencia internacionales que regulan la gestión de proyectos de tecnología. La elección del marco depende del tipo de proyecto (predictivo frente a adaptativo). PMBOK (Project Management Body of Knowledge): Estándar del PMI. Tradicionalmente centrado en las metodologías cascada (Waterfall); es ideal para

proyectos donde de antemano se tienen claros los requisitos, como por ejemplo proyectos de infraestructura o construcción de centros de datos.

PMBOK (Project Management Body of Knowledge): Estándar del PMI. Tradicionalmente centrado en las metodologías cascada (Waterfall); es ideal para proyectos donde de antemano se tienen claros los requisitos, como por ejemplo proyectos de infraestructura o construcción de centros de datos (Project Management Institute (PMI), 2021).

PRINCE2 (Projects IN Controlled Environments): Metodología basada en procesos, muy usada en Europa y en el sector público. Se centra en la justificación comercial continua del proyecto (Axelos, 2017).

Agile/Scrum: Marcos de trabajo iterativos e incrementales. Se consideran las "buenas prácticas" estándar en el desarrollo de software actual donde los requisitos pueden cambiar con frecuencia y donde se prima la entrega rápida de valor en lugar del control de la documentaciónde (Schwaber & Sutherland, 2020).

ISO 21500: Norma internacional que ofrece una guía genérica sobre conceptos y procesos de gestión de proyectos (International Organization for Standardization ISO, 2020).

1.15 Norma 410-08 desarrollo, mantenimiento y adquisición de software

Este dominio garantiza que los sistemas de información sean desarrollados, adquiridos y mantenidos dentro de un marco de control que asegure su funcionalidad, seguridad y alineación con los objetivos empresariales (ISACA, 2019).

1.15.1 Matriz de controles por fase de desarrollo

Con el objetivo de reducir el riesgo, se establecen controles específicos ("Quality Gates") en cada fase del Ciclo de Vida de Desarrollo de Software (SDLC). Un ejemplo de ello es el estudio de Pressman y Maxim (2020) que muestra que el coste de corregir un error detectado en una fase avanzada del SDLC se incrementa exponencialmente si este error no se detecta hasta mucho más tarde.

La tabla 2, muestra aquellos controles clave que la norma ISO/IEC 12207 exhorta realizar en cada fase del ciclo de vida del desarrollo de software (SDLC) y persigue asegurar que el proceso de desarrollo sea coherente, seguro y orientado a los objetivos del proyecto a realizar desde que se definen los requisitos hasta el despliegue final.

Tabla 2. Matriz de controles por fase de desarrollo

Fase del SDLC	**Control Sugerido (ISO/IEC 12207)**	**Objetivo del Control**
Requisitos	Aprobación formal del documento de requisitos	Evitar el "deslizamiento del alcance" (*scope creep*) y asegurar alineación

	por el usuario final (*Stakeholder Sign-off*).	
Diseño	Revisión de arquitectura de seguridad y modelado de amenazas.	Identificar vulnerabilidades de diseño antes de escribir código.
Desarrollo (Codificación)	Uso de estándares de codificación segura (ej. OWASP Top 10) y revisión por pares (*Code Review*).	Prevenir la inyección de código malicioso o errores lógicos.
Pruebas (QA)	Segregación de ambientes: Desarrollo ≠ Pruebas ≠ Producción.	Asegurar que los datos de prueba no sean reales (anonimización) y validar funcionalidad.
Despliegue	Aprobación del Comité de Cambios (CAB) y plan de reversión (*Rollback plan*).	Garantizar que el paso a producción no interrumpa el servicio.

Fuente: Maxim, (2020)

Nota: Adaptado de la matriz de controles en fase de desarrollo en base a la norma ISO/IEC 12207

El análisis de esta Tabla 2, pone en evidencia cómo cada una de las fases del SDLC incorpora los controles necesarios para evitar riesgos y asegurar la calidad del producto. Por ejemplo, en la fase de requisitos, la aprobación formal del usuario evita desviaciones del alcance y permite garantizar que existe una mejor comprensión del proyecto. En la fase de diseño, la revisión del engendro arquitectónico y el modelado de amenazas permiten reconocer vulnerabilidades antes del momento de la construcción de software, lo que disminuye los fallos futuros.

En la fase de desarrollo, la utilización de estándares de codificación segura y la revisión por pares contribuyen a atender errores lógicos e inyecciones maliciosas, mientras que, en la fase de pruebas, la separación clara entre entornos y la anonimización de datos resguardan la información sensible y permiten validar adecuadamente la última funcionalidad. En la fase de despliegue, la revisión del Comité de Cambios y un plan de reversión del software garantizan el efecto de una separación de la transición, evitando la interrupción del servicio. Estos controles refuerzan un tipo de trazabilidad, seguridad y confiabilidad del proceso de desarrollo, de manera conjunta.

1.15.2 Indicadores técnicos

Los indicadores técnicos permiten cuantificar la calidad intrínseca del software y la propia eficiencia del proceso de mantenimiento.

- **Densidad de defectos:** Número de errores confirmados por cada 1,000 líneas de código (KLOC). Un índice alto puede ser indicativo de un problema en la fase de codificación o en la fase de diseño (Sommerville, 2016).
- **Complejidad ciclomática:** Una métrica que establece el grado de complejidad lógica del programa.Un índice de complejidad elevado (>10) implica un código que resulta prácticamente inasequible de mantener y que, además, tiene muchas posibilidades de fallar (Watson & McCabe, 1996).
- **Deuda técnica:** Costo presupuestado del retrabajo que hay que realizar como consecuencia de optar por una solución "rápida y

sucia" en lugar de una alternativa que sería mejor pero que requeriría más tiempo (Fowler, 2019).

- **Tiempo medio de reparación (MTTR):** Tiempo promedio que se tarda en reparar un bug crítico en producción.

1.15.3 Evidencias requeridas

El auditor que haga una auditoría de sistemas buscará evidencias documentales que demuestren que fue controlado el proceso.

- **Documento de Especificación de Requisitos (SRS):** Validado y firmado.
- **Resultados de Pruebas (Unitarias, Integración y UAT):** Prueba de las pruebas; el software ha de haber pasado exitosamente antes de salir a producción.
- **Registros de Análisis de Código Estático (SAST):** Informes automatizados para demostrar que el código fue escaneado a la búsqueda de vulnerabilidades de seguridad (OWASP , 2021).
- **Contratos de Nivel de Servicio (SLA) y Licencias:** En el caso de adquisiciones de software, contratos que hagan referencia a soporte, actualizaciones, propiedad intelectual.

1.15.4 Lista de verificación

Herramienta de verificación para la seguridad y calidad previas a la puesta en marcha ("Go-Live").

- [ ] ¿Se han eliminado las cuentas de prueba y contraseñas por defecto antes del despliegue? (NIST, 2020).

- [ ] ¿La separación de funciones (SoD) es clara? (los desarrolladores no deben tener acceso de escritura a Producción).
- [ ] ¿Se ha efectuado una prueba de carga (Stress Testing) para asegurar que el sistema soporta la concurrencia esperada?
- [ ] ¿El código fuente está respaldado en un repositorio centralizado y versionado convenientemente?

1.15.5 Riesgos de desarrollos no controlados

La no existencia de una metodología de desarrollo, popularmente conocida como "programación de vaquero" (cowboy coding), comporta un riesgo importante para la organización.

- **Shadow IT:** Departamentos de forma aislada que producen o adquieren software sin conocimiento del área de TI, generando silos de información y brechas en seguridad (Silic & Back, 2014).
- **Vulnerabilidades de seguridad:** Código no revisado en relación con vulnerabilidades que permiten un ataque de, por ejemplo, inyección SQL o Cross-Site Scripting (XSS).
- **Dependencia de personas clave:** Código "espagueti" que sólo entiende su autor, lo que dificulta su mantenimiento si esa persona sale de la organización.

1.15.6 Trazabilidad de cambios

La trazabilidad es la capacidad de rastrear un cambio en el sistema desde su origen (una solicitud del usuario) hasta su implementación final.

- **Control de versiones:** Uso de herramientas como Git para registrar quién ha modificado qué línea de código y cuándo (Loeliger & McCullough, 2012).
- **Vinculación ticket-código:** Buenas prácticas (como DevOps) requieren que cada "commit" en el código esté asociado a un número de ID de un ticket de requerimiento o incidencia (ej. JIRA-123).
- **Línea base de configuración:** Consiste en mantener un registro del estado aprobado del sistema en un momento dado para futuras comparaciones (ISO, 2018).

1.16 Norma 410-09 adquisición de infraestructura tecnológica

La adquisición de la infraestructura tecnológica no está solamente sujeta a la compra de un determinado equipamiento. Es un proceso estratégico que se debe alinear con la arquitectura empresarial y que debe también garantizar el retorno de la inversión. Con la norma ISO/IEC 19770 (Gestión de Activos de TI), el objetivo debe ser el de maximizar el valor y minimizar riesgo y coste no sólo a la hora de adquirir dicho activo sino a lo largo de su ciclo de vida (International Organization for Standardization ISO, 2017).

1.16.1 Indicadores de adquisición

Para poder gestionar la eficiencia en las compras de tecnología, se utilizan indicadores financieros y operativos. El más importante en infraestructura es el TCO (Total Cost of Ownership)

- **Costo Total de Propiedad (TCO):** Se considera no solo el precio de adquisición, sino también el coste de la utilización del equipo a lo largo de su vida útil (consumo de energía, refrigeración, asistencia, licencias, etc.)

$$TCO = I + O + M + D$$

Donde:

I: Inversión inicial.

O: Costes de utilización (consumo de electricidad, personal).

M: Costes de mantenimiento y licencias.

D: Costes de eliminación/reciclado (Ellram, 1995).

- **ROI de infraestructura:** Rendimiento de la inversión medida en función del incremento en la productividad o de la reducción de los riesgos introducidos con la nueva tecnología (Gartner, 2020).
- **Tiempo de aprovisionamiento:** Tiempo que transcurre desde el momento en que se pide el equipo hasta que está instalado y operativo en el escritorio del usuario o en el Data Center.

1.16.2 Evidencias y documentación soporte

En una auditoría (en especial en el ámbito público o universitario), la trazabilidad de los documentos es necesaria para demostrar que no hay fraudes ni sobrecostes.

- **Solicitud de propuesta (RFP - Request for Proposal):** Documento técnico que se envía a los proveedores para detallar lo que se necesita.
- **Cuadro comparativo de ofertas:** Matriz en la cual se evalúan técnica y económicamente las ofertas de los postores. Debe hacer evidente la elección del proveedor ganador (Monczka y otros, 2020).
- **Contratos y garantías:** Documentos legales que garantizan el soporte técnico (SLA de reparación/reemplazo) por parte del fabricante.
- **Acta de conformidad:** Documento firmado por el área técnica certificando que lo recibido coincide con lo que solicitó la orden de compra.

1.16.3 Lista de verificación técnica

Antes de recibir la infraestructura, hay que verificar que la propia infraestructura cumpla con los requisitos físicos y lógicos.

1. **Compatibilidad:** ¿El nuevo hardware es compatible con los sistemas operativos y periféricos (Legacy systems)?
2. **Escalabilidad:** ¿El servidor/equipo permite incrementar memoria RAM o disco sin requerir la sustitución de toda la unidad? (Stallings, 2019).
3. **Eficiencia energética:** ¿Cumple con las especificaciones Energy Star o normas de Green IT? Esto lo es para reducir la huella de carbono institucional (Murugesan & Gangadharan, 2012).

4. **Certificaciones de seguridad:** ¿El hardware incluye módulos TPM (Trusted Platform Module) para realizar cifrado por hardware?

1.16.4 Estándares mínimos de equipos

A fin de eludir la heterogeneidad que obstaculiza el soporte técnico, la institución tiene que definir un "Entorno Operativo Estándar" (SOE).

- **Estandarización:** Definir los perfiles de usuario (ej. "Perfil Administrativo", "Perfil Diseño/Ingeniería", "Perfil Docente").
- **Ejemplo perfil administrativo:** Procesador i5/Ryzen 5, 16GB RAM, 512GB SSD.
- **Ejemplo perfil servidor BD:** Procesador Xeon/Epyc, RAID 10, Redundancia de fuente de poder.
- **Ciclo de renovación:** Política que define cada cuanto se van sustituyendo los equipos (normalmente 3-5 años para PCs, 5-7 años para servidores) (Laudon & Laudon, 2020).

1.16.5 Matriz de control de adquisiciones

Herramienta de gestión para controlar el estado de las compras en trámite. La Tabla 3, presenta un registro para dar seguimiento al ciclo completo de adquisición de activos tecnológicos, desde la solicitud, el proveedor, la entrega, la inspección técnica y la ubicación final. Este tipo de herramienta permite la trazabilidad y la gestión administrativa de los bienes en tránsito y de los recibidos.

Tabla 3. Herramienta de gestión para monitorear el estado de las compras

ID Req.	Descripción del Activo	Proveedor	Fecha Orden	Fecha Entrega	Estado	Inspección Técnica	Ubicación Final
HW-001	Servidor Rack Dell	TechData	12/01/2025	15/02/2025	En tránsito	Pendiente	Data Center 1
HW-002	30 Laptops HP	Compudiskett	10/01/2025	20/01/2025	Recibido	Conforme	Lab. Computo 3

Fuente: Laudon & Laudon, (2020)

Nota: Adaptado y con datos del autor

La Tabla 3, tiene por finalidad mostrar un proceso de compras perfectamente ordenado y transparente, en el cual cada activo tiene un pudiera de identificador único, así como una descripción precisa y un proveedor sentado. Esta estructura aporta la trazabilidad documental; las fechas de orden y de entrega permiten verificar el cumplimiento de plazos, mientras que el estado del trámite (como "En tránsito" o "Recibido") recopila la información más actualizada sobre los avances. La revisión de la inspección técnica se presenta como un proceso que evidencia que los bienes cumplen con los estándares exigidos antes de poder su uso. En la fase de entrega, la ubicación final que describe el movimiento físico del inventario. En su conjunto, esta herramienta contribuye a una gestión más eficiente, a reducir errores sanitarios y aporta una base para auditorías internas o para auditorías externas.

1.17 Norma 410-10 mantenimiento y control de infraestructura tecnológica

El mantenimiento de la infraestructura tecnológica incluye y engloba las actividades técnicas y administrativas que tienen como fin conservar los activos de TI o bien restaurarlos a un estado donde sean capaces de realizar correctamente la función requerida. La norma ISO/IEC 20000 sostiene que la adecuada gestión del mantenimiento es uno de los pilares que asegura la calidad y disponibilidad de los servicios de TI (International Organization for Standardization ISO, 2018).

1.17.1 Indicadores de mantenimiento

Con la finalidad de auditar la adecuación del mantenimiento se emplean métricas de ingeniería de fiabilidad y gestión de servicios (ITIL).

- **MTBF (Mean Time Between Failures - Tiempo Medio Entre Fallas):** Es una métrica que describe la fiabilidad de un activo. Esta métrica corresponde al tiempo que un sistema funciona sin producir interrupciones; un MTBF alto es sinónimo de fiabilidad.
- **MTTR (Mean Time To Repair - Tiempo Medio Para Reparar):** Describe la eficiencia del equipo de soporte.Es el promedio de tiempo que tarda la restauración del servicio tras una avería (Dhillon, 2006).
- **Disponibilidad (A):** Porcentaje del tiempo durante el cual está operativa la infraestructura. Se calcula como:

$$A = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}\ x\ 100$$

- **Cumplimiento del plan preventivo:** Porcentaje de mantenimientos preventivos programados que se realizaron de hecho en la fecha prevista.

1.17.2 Registro técnico obligatorio

La inexistencia de registros históricos, registros ("bitácoras") es una de las "No Conformidades" de nivel mayor cuando se trata de auditorías de sistemas. Cada obra debe de estar registrada de tal manera que garantice la trazabilidad.

- **Bitácora de centro de datos:** Registro físico o digital del acceso al Data Center, intervención en racks y motivo de la intervención (NIST, 2020).
- **Hoja de vida del equipo:** Expediente individual por cada activo crítico (servidores, switches core) que contenga:
- Fecha de compra y de fin de la garantía
- Historial de reparaciones y reemplazos de piezas.
- Actualizaciones de firmware y parches de seguridad aplicados (Souppaya & Scarfone, 2018).
- **Informes de mantenimiento externo:** Si el mantenimiento es de externalización, los informes técnicos, firmados por el contratista, son prueba contractual.

1.17.3 Matriz de seguimiento

Herramienta de control que refleja la programación de actividades preventivas versus correctivas. La Tabla 4, proporciona un registro ordenado del mantenimiento de los activos tecnológicos, en la que se

pone de manifiesto la periodicidad, el tipo de intervención, el responsable que ejecuta dicha actividad y el estado de la misma a nivel de cuándo se han realizado, o bien este estado refleja el que pase a hacerse una intervención. Esta herramienta permite planificar y llevar un control del mantenimiento de actividades y de acciones de tipo preventivo y de tipo correctivo.

Tabla 4. Herramienta de control de la programación de actividades preventivas vs las correctivas

Activo ID	**Ubicación**	**Tipo Mantenimiento**	**Frecuencia**	**Última Ejecución**	**Próxima Ejecución**	**Responsable**	**Estado**
SRV-APP-01	Data Center	Preventivo (Limpieza física y logs)	Trimestral	15/1/2025	15/4/2025	Admin. Redes	Programado
UPS-CORE	PC-LAB-05	Predictivo (Test de baterías)	Semestral	1/12/2024	1/6/2025	Proveedor Ext.	Vigente
PC-LAB-05	Lab. Cómputo	Correctivo (Cambio disco duro)	N/A	8/2/2025	N/A	Soporte L1	Cerrado

Fuente: Souppaya & Scarfone, (2018)

Nota: Herramienta de control de la programación de actividades preventivas y correctivas

La Tabla 4, ofrece un control estructurado del mantenimiento institucional al clasificar el tipo de actuación según las necesidades de cada uno de los activos, de modo que las actividades de tipo preventivo, tal y como son, la limpieza de los equipos y la revisión de los logs, permiten “prever averías”, tal y como se mencionó más arriba, porque se realizan con periodicidad fija, lo que permite sacar la conclusión de que se lleva a cabo una gestión proactiva. Por otro lado, las actividades de tipo correctivo son las que nacen tras el fallo ya ocurrido, de las que se pueden poner ejemplos como el cambio del disco duro seguro de un equipo; se hace un registro de cada una de las actividades que permite ver cómo se realizan las intervenciones, a través de las fechas que sirven para que éstas cierren (dentro del correspondiente protocolo de actuación).

Con respecto a la columna de responsables, queda claro quién es el que hace cada tarea y, de la misma manera, el estado actual (programado, vigente o cerrado) de cómo se van realizando las intervenciones. En su conjunto, la tabla refuerza dicha trazabilidad operativa y sirve de ayuda para la correcta toma de decisiones para asegurar la continuidad del servicio operativo tecnológico.

1.17.4 Inventario tecnológico

A diferencia de "adquisición" (punto 1.15), el Inventario aquí se centra en el control operativo y Gestión de la Configuración (CMDB). No sirve solo saber lo que se ha adquirido, sino saber qué tienen que ver esas adquisiciones con el servicio.

- **CMDB (Configuration Management Database):** Base de Datos de Gestión de la Configuración) - Base de datos que contiene no solo los atributos de los dispositivos (CI - Configuration Items), sino también aquellas relaciones entre ellos (ej. "El Servidor X soporta el Sistema de Matrículas Y") (Axelos, 2019).
- **Conciliación de Inventario:** Proceso de auditoría física (conteo) versus registro lógico para detectar robos, pérdidas o "activos fantasma" (dispositivos que pagan licencias, pero no existen).

1.17.5 Riesgos por falta de mantenimiento

La negligencia del mantenimiento comporta riesgos operacionales y de seguridad que pueden paralizar la institución.

- **Obsolescencia no planificada:** Equipos que fallan de forma prematura por falta de limpieza (polvo, calor) o falta de actualización, lo que obliga a gastos de emergencia (inversión no presupuestada).
- **Brechas de seguridad:** La falta de mantenimiento de software (parcheo) es la principal vía de entrada a vulnerabilidades que pueden ser explotadas. El famoso ataque de WannaCry afectó a sistemas que no habían recibido mantenimiento de seguridad (Stallings & Brown, 2018).
- **Pérdida de garantía:** Muchos fabricantes invalidan la garantía del dispositivo si no se logra demostrar que el dispositivo mantuvo unas condiciones ambientales controladas y un mantenimiento periódico.

1.18 Norma 410-11 seguridad de tecnologías de información

La seguridad de la información no se reduce únicamente a la "instalación de antivirus y a la existencia de firewalls"; más bien puede definirse como la salvaguarda de la Confidencialidad, Integridad y Disponibilidad (Tríada CID) de la información. En el ámbito del entorno universitario esto puede traducirse en asegurar u ofrecer protección a los datos personales de los estudiantes, o dar cobertura a las investigaciones científicas o incluso las patentes (Whitman & Mattord, 2021).

1.18.1 Indicadores de seguridad

La seguridad de la información no se reduce únicamente a la "instalación de antivirus y a la existencia de firewalls"; más bien puede definirse como la salvaguarda de la Confidencialidad, Integridad y Disponibilidad (Tríada CID) de la información. En el ámbito del entorno universitario esto puede traducirse en asegurar u ofrecer protección a los datos personales de los estudiantes, o dar cobertura a las investigaciones científicas o incluso las patentes.

- **MTTD (Mean Time To Detect):** Tiempo medio que tarda la organización en detectar una intrusión de seguridad.
- **MTTR (Mean Time To Respond/Remediate):** Tiempo medio que la organización requiere para contener y solucionar el incidente de seguridad una vez este ya ha sido detectado.
- **Porcentaje de cobertura de parches:** Porcentaje de servidores y estaciones de trabajo donde se encontraban instalados los parches

críticos de seguridad en el plazo de 30 días desde su lanzamiento (Scarfone et al., 2008).

- **Tasa de éxito en phishing (simulacros):** Porcentaje de empleados/docentes que hicieron clic en un vínculo malicioso con ocasión de una prueba controlada. Un porcentaje alto indicaría la necesidad de realizar una capacitación para los empleados (Hadnagy, 2018).

1.18.2 Evidencias del SGSI institucional

El Sistema de Gestión de Seguridad de la Información (SGSI) necesita de documentación probatoria para la realización de la auditoría; sin esta no puede considerarse la seguridad del SGSI más que "ad hoc" o desordenada.

- **Política General de Seguridad de la Información:** Documento de alto nivel (dirección) que cuenta con la aprobación del Rectorado o del Consejo Universitario, mediante el cual se determina el compromiso de la Institución en cuestiones de seguridad (ISO, 2022).
- **Declaración de Aplicabilidad (SoA - Statement of Applicability):** Documento requerido en la norma ISO 27001 que funciona como un listado de los controles de seguridad (del Anexo A) que se encuentran en marcha y de los cuales se justifican las exclusiones.
- **Registros de Incidentes:** Registro histórico de las violaciones de seguridad, análisis de la causa raíz y acciones correctivas adoptadas.

- **Acuerdos de Confidencialidad (NDA):** Firmados por los administradores de los sistemas y por terceras personas con acceso a informaciones sensibles.

1.18.3 Checklist de controles mínimos

Se basa en los Controles CIS (Center for Internet Security) y permite comprobar la "higiene cibernética" mínima.

- [ ] Inventario de Activos y Software: ¿Se sabe ya de cada uno de los equipos que se encuentra en Conectivities en la red universitaria? (No se puede proteger lo que no se sabe que existe).
- [ ] Defensa contra Malware: ¿Hay protección endpoint (EDR/Antivirus) actualizada en el 100% de los equipos administrativos?
- [ ] Protección de Datos: ¿Los datos sensibles (notas, nóminas) están cifrados tanto en reposo (en base de datos) como durante eventos de tráfico (HTTPS/TLS)? (Stallings, 2017).
- [ ] ¿Se realizan escaneos de vulnerabilidades de forma automatizada al menos cada tres meses?
- [ ] Concientización: ¿Hay un programa anual de capacitación en seguridad para el personal?

1.18.4 Matriz de riesgos de seguridad

La matriz de riesgos de seguridad es diferente de la matriz de riesgos de proyecto (1.13.3) definida en la norma ISO/IEC 27005, ya que la matriz de seguridad se basa en amenazas cibernéticas y vulnerabilidades técnicas.

Estructura de evaluación:

$$Riesgo = (Amenaza\ x\ Vulnerabilidad\ x\ Impacto)$$

La Tabla 5, se presenta la matriz de evaluación de riesgos la cual permite realizar la identificación, valoración y tratamiento de los riesgos inherentes a diversos activos tecnológicos considerándolos críticos. La "Matriz de evaluación de riesgos", mediante el análisis de amenaza, de vulnerabilidad, de impacto y de nivel de riesgo, permite priorizar acciones de mitigación a llevar a cabo con el fin de mejorar la seguridad de la infraestructura institucional.

Tabla 5. Matriz de evaluación de riesgos

Activo	**Amenaza**	**Vulnerabilidad**	**Impacto (C-I-D)**	**Nivel Riesgo**	**Tratamiento**
Servidor Web Notas	Ataque DDoS	Ancho de banda limitado sin mitigación	Alto (Disponibilidad)	Extremo	Contratar servicio Anti-DDoS (Cloudflare/Akamai)
Base de Datos RRHH	Ransomware	Falta de copias offline (inmutables)	Crítico (Integridad/Disp.)	Crítico	Implementar Backups 3-2-1 con cinta o nube inmutable
Portal Docente	Inyección SQL	Código no sanitizado en login	Alto (Confidencialidad)	Alto	Corregir código y aplicar WAF (Web App Firewall)

Fuente: Stallings, (2017)

Nota: Matriz de evaluación de riesgos que afectan a los activos tecnológicos

La matriz pone en evidencia una evaluación elaborada que permite conocer cómo diversas amenazas afectan a los activos tecnológicos de forma diferenciada. Para el servidor web, un ataque de tipo DDoS entiende por un riesgo extremo, por el impacto que puede llegar a tener en la Disponibilidad de un servicio y la vulnerabilidad manifiesta por la limitada capacidad de ancho de banda de la infraestructura y por eso se propone la ejecución de servicios de mitigación especializados.Referente a la base de datos de RRHH, la ausencia de copias offline provoca que sea muy vulnerable al ransomware, lo que da sentido a la recomendación de poner en marcha un esquema de respaldos 3-2-1 que permitan estar seguros de la integridad y recuperación; finalmente, el portal del docente tiene vulnerabilidad de código no sanitizado, lo que aumenta el riesgo de inyección SQL y pone en riesgo la confidencialidad; por ello, hace falta corregir el código e incrementar la protección mediante un WAF; por ello, la matriz sirve para priorizar las medidas de acuerdo con la criticidad, optimizando así la gestión de riesgos y la continuidad de la operación.

1.18.5 Auditoría interna de seguridad

Es la validación independiente (fase "Check" del ciclo PHCA), para validar que los controles funcionan para mitigar el problema que hay que mitigar.

- **Pruebas de penetración (pentesting):** Simulaciones de ataques de forma ética ("Hacking Ético") para localizar agujeros de seguridad antes de que lo haga un criminal (Engebretson, 2013).
- **Revisión de logs:** Auditoría de los logs de acceso de administradores en los sistemas informáticos para detectar comportamientos anómalos o abuso de privilegios.
- **Auditoría de cumplimiento:** Confirmar que las configuraciones de los servidores sean conformes a los estándares de endurecimiento (Hardening) como los benchmarks de CIS (ISACA, 2019).

1.19 Norma 410-12 contingencia y continuidad operativa

La continuidad operativa tiene como objetivo garantizar que las funciones críticas de la organización continúen operando, es decir, que se pueda recuperar la funcionalidad en cuanto haya una interrupción grave (desastre natural, ciberataque, fallo significativo). A diferencia de la contingencia (tendiendo a ser un plan "B" inmediato), en la continuidad operativa se puede hablar de una estrategia de negocio transversal (International Organization for Standardization ISO, 2019).

1.19.1 Indicadores de continuidad

Éstos son los parámetros técnicos que permiten definir la arquitectura de respaldo. Sin definir estos tiempos, se hace imposible diseñar una estrategia de recuperación (económica).

- **RTO (Recovery Time Objective - Objetivo de Tiempo de Recuperación):** Tiempo máximo tolerable que puede estar un

sistema "caído" antes de que la afectación sea inaceptable. Ejemplo: El sistema de biblioteca quizás tenga un RTO de 48 horas, pero el sistema de matrículas en rige de inscripciones quizás tenga un RTO de 4 horas.

- **RPO (Recovery Point Objective - Objetivo de Punto de Recuperación):** Cantidad máxima de datos (en términos temporales) que la organización aceptará perder. Determina con qué frecuencia hay que hacer los backups. Ejemplo: Un RPO de 24 horas significa que, si el sistema se detiene hoy, aceptamos perder la información introducida hasta ayer (Snedaker & Rima, 2013).
- **MTPD (Maximum Tolerable Period of Disruption):** el tiempo límite absoluto en el cual la viabilidad de la organización está de forma irrevocable comprometida.

1.19.2 Matriz de impacto al negocio

El BIA es el corazón del plan de continuidad. Permite distinguir entre lo "urgente" y lo "crítico". Asimismo, como señala NIST SP 800-34, el BIA detecta los procesos de negocio y cuantifica el impacto de su parada (Swanson y otros, 2010).

La Tabla 6, da lugar a un ejemplo de BIA (Business Impact Analysis) aplicado a procesos clave dentro de una universidad. Su objetivo es el de detectar el nivel de importancia en cada uno de los procesos, las posibles consecuencias financieras, legales y de reputación derivadas de la interrupción del mencionado proceso y un RTO (Recovery Time

Objective) sugerido para priorizar actuaciones dentro del Plan de Continuidad Institucional.

Tabla 6. Ejemplo de estructura BIA para Universidad

Proceso	**Impacto Financiero**	**Impacto Legal/Reputación**	**RTO Sugerido**	**Nivel de Criticidad**
Procesamiento de Notas	Medio (Retraso en becas)	Crítico (Demandas, descrédito académico)	24 horas	Alto
Plataforma E-learning	Bajo (Clases asincrónicas)	Medio (Quejas estudiantiles)	48 horas	Medio
Sistema de Cafetería	Bajo	Bajo	1 semana	Bajo

Fuente: Swanson y otros, (2010)

Nota: Ejemplo de estructura BIA para universidades en base a la norma NIST SP 800-34

El análisis muestra que Procesamiento de Notas es el proceso más crítico, puesto que tiene un impacto directo en las becas, la suficiencia académica e incluso reclamaciones legales, por esta razón se sugiere un RTO de 24 horas. La Plataforma E-learning presenta un nivel de criticidad medio; si bien sus impactos son menores, una interrupción en este proceso afecta la experiencia del estudiante, lo que justifica un RTO de 48 horas. Finalmente, el Sistema de Cafetería muestra el menor nivel de impacto y criticidad ya que su interrupción no afecta directamente a las funciones académicas o administrativas, decantándose por un RTO

de una semana. En definitiva, la tabla permite priorizar recursos y estrategias atendiendo a la práctica importancia de los procesos.

1.19.3 Plan de contingencias

Conjunto de procedimientos técnicos y operativos a llevar a cabo ante la crisis. Éste tiene ser un "Playbook" paso a paso, no un documento teórico.

- **Plan de Recuperación de Desastres (DRP):** Sólo en TI (restaurar servidor, redes, datos).
- **Plan de comunicación de crisis:** Protocolo para informar a los stakeholders (alumnos, prensa, gobierno) y controlar la narrativa sin generar miedo (Coombs, 2014).

Estrategias de recuperación:

- Hot site: Data Centre espejo, en condiciones de funcionar inmediatamente; muy caro.
- Warm site: Equipos disponibles, pero hay que restaurar datos; coste medio.
- Cold site: Espacio físico disponible, pero sin equipos instalados; bajo coste y lento en la recuperación.

1.19.4 Evidencias de pruebas y simulacros

Un plan no probado no es un plan y por consiguiente no existe tal plan. La norma ISO 22301 establece como obligación la realización de

pruebas de modo certero y periódico como una manera de validar la eficacia del plan y la formación del personal para utilizarlo.

- **Pruebas de escritorio (tabletop exercises):** Reunión de líderes para discutir un escenario imaginario (ej. "Inundación del Data Center") y validar la toma de decisiones.
- **Simulacros funcionales:** Prueba de partes concretas (ej. restaurar backup completo en un servidor aislado para comprobar que su contenido es legible).
- **Simulacro total (Full-Scale):** Desconexión real del sitio principal y utilización del sitio de contingencia (casi nunca se desarrolla por el riesgo operativo) (Elliott y otros, 2025).
- **Informe de lecciones aprendidas:** Documento posterior al simulacro que incluye lo que funcionó, lo que falló y lo que debe ser corregido del mismo.

1.19.5 Lista de verificación técnica

Elementos tangibles que debe revisar físicamente el auditor.

- [ ] Lista de Llamadas (Call Tree): ¿Se encuentran actualizados en el equipo de crisis los números de teléfono personales? (Puede que el correo corporativo no funcione en un escenario catastrófico).
- [ ] Acceso a Backups Off-site: ¿Las cintas o la nube de backup se pueden acceder desde una ubicación diferente al campus habitual?
- [ ] Suministro Eléctrico: ¿El grupo electrógeno tiene combustible y contrato de reabastecimiento garantizado?

- [ ] Documentación Impresa: ¿Existe copia del plan de contingencia? (Si la red no funciona no se podrá acceder al PDF en el servidor).

1.20 Norma 410-13 administración del soporte tecnológico

La gestión del soporte tecnológico, normalmente centralizada en una Mesa de Servicios (Service Desk), representa el punto único de contacto (SPOC) que tienen los usuarios de la tecnología y el proveedor de servicios de TI; no solo se trata de "arreglar cosas", también se recomienda restaurar lo antes posible la operación normal del servicio y minimizar la afectación negativa en las operaciones del negocio (Axelos, 2019).

1.20.1 Indicadores del servicio

Para auditar la eficacia del soporte, deben medirse métricas de rendimiento que tracen tanto la rapidez como la calidad de la atención proporcionada.

- **FCR (First Contact Resolution - Resolución al Primer Contacto):** Es el porcentaje de tickets que se resuelven en la primera llamada o interacción, sin escalar a niveles superiores, y es el indicador más sólido de eficiencia y satisfacción del usuario (HDI, 2028).
- **Tiempo Promedio de Resolución (MTTR - Mean Time to Resolve** por sus siglas en inglés): Este es el tiempo medio que pasa desde que se abre el ticket, hasta que el ticket llega a su cierre como tal.

- **Tasa de abandono de llamadas:** porcentaje de usuarios que cuelgan el teléfono antes de ser atendidos. Una tasa elevada (>5-8%) puede ser un indicativo de falta de profesionales y/o de un flujo de trabajo poco eficiente en el triage (Thess, 2016).

1.20.2 Gestión de tickets

La gestión de tickets se basa en el flujo de trabajo estructurado para gestionar incidentes y solicitudes. Es importante diferenciar entre ambas:

- **Incidente:** Interrupción no planificada de un servicio (ej. "no funciona el proyector del aula 101").
- **Solicitud de servicio:** Petición de información o acceso preaprobado (ej. "necesito que me instalen SPSS en mi portatil").
- El ciclo de vida del ticket debe ser auditable: Apertura → Clasificación → Asignación → Resolución → Cierre (Axelos, 2019).

1.20.3 Matriz de tiempos de respuesta

Los tiempos de respuesta no se deciden al azar, sino que se establecen en función de la Prioridad, que se calculará cruzando el Impacto (a cuántas personas afecta) y la Urgencia (qué tan rápido se necesita una solución).

La Tabla 7 incorpora una matriz de priorización de la norma ISO/IEC 20000, la cual prescribe la clasificación de los incidentes según su nivel de urgencia e impacto que generan en la institución. Este diagrama

permite establecer tiempos de respuesta y resolución adecuados en función de la urgencia que presenta el incidente, permitiendo así que con esa definición se permita la correcta asignación de los recursos de la sección de soporte en función de la criticidad del servicio que resulta afectado.

Tabla 7. Ejemplo de Matriz de Priorización (Basada en ISO/IEC 20000)

Urgencia / Impacto	**Impacto Alto (Toda la Univ.)**	**Impacto Medio (Un Depto.)**	**Impacto Bajo (Un Usuario)**
Urgencia Alta	P1 - Crítico (Resp: 15 min / Res: 4h)	P2 - Alto (Resp: 30 min / Res: 8h)	P3 - Medio (Resp: 2h / Res: 24h)
Urgencia Media	P2 - Alto (Resp: 30 min / Res: 8h)	P3 - Medio (Resp: 2h / Res: 24h)	P4 - Bajo (Resp: 4h / Res: 48h)
Urgencia Baja	P3 - Medio (Resp: 2h / Res: 24h)	P4 - Bajo (Resp: 4h / Res: 48h)	P5 - Planificado (Resp: 8h / Res: 1 semana)

Fuente: ISO/IEC (20000)

Nota: Ejemplo de matriz de priorización. "Resp = Tiempo para primera respuesta humana; "Res" = Tiempo para solución definitiva).

La matriz contempla cinco niveles de prioridad (P1 a P5) que son establecidas en función de una combinación entre urgencia e impacto. Los incidentes que presentan urgencia alta y afectan a una institución son clasificados como P1 - Crítico y requieren de una respuesta inmediata (la respuesta es de 15 minutos y la resolución en 4 horas). A

medida que el impacto de un incidente desciende a nivel departamental o a nivel de un usuario la prioridad pasa a ser P2 o P3 y los tiempos de resolución son más extensos. Los incidentes que presentan urgencia media suelen tener prioridades intermedias (P2, P3 y P4) y reflejan la urgencia por atacarlos, pero con ello no aparecen las presiones críticas de tener una gran afectación.

Finalmente, los eventos o incidentes que presentan urgencia baja suelen clasificarse como P3, P4 y P5 siendo esta última la que comprende requerimientos planificados o incidentes con bajo impacto y con tiempos de resolución que pueden por tanto alargarse hasta una semana. En definitiva, la matriz permite la gestión de incidentes ordenadamente, de manera que los incidentes con mayor impacto operativo y reputacional sean resueltos rápidamente y se pueda optimizar el uso del personal y de los recursos de TI.

1.20.4 Evidencias del soporte

El auditor comprobará la existencia de comprobantes que indiquen que la forma de soporte no es informal (WhatsApp personal o "de favor"), sino que se trata de un soporte institucional:

- Sistema de Ticketing (ITSM Tool): Base de datos que almacena la trazabilidad (de un modo como Jira Service Management, GLPI, Freshservice, etc.).
- Base de Conocimiento (Knowledge Base - KB): Repositorio de soluciones extraídas para problemas frecuentes. Las permite para que los técnicos de Nivel 1 puedan resolver problemas

complicados a partir de guías de solución, también asegurando la consistencia (Consortium for Service Innovation, 2017).

- Registros de Escalamiento: (Evidente de cuándo y por qué el ticket cambió de un Nivel 1 (Help Desk) a un Nivel 2 (Technical Help) o Nivel 3 (Suppliers/Development)).

1.20.5 Evaluación del servicio

La calidad percibida es un concepto subjetivo pero medible.

- Encuestas CSAT (Customer Satisfaction Score): Encuesta enviada automáticamente al cerrar un ticket (ej. "¿Cómo calificaría la atención? de 1 a 5 estrellas").
- Modelo SERVQUAL: Primer modelo académico propuesto para medir la diferencia entre la expectativa de un usuario y su percepción específica del servicio recibido como tal. Mide 5 dimensiones: fiabilidad, capacidad de respuesta, seguridad, empatía y elementos tangibles (Parasuraman y otros, 1988).
- Aplicación en tesis: se adapta muy bien a buscar correlaciones entre el soporte tecnológico y la satisfacción del estudiante en tu estudio.

1.21 Norma 410-14 monitoreo y evaluación de servicios tecnológicos

El monitoreo y evaluación de forma continua son procesos que permiten observar cómo se comportan los sistemas de forma continua con el fin de detectar anomalías, medir el rendimiento y planificar la capacidad a futuro. Para NIST SP 800-137, el monitoreo continuo es vital para poder

mantener de forma continua una consciencia situacional de la seguridad y operatividad de la infraestructura (Dempsey y otros, 2011).

1.21.1 Indicadores operativos

Para evaluar la salud de los servicios tecnológicos, en la industria se ha adoptado el framework de las "Cuatro Señales de Oro" (Four Golden Signals) de Google en su disciplina de SRE.

1. **Latencia:** El tiempo que tarda en responder el sistema ante una solicitud. Una latencia alta en el portal estudiantil va de la mano con la insatisfacción del usuario (Beyer y otros, 2016).
2. **Tráfico:** Se refiere a la demanda que recibe el sistema (ej. solicitudes HTTP por segundo o transacciones de base de datos).
3. **Errores:** La cantidad de solicitudes que fallan (ej. Errores HTTP 500).
4. **Saturación:** El estado de que tan "lleno" está el sistema (ej. uso de CPU al 95% o memoria RAM al límite).

1.21.2 Modelo de monitoreo continuo

La supervisión no es una actividad estática, sino un ciclo de vida. El modelo ISCM (Information Security Continuous Monitoring) define una planificación de 3 niveles:

- Nivel de Organización: Define las métricas de riesgo y de gobernanza.
- Nivel de Proceso: Supervisar la arquitectura y los flujos de trabajo.

- Nivel de Sistema: el muestreo técnico de logs y eventos de servidores y REDES (Dempsey y otros, 2011).

El propósito es transformar el modelo "Reactivo" (actuar una vez se produce la avería) a uno "Proactivo" (anticiparse a la avería antes de que la detecte el usuario).

1.21.3 Evidencias de trazabilidad

El objetivo de la auditoría es comprobar que el monitorio da pie a la creación de logs inalterables (análisis forense) que nos permitan volver atrás y reconstruir eventos pasados.

- Logs Centralizados: Arboles de logs que hay que hacer llegar a un servidor seguro (Syslog server) impidiendo la manipulación local de los logs.
- Informes de Disponibilidad (Uptime Reports): Se trata de documentos generados automáticamente que verifican (por ejemplo) que un "Aula Virtual" ha estado 99.9% disponible a lo largo de un mes (SLA Compliance).
- Análisis de Causa Raíz (RCA): Documento formal generado tras una caída crítica en el servicio que presenta qué es lo que ha fallado, por qué ha ocurrido aquello y qué se llevó a cabo para evitar la repetición del mismo (Limoncelli y otros, 2014).

1.21.4 Herramientas de monitoreo

La exigencia de monitorizar a mano dado el gran tamaño de las redes universitarias (no es conveniente emplear esto) da lugar a la aparición

de herramientas que podemos clasificar en herramientas de infraestructura y de aplicaciones.

- NMS (Network Monitoring Systems): Herramientas como Nagios, Zabbix o PRTG que a través de Ping/SNMP son capaces de verificar que todos los dispositivos están "vivos" (Stallings, 2016).
- APM (Application Performance Monitoring): Herramientas como New Relic o Dynatrace que miran dentro del código y son capaces de verificar qué consulta a base de datos está provocando la lentitud del sistema.
- SIEM (Security Information and Event Management): plataformas como Splunk que correlacionan eventos de seguridad cuando los detectan como ataques y crean eventos de seguridad (Miller y otros, 2021).

1.21.5 Matriz de debilidades frecuentes

En la evaluación el auditor suele frecuentemente encontrar falencias recurrentes en la estrategia de monitorio. La Tabla 8 ilustra la matriz de debilidades que se han detectado en el proceso de supervisión y de gestión de los servicios de TI. Su objetivo es poner de manifiesto el impacto que determinadas fallas de funcionamiento tienen sobre la calidad del servicio, así como proporcionar recomendaciones de auditoría para mitigar los riesgos, aumentar la observabilidad y cumplir con la normativa en la organización.

Tabla 8. Ejemplo de matriz de debilidades

Debilidad Detectada	Impacto en el Servicio	Recomendación de Auditoría
Fatiga de Alertas	Los administradores ignoran las alertas críticas porque reciben miles de correos irrelevantes al día ("Ruido").	Implementar umbrales inteligentes y agrupar alertas (Beyer et al., 2016).
Monitoreo en Silos	Redes monitorea switches y Desarrollo monitorea Apps, pero nadie tiene la visión completa del servicio.	Implementar tableros (Dashboards) unificados de servicio integral.
Puntos Ciegos (Blind Spots)	Se monitorea el servidor, pero no la experiencia del usuario final (el servidor funciona, pero la web no carga).	Implementar monitoreo sintético (robots que simulan ser alumnos navegando).
Retención Insuficiente	Los logs se borran cada 24 horas por falta de espacio en disco.	Establecer políticas de retención de logs de mínimo 90 días por cumplimiento legal (ISACA, 2019).

Fuente: ISACA, (2019)

Nota: Ejemplo de matriz de debilidades en el proceso de supervisión y de gestión de los servicios de TI

La matriz muestra cuatro debilidades complejas. La fatiga con las alertas hace que los administradores terminen ignorando alertas críticas, ya que están saturados de correos irrelevantes, lo que aumenta el riesgo de perder eventos de alta importancia; la recomendación es la de incluir umbrales inteligentes y de agrupar las alertas por familias. El monitoreo en silos pone en evidencia que cada área supervisa solamente su entorno

(redes, aplicaciones, etc.), generando una falta de visibilidad de la calidad y del estado del servicio; para solucionarlo se recomienda acudir a dashboards que permitan unificar la supervisión de la calidad y del estado de todos los servicios de TI bajo una única vista. Los puntos ciegos (blind spots) comprometen la visibilidad de este, ya que solamente se supervisa el servidor, pero no se tiene en cuenta la experiencia del usuario final, ocultando potenciales problemas de navegación y de desempeño.

La recomendación es revisar la implementación de un enfoque de monitoreo sintético utilizando robots para simular la actividad de los usuarios finales. Por último, dado el fenómeno de la retención insuficiente de logs debido a la falta de espacio, se aconseja establecer una política de retención de logs mínima de al menos 90 días para cumplir con requerimientos legales y de auditorías internos. En síntesis, las debilidades son una clara manifestación de que hay que incrementar la madurez de la gestión de la supervisión del servicio de TI, aumentar la visibilidad del mismo y optimizar la madurez operativa de los servicios de TI.

1.22 Norma 410-15 portal web, intranet y servicios telemáticos

Este dominio examina la gestión, la usabilidad y la seguridad de los canales digitales de la organización (Página Web Institucional, Intranet docente/alumno y Campus Virtual). Tiene como finalidad garantizar que los servicios ofrecidos sean accesibles, útiles y que se alineen con la estrategia de comunicación institucional (Laudon & Traver, 2021).

1.22.1 Indicadores de gestión del portal

Sería inútil tener una página web sin ser evaluada, por lo que los indicadores deben tener que ver con la experiencia del usuario (UX) y con la utilidad de la información.

- Tasa de rebote (Bounce Rate): Porcentaje de visitas que entran al portal web y salen de él sin interactuar. Una tasa de rebote que sea alta (>60-70%) en la página de "Admisión" o en la de "Matrícula" da la siguiente información: o bien el estudiante que visita esta página no ha hallado lo que buscaba o bien el diseño es poco amigable para el usuario (Kaushik, 2013).
- Tiempo de permanencia: Es el tiempo medio que un usuario pasa en el sitio web.Efectuando la lectura de tiempos de acceso muy bajos en la página del "Repositorio de Tesis", en el contexto de un ambiente académico, se puede suponer que, la información no suponga una determinada evolución laxista y que su contenido sea irrelevante.
- Tasa de conversión (Micro-conversiones): porcentaje de personas que llevan a cabo una determinada acción deseada (ej., descargar el sílabo, realizar una pre-matrícula, reservar un libro).
- Disponibilidad del servicio (Uptime): porcentaje de tiempo al que está activo el portal.

$$Disponibilidad = \frac{\text{Tiempo Total } - \text{Tiempo Caída}}{\text{Tiempo Total}} x100$$

1.22.2 Estándares de accesibilidad

Las universidades públicas tienen la responsabilidad ética y legal de hacer disponibles sus servicios a las personas con defectos (visuales, de movilidad o cognitivos).

- WCAG 2.1 (Web Content Accessibility Guidelines): Estándar internacional del W3C. Se fundamentan en cuatro principios (POUR):
- Perceptible: La información no puede ser invisible para los sentidos (ej. texto alternativo en imágenes para lectores de pantalla).
- Operable: La interfaz debe poder manejarse solo con teclado (sin mouse).
- Comprensible: El lenguaje tiene que ser claro y la navegación predecible.
- Robusto: compatible con tecnologías de asistencia futuras (W3C, 2018).
- Validación: Con el uso de herramientas automatizadas (en particular WAVE y Google Lighthouse) para auditar el cumplimiento de los niveles A, AA o AAA.

1.22.3 Evidencias obligatorias

Para la auditoría de conformidad, debe haber evidencias documentales de que existe la gobernanza del contenido web.

- Política de publicación web: Documento que establece quién puede publicar noticias o modificar fechas en el calendario académico de modo que evita las publicaciones no oficiales.

- Mapa del sitio (sitemap): Representación jerárquica de la arquitectura de la información con fines de comprobar que no haya secciones muy relevantes que pudieran quedar "huérfanas" (ser las únicas que no poseen ningún enlace) (Rosenfeld y otros, 2015).
- Registros de mantenimiento de contenidos: Bitácora donde se comprueba la revisión periódica de la información estática (ej. comprobar que la lista de las autoridades universitarias está vigente).
- Informe de cumplimiento de transparencia: En el caso de entidades públicas (Perú), evidencia de cómo ha sido homologado el "Portal de Transparencia Estándar" (PTE).

1.22.4 Lista de verificación de contenido

Una checklist para controlar y garantizar la calidad del contenido antes de ser publicado; los errores aquí tienen un efecto directo sobre la credibilidad institucional.

- [ ] Enlaces rotos (link rot): Enlaces Rotos (Link Rot): Se usa alguna herramienta para detectar los enlaces que conducen a una página “404 Not Found”? (Nielsen, 2011).
- [ ] Adaptabilidad móvil (responsive design): ¿El portal se visualiza y se comporta correctamente en dispositivos móviles? (Hoy, más del 70% de los estudiantes acceden desde smartphone).
- [ ] Fechas de vigencia: ¿Las convocatorias antiguas, las programaciones de semestres pasados, se han retirado o archivad para no generar confusión al alumno?

- [ ] Información de contacto: ¿Cada facultad, o sus departamentos, tienen un correo y un teléfono que funcionen y que sean claramente visibles?

1.22.5 Riesgos operativos

Riesgos específicos asociados a la presencia digital de la universidad. En la Tabla 9 se expresan los riesgos más relevantes asociados al estar presente digitalmente en el seno de una universidad, sobre todo, en lo que concierne a la institución web misma y a las plataformas de información. La finalidad es la de determinar las amenazas concretas (comunes) que afectan a la satisfacción de los usuarios y a la imagen institucional, así como también la de comprender en qué manera los riesgos, podrían impactar los procesos académicos-administrativos.

Tabla 9. Riesgos específicos asociados a la presencia digital en la Universidad

Riesgo	**Descripción**	**Impacto (Satisfacción/Imagen)**
Defacement (Desfiguración)	Ciberataque que cambia la apariencia visual de la web (ej. poner banderas o mensajes políticos).	Alto: Daño reputacional severo y sensación de inseguridad.
Información Desactualizada	Publicar cronogramas de matrícula erróneos o antiguos.	Crítico: Estudiantes pierden plazos, generando quejas y trámites manuales.
Saturación en Picos	Caída del portal durante la publicación de resultados de admisión o matrícula.	Alto: Estrés en los usuarios y percepción de incompetencia técnica.

Fuente: Nielsen, (2011)

Nota: Riesgos más relevantes asociados al estar presente digitalmente en la universidad

En la matriz observamos tres riesgos relevantes. El mauro o defacement del website es considerado un ataque de alto impacto, ya que afecta a la imagen oficial y produce una fuerte afectación reputacional, además de la inseguridad que transmite a la comunidad universitaria. Por otro lado, la información desactualizada de los cronogramas correspondientes a la matrícula o procesos académicos de la universidad, se considera un riesgo de alto nivel, puesto que puede llegar a ocasionar la deserción de estudiantes por no haber prestado atención a un importante plazo que terminó, generando quejas, retrasos, aumento de la carga operativa.

De tal forma, la saturación en los picos de demanda cuando se publican los resultados de admisión o matrícula provocan caídas del portal de manera que se percibe menos eficiente a nivel técnico y, al ser un riesgo de alto impacto, produce frustración en los usuarios y un deterioro de la confianza en los servicios digitales institucionales. En resumen, la tabla pone de relieve la urgencia de que la universidad mejore el refuerzo de la seguridad web, que sea más cuidadosa en la actualización de los contenidos de la página web y que adapte una infraestructura capaz de soportar los picos de uso.

1.23 Norma 410-16 capacitación en tecnologías de la información

La capacitación (de TI) no es exclusiva para el personal técnico; hace parte del desarrollo de la competencia digital de toda la organización

para que esta pueda hacer un uso competente de los recursos tecnológicos que tiene a su disposición. La norma ISO 10015 (Gestión de la calidad: Directrices para la gestión de la competencia y el desarrollo de las personas) establece que la organización debe determinar la competencia que necesita y formar para cerrar las carencias existentes (International Organization for Standardization ISO, 2019).

1.23.1 Indicadores de capacitación

La capacitación debe medirse para que se considere una inversión y no un gasto. El modelo más aceptado en este ámbito es el de Kirkpatrick que estudia los cuatro niveles, aunque en auditoría operativa suele realizarse el análisis correspondiente únicamente a los niveles 1 y 2 y el de las métricas de cobertura.

- Horas de capacitación por empleado: Indicador del promedio de horas anuales dedicadas a la formación tecnológica.
- Cobertura del plan anual: Número de personales que realizaron los cursos obligatorios que valoramos (ej. "Uso del Aula Virtual" para docentes).
- Nivel de aprobación: Porcentaje de los participantes que superan la evaluación final con nota satisfactoria.
- Reducción de tickets de soporte (nivel 4 - impacto): Porcentaje de los participantes que superan la evaluación final con nota satisfactoria (Kirkpatrick & Kirkpatrick, 2016).

1.23.2 Matriz de necesidades

No se debe formar "a ciegas". El DNC se encarga de cruzar el perfil del puesto con las herramientas tecnológicas que requiere. Ejemplo de matriz para universidad, la Tabla 10 incluye la matriz de evaluación de las competencias digitales adecuadas a distintas familias y perfiles de puesto en la Universidad. Se ha pensado en una matriz que permita identificar, en primer lugar, el nivel de competencias digitales deseables en cada uno de los puestos individuales; en segundo lugar, el nivel de competencias digitales que presenta el personal; y, en tercer lugar, el nivel de brechas (GAP) existente, que permita definir un conjunto de acciones formativas dirigidas a fortalecer las capacidades de la institución.

Tabla 10. Ejemplo de matriz para la Universidad

Perfil de Puesto	**Herramienta Crítica**	**Nivel Requerido**	**Nivel Actual (Promedio)**	**Brecha (GAP)**	**Acción Formativa**
Secretaria Académica	Sistema ERP (Módulo Matrículas)	Avanzado	Básico	Alta	Curso taller intensivo de ERP
Docente Tiempo Completo	Moodle / Teams	Avanzado	Avanzado	Nula	Actualización opcional
Tesorería	Excel / Power BI	Intermedio	Intermedio	Media	Curso de Macros y Dashboards

Fuente: Elaboración propia del autor

Nota: En base a las brechas de la universidad como ejemplo de matriz

La matriz permite observar claramente las diferencias existentes entre el nivel de competencias digital requerido con el nivel de competencias digitales existente. En el caso de la Secretaría Académica, hemos podido observar que existe una brecha muy alta, ya que el perfil del puesto, que demanda un nivel avanzado en el uso del sistema ERP para matrículas, es contrastado con el nivel cognitivo del personal, que se encuentra en un nivel básico. Por lo que la recomendación es establecer un curso intensivo que permita obtener el dominio de la herramienta.

Para el personal docente a tiempo completo, no se detecta ninguna brecha porque el nivel requerido y el nivel existente en Moodle y Teams son iguales (avanzado). Por lo que se recomienda una autoformación para poder realizar una actualización opcional de las herramientas y sus nuevas funcionalidades. En el caso de Tesorería existe una brecha media en Excel y Power Bi, ya que si bien el nivel requerido (intermedio) es igual al nivel existente (intermedio), existen ámbitos de mejora que son visibles. La reccomendación es realizar un curso que permita obtener un buen nivel de competencias digitales en el uso de Macros y Dashboards para ayudar a la mejora del proceso de gestión financiera. En su conjunto, la tabla muestra necesidades de formación concretas, y permite la priorización de acciones formativas.

1.23.3 Evidencias de capacitación

La formación de la que se da cuenta en la auditoría tiene que ser trazable; sin trazabilidad no existe preparación formal.

- Plan Anual de Capacitación (PAC): La formación de la que se da cuenta en la auditoría tiene que ser trazable; sin trazabilidad no existe preparación formal.
- Listas de asistencia: Registros firmados (en papel o digitales) donde se puede revisar la participación.
- Sílabos o contenidos: Registros firmados (en papel o digitales) donde se puede revisar la participación.
- Certificados: Documentos que acreditan la competencia adquirida.

1.23.4 Evaluación de competencias digitales

Aquí se evalúa la competencia digital general, más allá de una capacitación especial, el marco de referencia europeo DigComp 2.2 es la norma académica para ello.

Áreas de competencia:

1. Alfabetización en información y datos.
2. Comunicación y colaboración.
3. Creación de contenidos digitales.
4. Seguridad.
5. Resolución de problemas (Vuorikari y otros, 2022).

Evaluación pre y post: Aplicar un test diagnóstico antes de la formación y uno final para evaluar la ganancia de aprendizaje (Learning Gain).

1.23.5 Seguimiento del desarrollo del personal

La formación es un proceso que se alarga (*Lifelong Learning*).

- **Historial de capacitación (kárdex):** Registro individual en el sistema de RRHH donde figuran todos los cursos tecnológicos realizados por el empleado.
- **Encuestas de eficacia (post-capacitación):** Evaluación que se hace 3 o 6 meses después de la formación al jefe inmediato preguntando, ¿El empleado pone en práctica lo que ha aprendido en su trabajo diario? (Noe, 2017).

1.24 Norma 410-17 firmas electrónicas en la administración pública

La incorporación de firmas electrónicas y digitales constituye la base de la digitalización en el ámbito público. Permitiendo garantizar, en consecuencia, la autenticidad (identidad del firmante), la integridad (el documento no ha sufrido modificaciones) y el no repudio (el firmante no puede renegar el hecho de haberlo firmado) de los actos administrativos (Presidencia del Consejo de Ministros, 2019).

1.24.1 Indicadores de uso

La medida de uso, a través de la firma electrónica, nos permite conocer hasta qué punto se avanza en la política de cero papel.

- **Tasa de adopción digital:** Porcentaje de documentos oficiales (resoluciones, memorandos) emitidos digitalmente respecto a lo que ha sido el total emitido.

$$Tasa = \frac{\text{Docs. FirmadosDigitalmente}}{\text{Docs. Totales}} x\ 100$$

- **Ahorro de costos operativos:** Valoración financiera en ahorro en papel, tóner, almacenamientos físicos y horas-hombre de mensajería (United Nations, 2020).
- **Tiempo de tramitación:** Reducción en el tiempo medio en la aprobación de un expediente (ciclo de firma) en el flujo del físico (flujos f) frente al flujo digital.

1.24.2 Evidencias de implementación

De forma paralela a la auditoría, habrá de comprobarse que la firma no es sólo un dibujo que se pega en un PDF (firma digitalizada), sino que se trata de una firma válida, en clave criptográfica.

- Acreditación de la Autoridad de Certificación (CA): Contratos en vigor con entidades acreditadas (en Perú la RENIEC de funcionarios públicos) para la emisión de certificados digitales.
- Software de firma (cliente de firma): Evidencia del software que se utilizó para firmar (ej. ReFirma, Adobe Sign) y cómo se integra al sistema de gestión documental (SGD).
- Políticas de uso de certificados: Documento normativo interno en el cual queda prohibido que los funcionarios compartan la clave privada o el token físico (ISO/IEC, 2013).

1.24.3 Lista de control

Con el fin de conseguir la contrapartida de la validez legal del acto administrativo, es necesario que el funcionario cumpla por lo menos ciertos requisitos técnicos que deben llevar a la validez legal.

- [ ] Vigencia: ¿El documento con la firma electrónica hecha, presenta el certificado de la persona interviniente en su estado de invalidado (o sea, vigente) en el momento de ejecutar la firma?
- [ ] Modulo seguro: ¿La clave privada utilizada para la aplicación de la firma se guarda en un módulo criptográfico seguro (o sea, Tarjeta inteligente o Token USB) y no se encuentra en un archivo del escritorio del ordenador?
- [ ] Sello de tiempo (timestamping): El documento tiene aplicado un sello de tiempo oficial certificador el instante y la hora en que se ejecuta la firma, cosa que no usa el reloj del ordenador? (ETSI, 2016).
- [ ] Validación LTV (Long Term Validation): el formato de firma permite realizar dicha validación del documento para el futuro para cuando el certificado original ya no sea válido?

1.24.4 Verificación de certificados

El proceso técnico para asegurar que una firma es válida consiste en la ejecución de las consultas criptográficas.

- Listas de Revocación (CRL): La consulta del pasaporte tiene que ser automática a la hora de la revocación del certificado (por pérdida o robo del token de certificación) en el momento de ejecutar la firma.

- Protocolo OCSP (Online Certificate Status Protocol): Protocolo para la verificación del estado del certificado digital. Esta verificación se hace en tiempo real y contra los servidores de la entidad emisora de este (Santoso y otros, 2017).
- Integridad del Hash: El sistema receptor vuelve a calcular el hash (o sea, resumen) del documento y lo compara con características del hash que esté cifrado en la firma, si cambia sólo un bit en el documento, la firma será declarada automáticamente inválida.

1.24.5 Riesgos del uso incorrecto

El uso inadecuado de la identidad digital puede conllevar riesgos legales muy graves y administrativos. En la Tabla 11 se encuentra un ejemplo de uso inadecuado de la identidad digital hace alusión a la multitud de riesgos asociados a la digitalización de los procesos de firma, que pueden llegar a comprometer la validez legal o la seguridad de los actos administrativos. Clasifica los problemas en tres grandes grupos: operativos, tecnológicos y procedimentales, indica el impacto que tienen (crítico o alto) y menciona algunas medidas de control que permitieran mitigar la falta de control en su caso.

Se considera este análisis fundamental para aceptar que la mala gestión de las credenciales, el uso de tecnología obsoleta y el desconocimiento de lo que implica desde un punto de vista legal puede llegar a causar la invalidación de una firma digital y, en consecuencia, el dejar sin efecto el no repudio y la autenticidad que está asociado por lo general con la firma digital.

Tabla 11. Ejemplo del uso inadecuado de la identidad digital

Riesgo Identificado	Descripción	Impacto	Control Sugerido
Préstamo de Credenciales	El jefe entrega su token y clave a la secretaria para que "firme por él".	Crítico: Repudio legal y nulidad de actos administrativos.	Auditoría de logs (verificar si se firmó cuando el jefe estaba de vacaciones).
Obsolescencia de Algoritmos	Firmar usando algoritmos antiguos y vulnerables (ej. SHA-1) en lugar de actuales (SHA-256).	Alto: Posibilidad de falsificación técnica.	Actualización forzada del software de firma.
Firma Digitalizada (Scan)	Pegar la imagen de la firma manuscrita creyendo que tiene validez legal digital.	Crítico: Documento sin valor probatorio en entorno digital (facilidad de copia).	Capacitación obligatoria sobre la Ley 27269 (Perú).

Fuente: Santoso y otros, (2017)

Nota: Adaptado a la Ley 27269 como ejemplo de la mala gestión de la identidad digital

El primer grupo de riesgos este se focaliza en la mala gestión de las credenciales, en la aplicación de la normativa legal. La práctica llamada "Préstamo de Credenciales" se considera un riesgo alto, puesto que prestar un token personal a un tercero (ej: una secretaria) destruye el principio de no repudiar de la firma digital. En este sentido, la forma de controlar el riesgo es mediante la auditoría de logs, donde es posible

demostrar que el firmante no controlaba su identidad al realizar la acción. Por otro lado, el procedimiento de "Firma Digitalizada (Scan)", que se convierte sólo en una imagen sin ningún soporte cripto, tiene un impacto alto, dado que el documento carece de valor probatorio. La solución para este tipo de casos pasa por la formación obligada del personal en la legislación sobre firma y el carácter personal e intransferible de la clave privada.

El segundo bloque se refiere al riesgo tecnológico por obsolescencia. La obsolescencia de algoritmos es un riesgo que se asocia a la práctica de crear hashes utilizando funciones de hashing poco robustas (ej: SHA-1) en vez de los algoritmos correctos para ello (ej: SHA-256). El riesgo tiene un impacto alto porque se puede llegar a falsificar técnicamente el documento manipulando la función criptográfica subyacente. El control sugerido es meramente técnico y obliga a la actualización del software de firma para garantizar que solo se utilicen algoritmos robustos y actualizados y al mismo tiempo se mantenga la integridad criptográfica y la fiabilidad de las transacciones digitales.

CAPÍTULO II

2 ETAPA 3: EVALUACIÓN Y CALIFICACIÓN DEL CUMPLIMIENTO

El presente capítulo establece la metodología del estudio y la aplicación operativa de la auditoría informática en la Universidad Nacional Autónoma de Chota (UNACH). Después del capítulo anterior donde se establece el marco regulatorio y los estándares técnicos basados en referencias internacionales como COBIT, ISO 27001 e ITIL, este capítulo se refiere a la contrastación empírica de los modelos teóricos con la realidad operativa de la institución. El objetivo de esta fase del estudio está enfocado en recoger, analizar y validar las evidencias objetivas necesarias para llegar a un diagnóstico del grado de madurez de los procesos tecnológicos y de la prestación del servicio educativo y sobre la satisfacción del estudiante, de acuerdo con los principios de integridad y el debido cuidado profesional exigido por la norma de auditoría (International Organization for Standardization ISO, 2018).

Conforme a la metodología, el presente capítulo se estructura en una serie de fases cuyos extremos oscilan entre la planificación del trabajo de campo hasta la calificación técnica de los hallazgos. En este sentido, se da cuenta del propio despliegue de los elementos de recolección de datos –listas de verificación (checklists), revisión de la documentación y entrevistas con personas clave-, aplicando para ello técnicas de triangulación con el fin de garantizar la consistencia de los hallazgos. En este desarrollo sistemático se pretende insertar el propio objetivo de identificar las desviaciones o "brechas" existentes conforme a la

normativa aplicable, dimensionar los riesgos asociados y establecer las acciones correctivas necesarias, lo que a la par proporciona soporte y sobresaturación cuantificable para el dictamen derivado de la auditoría en cuestión (Whittington & Pany, 2020).

2.1 Evaluación norma por norma

Normativa por normativa significa contrastar sistemáticamente la realidad operativa identificada con aquellos principios que son establecidos como la base de la auditoría, es decir, el contenido del Marco Teórico. En términos de la norma ISO 19011:2018 (Directrices para la auditoría de los sistemas de gestión), el auditor debería evaluar entonces la evidencia objetiva para determinar la medida en la que se cumplen los requisitos del criterio de auditoría (International Organization for Standardization ISO, 2018).

- Metodología de análisis de brechas (gap analysis): se analiza cada control (p. ej. "1.12.1 Indicadores de clasificación") bajo tres dimensiones:

1. Diseño: ¿El control existe en papel/política?
2. Implementación: ¿El control se aplica realmente en el día a día?
3. 3Efectividad: ¿El control mitiga el riesgo para el que estaba diseñado?

Para los fines de esta investigación en la UNACH se aplica una metodología de análisis de brechas (gap analysis) que desprende cada uno de los controles (por ejemplo, indicadores de clasificación de la información), bajo esta tríada evaluativa:

1. **Diseño (existencia formal):** se pregunta si el control existe o no, se pregunta si el control existe documentado o político. La universidad posee normativa aprobada y vigente que regula dicho proceso. Si no existe dicho diseño tenemos un vacío normativo esencial.
2. **Implementación (aplicación real):** Se comprueba si el control diseñado se realiza realmente en la operatividad cotidiana. Un control puede estar perfectamente descrito en un manual, pero ser ignorado tanto por el personal de TI, como por el administrativo.
3. **Efectividad (mitigación del riesgo):** se establece si el control puesto en marcha cumple con su función, la de mitigar el riesgo para el cual fue creado. Esta resulta ser la dimensión más crítica, dado que aporta la medición del resultado funcional desde el control sobre la seguridad y calidad del servicio dado, que se ha medido en su procesamiento.

2.2 Tabla de cumplimiento general

Para que la evaluación sea objetiva y se pueda hacer futuras comparaciones, se introduce un modelo de madurez, en especial se recomienda adaptar la escala de capacidad de COBIT 2019 que les otorga un valor numérico a los niveles de implantación de los procesos de TI (ISACA, 2019).

A continuación, se presenta, la tabla 12, la cual ofrece una propuesta operacional de una escala de valoración que permite medir el grado de madurez de la gestión de los procesos de la organización, así como una metodología que clasifica el estado de la gestión en seis niveles

jerárquicos, del 'nivel 0: inexistente' al 'nivel 5: optimizado'. En cada uno de los niveles jerárquicos se incorpora una descripción cualitativa (de los hallazgos esperados) así como un rango porcentual de cumplimiento asignado que permite emitir un diagnóstico objetivo, estandarizado y arbitrado sobre la capacidad actual de la organización para llevar a cabo sus operaciones.

Tabla 12. Escala de valoración de madurez de procesos (propuesta)

Nivel	**Estado de Madurez**	**Descripción del Hallazgo**	**% Cumplimiento Asignado**
0	Inexistente	El proceso no existe o no se aplica en absoluto.	0%
1	Inicial / Ad Hoc	El proceso es desorganizado, reactivo y depende de iniciativas individuales.	1%-20%
2	Repetible	Se sigue un patrón regular, pero no está formalmente documentado.	21%-40%
3	Definido	El proceso está documentado, estandarizado y comunicado a la organización.	41-60%
4	Administrado	El proceso se mide y controla mediante indicadores (KPIs).	61%80%
5	Optimizado	El proceso se mejora continuamente basándose en métricas y buenas prácticas.	81%-100%

Fuente: COBIT, (2019)

Nota: Escala de evolución de gestión improvisada y profesional

El análisis de la escala que propone la Tabla 12 pone de manifiesto una evolución clara entre una gestión improvisada y una gestión profesionalizada. En los momentos iniciales de una organización (Niveles 0, 1 y 2), nos encontramos ante un espacio donde los procesos son no existentes o "explotan" de forma excesiva de la propia iniciativa que solo se deja llevar ("Ad Hoc") hasta llegar a un cumplimiento que no sobrepasa el 40%. La variación relevante se produce en el Nivel 3 (Definido), donde la documentación y la estandarización ponen un punto y final a la informalidad, estableciendo un soporte donde los procesos se pueden comunicar a la organización y se puede pasar a un funcionamiento más predecible.

Por el contrario, la excelencia operativa se centra en los niveles más altos (4 y 5) donde la perspectiva cambia desde la mera actuación a la actuación mediante el control y la mejora del desempeño alineado. En el Nivel 4 (Administrado), se añade el uso de indicadores clave (KPIs) para evaluar el desempeño, mientras que el Nivel 5 (Optimizado) representa el máximo estado de madurez, con un cumplimiento situado entre el 81% y el 100%. Lo que significa que la organización no solo controla lo que hace, sino que se vale de las métricas y de las buenas prácticas para implantar la mejora continua, garantizando la sostenibilidad y eficiencia del sistema de gestión a lo largo de los años.

Finalmente, la inclusión de los rangos porcentuales de cumplimiento asignado (desde el 0% al 100%) le otorga un carácter pragmático a esta escala que supera la mera descripción teórica. La cuantificación de estados que habitualmente son subjetivos, como "desorganizada" o

"definida", que permite a la propuesta poder amortiguar la ambigüedad en las auditorías internas.

Este doble carácter cualitativa y cuantitativa permite la identificación precisa de las brechas del desempeño (gap analysis) que permite la gerencia no solo ubicar el estado actual de sus procesos sino, en torno a este, edificarse una hoja de ruta con hitos que se vuelven medibles para poder avanzar al siguiente nivel de madurez.

2.3 Identificación de desviaciones

Una desviación es el incumplimiento de un requisito normativo o técnico. En auditoría no todas las fallas tienen la misma valía, para la norma ISO/IEC 17021-1, las desviaciones deben ser consideradas a partir del grado de severidad, tal y como el impacto en la calidad del servicio (International Organization for Standardization ISO, 2015).

- **No conformidad mayor (NC+):** Ausencia total de un control crítico o una falla sistemática que afecta la integridad de los datos o la continuidad y disponibilidad del servicio. Un ejemplo claro sería la falta de copias de seguridad de los registros académicos, lo que provocaría la pérdida de continuidad del negocio.
- **No conformidad menor (NC-):** Refiere a una anomalía puntual o esporádica que no compromete la estructura global del sistema de gestión. Por ejemplo, un acta de reunión técnica sin firma no anula el conjunto de procesos, pero manifiesta la ausencia de disciplina administrativa.

- **Oportunidad de mejora (OBS):** Se da en el caso de que, aunque el control cumple con la norma vigente, disponemos de mecanismos para ejecutarlo de una forma más eficiente, más económica o mediante tecnología de más avanzada. Este tipo de oportunidades aportará valor añadido a la gestión institucional.

2.4 Priorización de debilidades

Tengamos en cuenta que los recursos de la universidad son escasos y es por ello por lo que habrá que elegir que corregir primero. Se aplica el enfoque basado en riesgos que describe NIST SP 800-30, procediendo a calcular la prioridad en función de la probabilidad y del impacto en la institución (Joint Task Force Transformation Initiative, 2012).

Matriz de priorización: $Nivel\ de\ riesgo = Probabilidad\ x\ Impacto$

- **Prioridad alta (crítico):** Hallazgos que a su vez ponen en peligro la seguridad de la información (Ley 29733) o afectando directamente la operatividad académica. Se requieren correcciones a realizar en un plazo de < 30 días.
- **Prioridad media:** Hallazgos que contribuyen a la reducción de la eficiencia administrativa, pero no paralizan la universidad. Se tienen que corregir en un periodo de < 6 meses.
- **Prioridad baja:** Hallazgos de tipo documental o de forma. Se corrigen según la disponibilidad de presupuesto.

2.5 Validación técnica de hallazgos

Antes de repetir los resultados en el informe final, resulta imprescindible validar la adecuación técnica de los hallazgos para no incurrir en errores de interpretación.

- **Triangulación de evidencias:** Técnica metodológica que consiste en probar con tres fuentes de datos que nos dicen lo que el personal muestra (entrevista), lo que el personal hace (observación) y lo que está escrito (documentación), toda esta técnica aporta la validez científica a la auditoría (Denzin, 2012).
- **Reunión de cierre técnica:** Congreso de trabajo con las personas responsables de TI (jefes de Soporte, Administradores de Red) para comunicarles los hallazgos preliminares, y obtener sus descargos o aclaraciones técnicas antes de elevar este último informe al rectorado.

CAPÍTULO III

3 ETAPA 4: IDENTIFICACIÓN Y CLASIFICACIÓN DE HALLAZGOS

El presente capítulo constituye la fase analítica y conclusiva del trabajo de campo de la auditoría informática, en la cual se identifica, clasifica y valora los hallazgos de la evaluación operativa de la actividad realizada en la etapa anterior. Hecho el trabajo con los instrumentos de recolección de datos, tales como listas de verificación, entrevistas y revisiones de documentos, esta fase tiene como objetivo someter la evidencia empírica a un proceso de depuración y síntesis inferencial, pero ahora para determinar técnica y certeramente las desviaciones existentes entre la realidad operativa de la Universidad Nacional Autónoma de Chota (UNACH) y la criterios normativos.

Conforme a lo que establece la Teoría de la Evidencia de Auditoría, un proceso que nos permite, a partir de una información desagregada, formular un juicio profesional no arbitrario en la trata básica de una observación que se encuentra documentada, dado que cada observación que está documentada puede ser revisada en su suficiencia, su pertinencia y sus competencias para poder sustentar el diagnóstico profesional de la madurez tecnológica institucional y su correlato de causalidad con la calidad del servicio educativo (Arens y otros, 2017; International Organization for Standardization ISO, 2018).

Igualmente, para poder establecer la jerarquía de los hallazgos se utiliza la metodología que la Auditoría Basada en Riesgos (Risk Based Audit) y los estándares de gestión de riesgos corporativos COSO ERM ayuda

a desarrollar. Este planteamiento, especialmente el último, hace que se pueda pasar de tener simplemente una relación de incumplimientos a la evaluación de la materialidad de cada desviación valiéndonos de su potencial impacto en el cumplimiento de los objetivos estratégicos que la universidad tiene marcados comenzando por distinguir riesgos inherentes y riesgos residuales.

De este modo, las deficiencias se clasifican en función de su gravedad desde las observaciones de la administración hasta las no conformidades mayores, lo que sugiere una priorización que no solo pone de manifiesto la vulnerabilidad de los activos de información, sino que también explica cómo estas brechas tecnológicas tienen un impacto directo en la satisfacción del estudiante y en la continuidad de las operaciones académicas, de acuerdo con los principios de objetividad y debido cuidado profesional exigidos por las normas internacionales (The Institute of Internal Auditors, 2017; Whittington & Pany, 2020).

3.1 Tipos de hallazgos

La La clasificación de los hallazgos en esta investigación va más allá de la simple dicotomía de "cumplimiento" versus "incumplimiento". Se utiliza una taxonomía basada en la premisa de Materialidad (definida en la NIA 320), entendiendo que una desviación es material si su ocurrencia puede influir razonablemente en las decisiones económicas o estratégicas de los producto de la información (International Federation of Accountants IFAC, 2018). En el ámbito universitario, el nivel de materialidad se encuentra determinado por el efecto que tienen sobre la

integridad de los registros académicos y sobre la prestación del servicio educativo.

- No conformidad mayor (NC+): Se entiende como la ausencia de un control crítico o la quiebra sistémica de un proceso que es crítico para cumplir con los objetivos de la organización. Dada la definición, el estándar ISO/IEC 17021-1 establece que una NC Mayor da pie a cuestionar la capacidad del sistema de gestión para alcanzar los resultados deseados.

  Análisis: En el contexto de la universidad, una NC Mayor corresponde a una vulnerabilidad estructural, y no un error de ejecución administrativa. Por ejemplo, la inexistencia de segmentación de red (VLANs) entre la red administrativa y la de laboratorio de alumnos puede ser considerada una NC Mayor dado que expone la base de datos central a inminentes ataques laterales. Dicha condición implica que la tecnología presente en el proceso de control interno constituye una "tecnología de Nivel 1" (Inicial) como se la define en CMMI, que se caracteriza por su imprevisibilidad y por determinar unos niveles de alto riesgo operativo (CMMI Institute, 2018).

- No conformidad menor (NC-): Es el cumplimiento de una vez, incidencia o incumplimiento específico, que no afecta a la funcionalidad global del sistema de control interno, salvo que se aprecie la ausencia de una disciplina de no cumplimiento o de una supervisión de desarrollo de los procedimientos.

Análisis: Un ejemplo sería que la bitácora de mantenimiento de un servidor específico correspondiente a un mes determinado no se haya actualizado, aunque el mantenimiento sí se haya realizado efectivamente por considerarse en los términos de la columna P. No hay un cese de funcionamiento, pero va acumulándose con el paso del tiempo y el número de NC Menores y puede llegar a derivar en un fallo de los sistemas a través de la interacción perdurable de resto de NCM que sí son clasificados, y finalmente, con excepción del propio sistema de control interno o de efectivos, ser un sistema de control interno normal (Whittington & Pany, 2020).

- Observación (oportunidad de mejora): Hallazgos que aunque se cumplen desde un punto de vista técnico de las normativas existentes, se encuentran en una situación subóptima. Responden a la idea de eficiencia operativa.

  Análisis: Se trata de una Observación el hecho de que la universidad utilice procesos manuales para convalidar cursos, cuando el sistema ERP de la universidad tiene un módulo justo para ello, es decir, se pueden comparar automáticamente las materias aprobadas por el estudiante con la de la misma materia en la universidad que proceden, aun así este hecho es irrelevante a efectos legales pero no es correcto y genera frustración del alumno al sobrecargar de burocracia (tiempos de espera de convalidación excesivos).

1. **Riesgo inherente y residual:** La identificación de hallazgos se fundamenta en el marco referencial GRC (COSO ERM, 2017) estableciendo de forma nítida la diferenciación entre el riesgo

natural de la universidad y el riesgo residual tras la aplicación de los controles. Esta diferenciación es muy relevante para evidenciar que la auditoría no solo es capaz de evidenciar que existen problemas a nivel instituciones, sino que además es capaz de evidenciar qué tanta desprotección hay.

2. **Riesgo inherente (Ri):** Se trata del riesgo existente en la actividad de una universidad pública previo a la consideración de los correspondientes controles. La UNACH maneja datos sensibles (socioeconómicos, de salud, calificaciones, etc.) y opera en infraestructura crítica abierta a miles de usuarios (estudiantes) que utilizan su propia infraestructura (BYOD).

Evaluación: El Ri se califica como ALTO. La naturaleza "abierta" de la cultura universitaria y los valores de los títulos profesionales en el mercado negro, signifiquen que la probabilidad de fraude o ataque es alta por defecto (Power, 2007).

3. **Riesgo Residual (Rr):** Este es el grado de riesgo que queda después de aplicar los controles de TI que tiene hoy en día. Para el caso de la fórmula, se entendería como:

$$Riesgo\ Residual = \frac{\text{Riesgo Inherente}}{\text{Eficacia del Control}}$$

4. **Hallazgo Crítico:** La auditoría pone de manifiesto que en varias instancias (por ejemplo, en la seguridad perimetral o en la gestión de backups), la eficacia del control es baja o es nula, lo que hace que el Riesgo Residual sea prácticamente igual al Ri.

Implicancia doctoral: Esto significa que la institución opera por encima del "Apetito de Riesgo". Considerando el primer supuesto, la universidad presenta una exposición que no tiene la capacidad para mitigar financieramente los posibles efectos si llegara a producirse un desastre (Committee of Sponsoring Organizations of the Treadway Commission COSO, 2017).

3.2 Matriz "Hallazgo – Evidencia – Riesgo – Recomendación"

Para que la aportación del informe sea sólida y para evitar sesgos subjetivos en la interpretación del hallazgo, cada hallazgo se extiende metodológicamente (conforme a las Normas Internacionales para la Práctica Profesional de la Auditoría Interna - IPPF) bajo el planteamiento de los "5 Atributos del Hallazgo"; esta matriz permite tener una lógica del síntoma hasta la solución.

Condición (lo que es - evidencia empírica): Es una descripción objetiva y de la propia situación que se ha encontrado. Se encuentra sostenida por papeles de trabajo referenciados (ej. "PT-SEG-004: Captura de pantalla de configuración del Firewall"). No tiene adjetivos calificativos, solo hechos verificables.

Criterio (lo que debe ser - marco normativo): (Lo que debe ser - Marco Normativo): se puede definir como la norma específica vulnerada que lleva a legitimar el hallazgo, debiendo ser una norma de ámbito legal (Art.13ª Ley de Gobierno Digital) estándar internacional (Control A.9.2 ISO 27001) o interna (Reglamento de la Universidad Nacional Autónoma de Honduras - UNACH). Sin criterio, no hay hallazgo, sólo opinión.

Causa raíz (etiología - por qué sucedió): Diagnóstico profundo del origen del problema. En esta tesis se evita la simplificación de culpar al "humano error". Se utilizan técnicas como los 5 Porqués o el Diagrama de Ishikawa para identificar causas estructurales: falta de presupuesto, debilidad en la gobernanza de TI, obsolescencia tecnológica o brechas de competencias digitales del personal (Human Capital Gap).

Efecto (impacto - consecuencia): Materialización del riesgo. Se debe vincular este efecto con la variable dependiente de la tesis: La satisfacción del estudiante.

Ejemplo: La caída del sistema de matrícula (condición) genera colas físicas de 6 horas (efecto operativo) que incrementan la percepción de ineficiencia y reducen la satisfacción del usuario (efecto estratégico)

Recomendación (tratamiento): Medidas correctivas que tienen que encauzarse a atacar la causa raíz. Las recomendaciones siempre deben ser SMART (específicas, medibles, alcanzables, relevantes y temporales).

3.3 Hallazgos transversales

Es la parte que se encarga de las patologías que se cruzan de forma transversal a toda la organización. Conocer los hallazgos transversales supone adquirir un nivel de conocimiento superior en sociología organizacional y gobernanza de TI (IT Governance).

Shadow IT (TI en la sombra): Se constató el uso generalizado de herramientas no institucionalmente legitimadas (Google drive personal

para guardar tesis, WhatsApp para comunicados oficiales, software no licenciado).

Fundamentación científica: Silic y Back (2014) sostienen que el Shadow IT no hay que entenderlo como la intrusión maliciosa del usuario, sino como el mecanismo de defensa ante los sistemas rígidos o ineficaces de los servicios oficiales de TI.Se trata de un indicador importante que evidencia que la oferta tecnológica de la Universidad no se encuentra alineada a las necesidades de la demanda (docentes/alumnos).

Desalineamiento estratégico (Business-IT Misalignment): Se constata una desconexión total entre el Plan Estratégico Institucional (PEI) y el Plan de Gobierno Digital. Se adquiere hardware (compra de servidores) sin un plan de implementación de software o de capacitación, provocándose el fenómeno de "tecnología de estantería" (subutilización de activos), y por tanto va en contra de los principios de valor de Val IT e ITIL 4 (Axelos, 2019).

3.4 Hallazgos específicos por norma

Se presenta la síntesis técnica de las desviaciones agrupadas por los marcos de referencia definidos en el capítulo 1, haciendo uso del rigor necesario en la verificación del cumplimiento.

3.4.1 Dominio: Seguridad de la información (ISO/IEC 27001 & Ley 29733):

La seguridad de la información se define, desde el ámbito de la gestión universitaria contemporánea, como el sistema de políticas, procedimientos, estructuras organizativas y controles técnicos orientados a salvaguardar las propiedades esenciales de los recursos de información institucional. Se trata de un ámbito que va mucho más allá de la simple protección tecnológica para constituirse como un proceso de gobernanza social de la organización que tiene como objetivo la gestión de riesgos y la obtención de la confianza de las partes interesadas (estudiantes, profesores y organismos reguladores).

Desde la perspectiva técnica, este ámbito se rige a partir de la normativa internacional ISO/IEC 27001, que establece los requisitos de un Sistema de Gestión de Seguridad de la Información.

Bajo este marco, la seguridad se materializa a partir de la preservación de la tríada CIA:

- **Confidencialidad:** la información académica y administrativa solo es accesible por personas autorizadas.
- **Integridad:** Garantía de que los registros (ej. notas, grados y títulos) son exactos y completos aun frente a intentos de modificaciones no autorizadas.
- **Disponibilidad:** Certeza de que los servicios educativos y la información crítica son accesibles cuando así lo requieren los usuarios legítimos.

Sin embargo, este dominio, en el ecosistema jurídico peruano, adquiere un espectro de cumplimiento legal y obligatorio a partir de la Ley N.º

29733, Ley de Protección de Datos Personales. Esta ley redefine la seguridad de la información, no como una buena práctica, sino como un elemento fundamental en la tutela del derecho de los ciudadanos a la privacidad. En consecuencia, la implementación de los controles ISO/IEC 27001 en la Universidad Nacional Autónoma de Chota (UNACH), se convierte en el soporte técnico para dar cumplimiento a la exigencia legal de implementar "medidas técnicas, organizativas y legales" que garanticen la seguridad de los bancos de datos personales y prevengan cualquier acceso, alteración, tratamiento o pérdida de datos personales no autorizados (Ministerio de Justicia y Derechos Humanos, 2011).

Por todo lo anterior, este dominio articula en perfecta consonancia la rigurosidad estandarizada (ISO) con la exigencia legal (Ley 29733), generando un escudo protector sobre el capital intelectual y los datos sensibles de la comunidad universitaria.

- Hallazgo: Debilidad crítica en la gestión de accesos lógicos. Se detectan cuentas genéricas compartidas ("admin", "usuario1") y ausencia de una política de contraseñas robustas.
- Impacto: Imposibilidad de garantizar la trazabilidad (Non-Repudiation) en caso de alteración de notas, violando la Ley de Protección de Datos Personales.

3.4.2 Dominio: Continuidad del negocio (ISO 22301)

En lo que respecta a la educación superior, la continuidad del negocio (Business Continuity) se sitúa en un nivel superior: es la capacidad

estratégica y operativa de una universidad para mantener la provisión de sus servicios esenciales docencia, investigación y gestión administrativa a determinados niveles de servicio establecidos y aceptables durante y después de una interrupción disruptiva. La continuidad del negocio, dividido o versus la recuperación ante desastres (la cual tiene un enfoque meramente tecnológico), es una disciplina de gobernanza integral que busca la resiliencia organizacional, de tal forma que la misión de formación de la UNACH persista frente a contingencias adversas (ciberataques, emergencias naturales, pandemias o fallas sistémicas).

Desde el punto de vista técnico-normativo, este ámbito queda delimitado bajo el estándar internacional ISO 22301:2019 (Security and resilience Business continuity management systems). Este marco establece un modelo que sirve para configurar un Sistema de Gestión de Continuidad de Negocios (SGCN) bajo el ciclo de mejora continua (Planificar-Realizar-Verificar-Actuar) y supone a la institución que:

- **Identificación de procesos críticos:** No todos los procesos tienen la misma urgencia. La norma obliga a realizar un BIA que permita diferenciar lo urgente (ej. plataforma de aulas virtuales en la época de exámenes) lo que puede diferirse para otro momento (ej. actualización de inventarios de biblioteca).
- **Determinación de tiempos de recuperación:** Establecer científicamente el RTO (*Recovery Time* Objective - tiempo máximo tolerable sin servicio) y el RPO (*Recovery Point Objective* - pérdida máxima de datos aceptable) para cada activo informático.

- **Estrategias de resiliencia:** Diseñar planes que garanticen que, ante la caída del centro de datos principal, existan mecanismos alternos (redundancia, trabajo remoto, procesamiento manual) que permitan garantizar la supervivencia institucional.

En el caso de la Universidad Nacional Autónoma de Chota (UNACH), aplicar la ISO 22301 no es un requisito burocrático, sino que es un aval de la fe pública y del propio derecho a la educación. Aplicar esta norma es asegurar que un incidente tecnológico no derive en la pérdida del historial académico de miles de estudiantes, ni en la cancelación de un semestre académico. Es, en último término, la puesta en práctica del deber custodial que la universidad tiene sobre el futuro profesional de sus alumnos y la integridad de sus investigaciones.

- Hallazgo: Ausencia de un Plan de Recuperación ante Desastres (DRP) probado. Se supone que se realizan copias de seguridad (Backups), pero no han realizado pruebas de restauración (Restore Tests).

- Impacto: Sensación de seguridad falsa. Se desconoce el Tiempo de Recuperación (RTO) real, quedando en entredicho la finalización del semestre académico contra un incidente mayor (Snedaker & Rima, 2013).

3.4.3 Dominio: Gestión de servicios (ISO/IEC 20000)

La Gestión de Servicios de Tecnología de la Información (también conocido como ITSM) se puede definir como un enfoque sistémico y procesal que persigue diseñar, entregar, gestionar y mejorar la manera

en que las tecnologías son utilizadas para aportar valor en la organización. Este ámbito en el entorno universitario supone un cambio paradigmático puesto que el departamento de IT deja de ser un simple ámbito técnico (que giraba únicamente en torno a hardware y software) para pasar a ser un aliado estratégico en términos de experiencia del usuario (estudiantes, docentes y personal administrativo) y la calidad del servicio educativo.

El reglamento que rige este área es el estándar internacional ISO/IEC 20000-1:2018 (*Information technology Service management*).Ésta norma define los requisitos de un Sistema de Gestión de Servicios (SGS) que permitan la alineación entre los objetivos de la tecnología y las necesidades del negocio.

La aplicación de la norma se basa en la adopción de un ciclo de vida del servicio que incluye:

1. **Catálogo de servicios:** La definición pública y explícita de qué servicios ofrece el área de TIC (ej. soporte aulas virtuales, conectividad en campus, gestión de matrículas), evitando los escenarios difusos en los niveles de expectativas de la comunidad universitaria.
2. **Acuerdos de nivel de servicio (SLA):** La formalización contractual o cuasi–contractual de los compromisos de calidad. Por ejemplo, establecer que una incidencia crítica en el sistema de notas debe resolverse en un máximo de 4 horas de forma tal que la promesa vaga de un "soporte rápido" se convierta en una métrica auditorable y exigible.

3. **Gestión de incidentes y problemas:** La separación técnico-conceptual entre el restablecimiento del servicio de forma rápida (incidente) y la búsqueda de la causa raíz que permita evitar que vuelva a ocurrir (problema), tal que se optimice la estabilidad operativa en el tiempo.

El paso de la Universidad Nacional Autónoma de Chota (UNACH) a la implantación de la ISO/IEC 20000 implica transformar la gestión reactiva ("apagar fuegos") de TI en una gestión proactiva y predecible. Ésta asegura que la tecnología no ueda un freno, sino más bien un recurso completamente transparente y eficiente capaz de facilitar los procesos académicos, donde la calidad no se mide en términos de sofisticación en los servidores, sino sólo en términos de satisfacción del estudiante y en la continuidad ininterrumpida de su formación académica.

- Hallazgo: Gestión de incidentes informal. La Mesa de Ayuda no registra el 100% de los casos en un sistema de tickets, lo que impide medir los Acuerdos de Nivel de Servicio (SLA).
- Impacto: El estudiante percibe que el soporte es "lento" o "arbitrario", afectando directamente la dimensión de "Capacidad de Respuesta" del modelo SERVQUAL.

CAPÍTULO IV

4 ETAPA 5: DISEÑO DEL PLAN DE MEJORAS

Una vez cerrada la etapa de diagnóstico y una vez identificadas de manera científica formal las brechas tecnológicas y los incumplimientos operativos de la Universidad Nacional Autónoma de Chota (UNACH), el presente capítulo se ocupa del diseño propuesto de la investigación: la formulación del Plan de Mejora (PM). Este Plan no es considerado un listado de técnicas de reparo aisladas, sino todo lo contrario, es un esquema de gobernanza estratégica que va en consonancia con los objetivos institucionales de la PQC y con el ciclo de mejora continua PDCA de Deming, dado que pretende cerrar las brechas existentes entre la situación real (As-Is) y el estado deseado (To-Be), convirtiendo así los hallazgos derivados de la auditoría en proyectos de intervención posibles.El diseño del plan establece que cada acción correctiva tenga trazabilidad inmediata frente a la eliminación de las causas raíz identificadas; esto hace que toda la inversión en tecnología devenga en un incremento en el ámbito de la calidad del servicio educativo y en la satisfacción del estudiantado, superando la visión tecnocentrista por una visión centrada en el usuario (International Organization for Standardization ISO, 2015).

La construcción de este plan se basa en la buena práctica en gestión de proyectos del Project Management Institute (PMI) y en la gestión de COBIT 2019, lo que establece la viabilidad técnica, económica y administrativa de la propuesta en el marco de la gestión pública del Perú, dado que los recursos universitarios son finitos. En ese sentido, el

capítulo establece unos criterios estrictos de priorización que permiten establecer la jerarquía de las intervenciones a partir de su valor público y su capacidad de atenuar riesgos críticos. También se definen procedimientos de control, seguimiento e indicadores de desempeño (KPI), se establece un sistema de rendición de cuentas (Accountability) claro, y se construyen matrices de asignación de roles. De este modo, el plan no sólo se presenta como un cumplimiento a las normativas de la SUNEDU y a la Ley de Gobierno Digital, sino que también establece las bases para la transformación digital sostenible y que se pueda auditar en el tiempo (Project Management Institute, 2021; ISACA, 2018)

4.1 Criterios de priorización

En En la administración pública, las mejoras de TI se combaten por recursos presupuestarios que son limitados. Por ello, resulta necesario aplicar una metodología científica para saber qué hallazgos se van a atender primero. Proponemos el diseño de una matriz de priorización Ponderada, basada en el concepto de la gestión en el portafolio de TI.

Teniendo en cuenta que los criterios de priorización son:

Impacto en la satisfacción estudiantil (peso: 40%): Se seleccionan aquellas acciones que son evidente al estudiante (ej. decrementar el tiempo de caída del aula virtual). Esto da sentida a la tecnología con la variable dependiente de la tesis.

Criticidad normativa y legal (peso: 35%): Acciones que se llevaran a cabo forzosamente para evitar sanciones y (Ley 29733 de Protección de

Datos) y cierres de los programas por incumplimiento de las Condiciones Básicas de Calidad (CBC).

Factibilidad técnica y económica (peso: 25%): Evaluación de la complejidad. Entenderes rápidos (quick wins) mejoras de bajo coste de alto impacto que dan como resultado la confianza en la gestión.

Fórmula de valoración:

$$\text{Prioridad} = (\text{Impacto x } 0{,}40) + (\text{Normativa x } 0{,}35) + (\text{Factibilidad x } 0{,}25)$$

4.2 Acciones correctivas

La acción correctiva, el cual está enmarcado exclusivamente en la auditoría de sistemas de información, no sólo repara a nivel superficial la no conformidad detectada. La norma ISO 19011:2018 define una acción correctiva como la acción que se hace para eliminar la causa de una no conformidad detectada y evitarla en un futuro. La acción correctiva es diferente al concepto de "corrección". Esta última está en el plano de actuación para atacar o tratar el síntoma que se presenta, como podría ser reiniciar un servidor colgado.

Mientras que la acción correctiva podría significar modificar la acción que se lleva a cabo en la realización de procesos, y asegurar así un comportamiento estable en el tiempo. Para garantizar la efectiva aplicación de la acción correctiva propuesta en la Universidad Nacional Autónoma de Chota (UNACH), la acción se estructura metodológicamente siguiendo el principio de Defensa en Profundidad

(Defense in Depth) clasificándola en tres ejes estratégicos de intervención que desarrollan la dimensión tecnológica, la dimensión procedimental y la dimensión humana de la organización.

Las acciones que se desarrollan para poder neutralizar la Causa Raíz y no su síntoma se entregan en tres ejes estratégicos de intervención:

4.2.1 Eje tecnológico (infraestructura y software)

Este eje corresponde a la agrupación de las intervenciones referidas a la arquitectura física y lógica que soporta los servicios de educación. En el contexto de la transformación digital en el ámbito universitario, la tecnología no es un simple recurso instrumental, sino la base de la continuidad operativa. Las acciones correctivas en este área se sustentan en estándares como NIST SP 800-53 e ISO/IEC 27002 y se dividen en dos tipos de acciones correctivas:

- Fuerza y "Hardening" de la Infraestructura de Hardware La infraestructura inadecuada, anticuada o mal configurada constituye la vía principal de ataque de las instituciones públicas. Aquí, la acción correctiva no es obligatoriamente capital inversión (CAPEX) sino la mejora de la configuración de seguridad de los hardware existentes, técnicamente denominado como Hardening.
- Control de obsolescencia de la tecnología: Aplicación de un plan de recambio cíclico, soportado en la medida MTBF (Mean Time Between Failures), así como en el end of life del fabricante. La utilización de servidores fuera de soporte pone a la universidad en

la diana de un ataque por vulnerabilidades sin parchear (Stallings & Brown, 2018).

- Redundancia y alta disponibilidad: Configuración de arquitectura de clúster y balanceo de carga para los servicios críticos (Matrícula, Aula Virtual). La acción correctiva diseñada para eliminar los Single Point of Failure (SPOF) detectados en el análisis de auditoría.
- Seguridad perimetral: Reingeniería de reglas de Cortafuegos de Nueva Generación (Next-Generation Firewalls - NGFW) de pasar de una política de "permitir todo menos prohibido" a una política de "prohibir todo menos lo explícitamente autorizado" (Zero Trust Architecture).

Ingeniería de software seguro y gestión de vulnerabilidades en el ámbito del software, las acciones correctivas deben abarcar tanto software desarrollado internamente como software adquirido a tercera parte. La literatura científica hace hincapié que el coste de corregir un defecto de software en producción es exponencialmente superior que hacerlo en la fase de diseño (Pressman & Maxim, 2020).

- Gestión de parches (patch management): Institucionalización de una política automatizada de despliegue de actualizaciones de seguridad. La evidencia empírica muestra que la mayoría de las brechas de datos exteriorizan vulnerabilidades para las cuales ya existían parches disponibles meses antes de la brecha.
- Ciclo de Vida de Desarrollo Seguro (SDLC): Para el software académico desarrollado de forma interna por la UNACH, la acción correctiva es adoptar metodologías DevSecOps, mezclando

pruebas de seguridad estáticas (SAST) y dinámicas (DAST) dentro del flujo de integración continua de manera que el código sea a la vez seguro.

- Control de versiones y deuda técnica: Institucionalización de un software de gestión de repositorios y auditoría de código que permitan mitigar la deuda técnica acumulada, la cual, si no se paga (no se corrige), se convierte en sistemas no sostenibles e inseguros a largo plazo.
- **Acción:** Implementación de redundancia lógica y física en servidores críticos.
- **Detalle:** Configuración de Failover Clustering para el SGA. En caso de que el servidor principal sufra una avería, de inmediato el secundario se hará cargo de la carga de trabajo automáticamente, de forma que el estudiante no detecte ninguna interrupción en el servicio.
- **Norma:** Alineado con ISO 22301 (continuidad del negocio).

4.2.2 Eje de gobernanza (políticas y procesos)

Si se considerase la tecnología como el "músculo" de la organización, la gobernanza sería el "cerebro" que ordena sus movimientos/movimientos de la organización. Este eje de intervención se basa en la reestructuración del marco normativo y la ingeniería de los procesos, con el objetivo de reducir la brecha existente entre la estrategia institucional de la UNACH y la ejecución operativa más diaria. La gobernanza no es estrictamente la escritura de reglamentos, según el estándar ISO/IEC 38500 (Gobernanza TI para la organización), sino la evaluación, la dirección y el monitoreo del uso de las TI para la

generación de valor (International Organization for Standardization ISO, 2015).

Las acciones correctivas desde este lugar serán de tal forma que transformen el "conocimiento tribal" (el conocimiento que poseían sólo algunos funcionarios antiguos) en "conocimiento explícito institucional", y se desarrollan en tres líneas de acción:

Estructuración de la jerarquía de la documentación (políticas, estándares y procedimientos), dado que la auditoría a menudo puede indicar confusión entre lo que es una política y un procedimiento (Kotter, 2012). La acción correctiva se traduce en establecer una arquitectura documental piramidal entendible:

- **Políticas (nivel estratégico):** Elaboración de documentos de alto nivel aprobados por el Consejo Universitario (ej. "Política General de Seguridad de la Información"). Su obligado cumplimiento define el "qué" y el "porqué".
- **Estándares y líneas base (nivel táctico):** Definición de requisitos técnicos obligatorios (ej. "Estándar de Cifrado AES-256 para bases de datos"). Proliferan la homogeneidad tecnológica.
- **Procedimientos y guías (nivel operativo):** Documentos explicativos del cómo (ej. "Manual de Alta de Usuario en el SGA"). La formalización de estos documentos reduce la variabilidad del proceso, así como su dependencia de las personas clave.

Reingeniería de procesos (BPM) y segregación de funciones (SoD). Muchos riesgos de la informática se producen por el mal diseño de procesos en los que una única persona tiene control absoluto sobre una transacción crítica.

- **Segregación de funciones (SoD):** La acción correctiva debe garantizar que no queda ninguna persona dotada de la autoridad para iniciar, aprobar y realizar la auditoría de forma simultánea de una operación crítica, por ejemplo, el administrador que regula la base de datos de las notas no debe tener permisos para promover cambios en las actas finales que estén sin la aprobación digital de la Secretaría General, evitando el riesgo de fraude interno (ISACA, 2019).
- **Optimización de flujos:** uso (valga la redundancia) de notación BPMN (Business Process Model and Notation) que permite rediseñar y eliminar los procesos burocráticos, evitando cuellos de botella, puntos de control innecesarios que no proporcionan valor a la operación, todo ello con el riesgo de la latencia del servicio educativo.

Institucionalización del cumplimiento creación de mecanismos de auditoría continua. La acción correctiva no finaliza con la publicación de la norma, sino también a partir de la introducción de métricas de cumplimiento (KPIs) que hagan llegar periódicamente la información al Rectorado sobre el grado de cantidad de adhesión a las nuevas políticas para convertir la cantidad de cumplimiento en una forma de vida y no en un evento anual.

- **Acción:** Institucionalización del Comité de Gobierno Digital.
- **Detalle:** Creación de un órgano colectivo (Rectorado, TI, Planificación) que apruebe aquellos gastos en tecnología y evite la compra aislada de forma "isleada", es decir, sin que dicha tecnología se interrelacione con el resto de la tecnología.
- **Norma:** Alineada con la Ley de Gobierno Digital (D. Leg. 1412).

4.2.3 Eje de capital humano (cultura y capacitación)

El ser humano es, a la vez y paradójicamente, el eslábón más débil y la primera línea de defensa en la seguridad de la información. La literatura científica existente sobre ciber psicología (Hadlington, 2017) afirma que las mejores inversiones tecnológicas pueden ser inutilizadas por una personas que hace clic en un enlace de phishing o que comparte su password. Por consiguiente, este eje es más que "adiestramiento técnico", ya que hace alusión a la gestión del cambio cultural y el desarrollo de competencias.

Las acciones de corrección en este ámbito se fundamentan en el estándar NIST SP 800-50 (*Building an Information Technology Security Awareness and Training Program*) y se desarrollan en las siguientes dimensiones:

Programa de concienciación, entrenamiento y educación (SETA) se hace necesario distinguir niveles pedagógicos de intervención:

- **Concientización:** Acciones masivas dirigidas a toda la comunidad universitaria (alumnos, docentes, administrativos) para cambiar comportamientos muy básicos. Ejemplo: Campañas

anti-phishing; manejo seguro de redes Wi-Fi; protección de datos personales. El objetivo es que el usuario "reconozca" el riesgo.

- **Formación:** Desarrollar habilidades prácticas para roles específicos. Ejemplo: Taller para secretarias sobre manejo de archivos cifrados o detección de ingeniería social en el teléfono (e.g., fraude de la Nigerian Prince). El objetivo es que el usuario "sepa hacer" su trabajo con seguridad.
- **Educación:** Desarrollar la teorización para los especialistas de TI. Ejemplo: certificaciones en ciberseguridad ética o gestión de redes para el personal del centro de datos .

Gestión de la resistencia al cambio en la implementación de controles (ej. doble factor de autenticación) suele generar resistencia y rechazo en la comunidad académica. La acción de corrección exige una estrategia de comunicación organizacional que justifique los beneficios de la seguridad, no como un freno burocrático, sino como una garantía de calidad y prestigio de la UNACH. Deben ser identificados "campeones de la seguridad" (Security Champions) en cada facultad para actuar como agentes de cambio e influencias positivas.

Definición de roles y responsabilidades a menudo la seguridad fracasa porque "es la responsabilidad de todos y al mismo tiempo de nadie". La acción de corrección exige la actualización de los instrumentos de gestión (ROF/MOF) para incorporar explícitamente las responsabilidades de seguridad de la información en las descripciones de puesto de cada funcionario asociando el cumplimiento de las políticas de TI con la evaluación del rendimiento laboral (ISACA, 2019).

- **Acción:** Programa de alfabetización digital administrativa.
- **Detalle:** Formación obligatoria y certificada del personal de ventanilla y secretarías en el uso eficiente del ERP académico y en la seguridad de la información (gestión de contraseñas y datos personales).
- **Norma:** Alineado con ISO 10015 (gestión de competencias).

4.3 Cronograma y responsables

Para evitar la confusión de las responsabilidades, que es muy habitual en los organismos públicos, se establecen claramente los roles mediante la matriz RACI (Responsible, Accountable, Consulted, Informed). El cronograma se distribuye en horizontes temporales razonables:

4.3.1 Fase 1: Saneamiento inmediato (0 - 3 meses):

Se denomina técnicamente "Triaje Ciberseguridad" a esta primera fase --la cual se ocupa de estabilizar operativamente y de mitigar las No Conformidades Mayores (NC+) detectadas en la auditoría-- cuya finalitat no es la perfección documental sino "contener daños" para garantizar la continuidad del servicio educativo, así como la protección de los activos de información más críticos frente a amenazas en curso. En este trimestre, la gestión es "de Comando y Control" priorizando acciones de Corrección de Alto Impacto y bajo esfuerzo de implementación, o sea *Quick Wins*, como la corrección de brechas de seguridad de perímetro, el cierre de accesos obsoletos y la ejecución de copias de seguridad inmutables de los sistemas críticos (matrícula y notas) (Center for Internet Security, 2021).

Desde el punto de vista de la norma ISO/IEC 27001, este momento corresponde a los controles pertenecientes a los dominios de "Seguridad Operativa" y "Gestión de Accesos". Correos electrónicos de advertencia, procedimientos de *hardening* (endurecimiento) de servidores y bases de datos; para implantar medidas que disminuyan la superficie de ataque eliminando servicios no necesarios y aplicando parches de seguridad que habían sido dejados de lado (Stallings & Brown, 2018). Es un periodo de gran exigencia técnica en el que se intentan sacar a la institución de la "zona del peligro", de modo que la Universidad Nacional Autónoma de Chota (UNACH) pueda cumplir los mínimos exigibles de la Ley de Protección de Datos Personales como para escapar de sanciones legales y reputacionales inmediatas.

Finalmente, este periodo culmina en la estabilización de la infraestructura tecnológica básica. Se establece un "Comité de Crisis de TI" temporal que debe supervisar la puesta en marcha de las correcciones urgentes y validar la recuperación de la integridad de los datos. El entregable central de este periodo no es un manual de procedimientos, sino una infraestructura resiliente capaz de absorber sin excesivas dificultades el trabajo cotidiano; una "no ruptura catastrófica" del funcionamiento diario. Al finalizar el tercer mes, la universidad ha de haber pasado de "riesgo inaceptable" a "riesgo controlado", asentando las bases técnicas para la posterior normativización administrativa (Whitman & Mattord, 2021).

Enfoque: seguridad y estabilidad.

Acciones: Parcheo de servidores, puesta en marcha de copias de seguridad inmutables, cambio de contraseñas de admin por defecto.

Responsable (R): Jefe de Infraestructura Tecnológica.

4.3.2 Fase 2: Estandarización y formalización (3 - 12 meses):

Ya superada la urgencia del momento operativo, esta fase concretamente se refiere al reto que supone la institucionalización del conocimiento. El objetivo estratégico consiste en eliminar la dependencia del "conocimiento tribal" (conocimiento tácito que poseen determinadas personas) para poder avanzar hacia el camino de la "gestión por procesos" (conocimiento explícito institucional) acorde con lo que exigen los requisitos de la norma ISO 9001:2015 e ISO/IEC 20000-1 (International Organization for Standardization ISO, 2018). A lo largo de estos 9 meses, se procederá a redactar, aprobar y socializar la jerarquía de arquitectura documental: políticas de seguridad, manuales de procedimientos operativos, guías técnicas y acuerdos de niveles de servicio (SLA) (Dumas y otros, 2018).

Durante este tiempo se pondrán en marcha los controles tácticos y administrativos que requieren el cambio cultural. Se ponen en marcha formalmente los procesos de Gestión de Cambios y Gestión de Incidentes garantizando que no exista cambio alguno en la infraestructura sin su correspondiente análisis e impacto y riesgo. Igualmente se valida formalmente el Ciclo de Desarrollo de Software Seguro (SDLC) para los aplicativos internos de la UNACH (ISACA, 2019). La estandarización quiere que las actividades de TI sean predecibles, repetibles y auditables y, además, eleva el nivel de madurez

de la organización desde un nivel Ad Hoc (Nivel 1) a un nivel Definido (Nivel 3) de acuerdo con el modelo de madurez del COBIT 2019.

La formalización también abarca la intensa capacitación del capital humano. Se llevan a cabo los programas de sensibilización y la formación técnica establecidas en el plan de acción asegurando que el personal no sólo tenga acceso a los nuevos manuales, sino que comprenda su papel en su cumplimiento. Al finalizar el primer año, la UNACH dispondrá de un "sistema de gestión" operativo donde las reglas del juego son claras, los roles definidos (Segregación de Funciones) y la tecnología operando bajo un marco de gobernanza aprobado por la Alta Dirección dejando atrás la improvisación administrativa.

Enfoque: Procesos y documentación.

Acciones: Implementación de mesa de ayuda (ticketera), redacción de manuales de usuario, formalización de políticas de seguridad.

Responsable (R): Director de tecnologías de información.

4.3.3 Fase 3: Optimización y transformación (12 - 24 meses):

La última fase de la planificación se centra en la suprema calidad de las operaciones y en la generación de valor público. Una vez estabilizados, seguros y normalizados todos los procesos, se da un giro hacia la eficiencia y la innovación bajo la óptica de la Mejora Continua (Continual Service Improvement - CSI) de ITIL v4. La gestión dejará de estar basada en la intuición y se fundamentará estrictamente en datos;

una vez conseguido esto, se implementa el Dashboard con Indicadores Clave de Desempeño (KPIs) y Métricas de Riesgo (KRIs) que permiten monitorizar la salud de los servicios tecnológicos y la satisfacción de la comunidad universitaria casi en tiempo real (Kaplan & Norton, 1996; Van Grembergen & De Haes, 2018).

En este nivel de madurez (Nivel 4-5), la seguridad y la tecnología se integran en la estrategia institucional. Realizamos auditorías internas y revisiones por la dirección internas periódicos y posteriormente se definirán desviaciones muy sutiles y detectar de oportunidades de automatización (Grajek, 2020). Las Oportunidades de Mejora (OBS's en inglés) detectadas en la auditoría inicial, no críticas, pero demasiado provechosas- son ahora ejecutadas en la fase final para la optimización de los recursos. La tecnología deja de ser vista como un cost center o como un soporte (support), para convertirse en un habilitador estratégico de la transformación digital y potenciar nuevos modelos de enseñanza-aprendizaje y servicios administrativos digitales (Cero Papel). Finalmente, esta fase afecta positivamente la cultura de la gobernanza adaptativa (Weill & Ross, 2005).

La UNACH ya no solo se muestra satisfecha con el cumplimiento normativo, sino que también es capaz de adaptarse con agilidad a los nuevos desafíos de las tecnologías (IA, Big Data, etc.) sin perder el control. El resultado de finalizar los 24 meses es una institución robusta y certificable en estándares internacionales, en la que podrá llevar a cabo nuevas acreditaciones de calidad educativa, donde la tecnología se comporta como un garante de la transparencia, de la eficiencia y de la excelencia académica.

Enfoque: Innovación y calidad.

Acciones: Certificación ISO 27001, integración de Business Intelligence (BI) para la toma de decisiones académicas.

Responsable (R): Vicerrectorado Académico / Comité de Gobierno Digital.

4.4 Matriz de seguimiento

El Plan de Mejoras requiere un seguimiento constante. Se sugiere recurrir al Cuadro de Mando Integral (Balanced Scorecard) adaptado al seguimiento de auditoría para visualizar en tiempo la situación de cada hallazgo.

4.4.1 Componentes de la matriz:

1. ID Hallazgo: Código único de trazabilidad (ej. NC-SEG-004).
2. Acción comprometida: Descripción entregable de la solución.
3. Fecha de vencimiento: Dead-line inamovible.
4. Estado de avance (%): Medición de la cuantía de progreso físico.
5. Evidencia de cierre: Documento o registro técnico que demuestra que el riesgo ha sido atenuado (ej. "Acta de Conformidad de Instalación del Firewall").

Este instrumento permite al auditor interno o al Comité de Calidad verificar si las acciones producen un efecto efectivo o si deben ser corregidos (Feedback Loop).

4.5 Indicadores de mejora continua

Con el fin de validar la hipótesis de la tesis, es decir que la auditoría es capaz de mejorar la calidad del servicio, se deben medir los impactos tras su implementación. Por tal motivo, se proponen varias métricas que están alineadas con el modelo SERVQUAL y las métricas de ITIL 4.

Disponibilidad del servicio crítico (D): Mide la fiabilidad técnica que percibe el estudiante.

$$D = \frac{\text{Tiempo Total Operativo}}{\text{Tiempo Total Planificado}}\ x\ 100$$

Líneas de objetivo: > 99.5% durante los periodos de matrícula y de exámenes.

Tasa de Resolución al Primer Contacto (FCR): Mide la eficacia del soporte administrativo.

Porcentaje de consultas estudiantiles resueltas a la primera interacción (ventanilla o teléfono) sobre el total de consultas sin que tuviesen que ser referidas.

Línea de objetivo: > 70%. (Impacta en la dimensión de la "capacidad de respuesta").

Índice de Satisfacción Digital (ISD): Mide la percepción subjetiva de calidad.

Instrumento: Encuesta tipo likert frecuencia encuesta semestral.

Pregunta clave: En una escala del 1 al 5, ¿qué tan seguros y eficientes considera los servicios tecnológicos que proporciona la universidad?

Línea de objetivo: Incrementar el promedio desde 2.5 (línea base hipotética) hasta 4.0, en 12 meses.

CAPÍTULO V

5 APLICACIÓN PRÁCTICA DE LA METODOLOGÍA (TRES CASOS DE ESTUDIO)

Diseñado el modelo de auditoría informática y estructurado el plan de mejoras correspondientes a las etapas anteriores, se debe exigir la validación empírica de la construcción teórica, donde se pueda constatar la fiabilidad, la flexibilidad y la capacidad de uso en entornos operativos. Para hacerlo, se ha optado por aplicar la estrategia metodológica de Estudio de Casos Múltiples (Multiple-Case Study Design), siguiendo las recomendaciones de (Yin, 2018), quien expone que esta técnica es adecuada para investigar fenómenos contemporáneos complejos como la gobernanza tecnológica en su contexto natural, en este caso el caso que estamos analizando y cuando las fronteras que delimitan el fenómeno y el contexto no son evidentes. La etapa de validación no se orienta hacia la generalización estadística sino a la generalización analítica. Es decir, el propósito de esta etapa es corroborar que el marco de auditoría previamente propuesto (basado en ISO, COBIT e ITIL) sea apto para diagnosticar y remediar las carencias estructurales de TI que perjudican la calidad del servicio público, mediante una lógica de causa-efecto que se ha replicado en contextos heterogéneos (Stake, 2013).

A fin de proporcionar validez externa a esta investigación se han seleccionado tres unidades de análisis que son representativas de la diversidad del ecosistema público peruano: una Institución Educativa Pública (la cual será el foco de la tesis), un Gobierno Autónomo Descentralizado (Municipalidad) y una Agencia Pública Reguladora. A

través del análisis de estas tres unidades de análisis se aspira a triangular la información obtenida de la fuente documental, de la observación directa y de las métricas de desempeño para confirmar la hipótesis central de la investigación: la sugerencia de que existe una correlación positiva y directa entre la madurez de los controles informáticos y la satisfacción de los usuarios finales. El capítulo ofrece una descripción de la situación de partida de todos los casos, la manera de aplicar los dominios de auditoría en la sección Capítulo 1 y los resultados una vez aplicada la intervención, mostrando cómo la gestión técnica de riesgos se traduce en valor público que se puede medir (Organisation for Economic Cooperation and Development OECD, 2020).

5.1 Caso 1: Institución educativa pública

Corresponde a una aplicación piloto del instrumento en una universidad nacional con características homólogas a la UNACH con el fin de validar la sensibilidad del modelo de la variable "satisfacción estudiantil".

5.1.1 Contextualización y diagnóstico inicial (el problema)

La institución tenía una crisis de legitimidad crónica en todos los procesos de matrícula del semestre. El sistema de gestión académica (SGA), con una arquitectura anterior muy monolítica, caía en el servicio (Downtime) por más de 48 horas a lo largo de la semana de inscripciones.

Impacto: Esto llevaba a más de 5.000 estudiantes a tener que hacer cola presencialmente desde la madrugada, impidiendo la posibilidad de hacer

posible la baja temperatura, la posibilidad de matrimonio en la entrega de la información y un NPS de -25 puntos.

Diagnóstico: La auditoría indicó que no era una cuestión de servidores, sino de deuda técnica y no escalabilidad.

5.1.2 Aplicación metodológica (intervención)

Se aplicaron los dominios 1.14 (desarrollo y mantenimiento de software) y 1.20 (monitoreo de servicios) del modelo propuesto.

Auditoría de estrés (Load Testing): Se simuló una carga de 3.000 usuarios concurrentes, comprobando el "cuello de botella" en las consultas a la base de datos no optimizadas (SQL ineficiente).

Reingeniería de procesos: Se propuso implementar un "turnos digitales" en "escalera" en la media ponderada para poder aplanar la curva de demanda.

5.1.3 Resultados y evidencia de mejora

Después de aplicar las recomendaciones del Plan de Mejoras (Capítulo 4):

- **Disponibilidad:** Se obtuvo un Uptime del 99.9% en el siguiente ciclo.
- **Eficiencia:** El tiempo medio de matrícula por alumno pasó de 4 horas (presencial/cola) a 15 minutos (digital).

- **Satisfacción:** El NPS pasó a ser de +40, corroborando que la estabilidad tecnológica es el predictor más sólido de la satisfacción administrativa de la universidad.

5.2 Caso 2: Gobierno autónomo descentralizado

Este caso pone a prueba la capacidad del modelo para auditar la Usabilidad y el Gobierno Digital en los servicios orientados al ciudadano común.

5.2.1 Contextualización y diagnóstico inicial (el problema)

La municipalidad lanzó el servicio de "Tributación Digital" para gestionar los pagos del impuesto predial y arbitrios. La intención era promover la recaudación y reducir los niveles de evasión.Pasados seis meses, la tasa de adopción del canal digital era inferior a un 3 %.

Diagnóstico: Los ciudadanos decían que el sistema era "confusión", solicitando papeles que la propia entidad ya tenía (duplicado del DNI escaneado), y generando desconfianza porque no daba comprobantes en el acto.

5.2.2 Aplicación metodológica (intervención)

Se activaron 1.21 (Portal Web y Servicios Telemáticos) y 1.23 (Firmas Electrónicas e Interoperabilidad).

Auditoría de Usabilidad (UX Audit): Se auditó el portal aplicado a la WCAG 2.1 y Ley de Gobierno Digital. Se detectó que el proceso de

pago requería 14 clics y que no era Responsive, excluyendo a la gran mayoría de la población.

I**nteroperabilidad:** Auditoría de la falta de conectividad con la RENIEC y la plataforma PIDE, obligando al ciudadano a subir archivos manualmente.

5.2.3 Resultados y evidencia de mejora

La intervención supuso simplificar drásticamente el proceso (reducido a 3 clicks) así como la integración con la Pasarela de Pagos Nacional (págalo.pe).

- **Impacto económico:** En el coste la recaudación online agrupó en el primer trimestre posterior a la auditoría un 250%.
- **Validación:** Prueba que la auditoría de usabilidad no es estética, sino un driver económico básico para la sostenibilidad financiera.

5.3 Caso 3: Agencia pública reguladora

Esta situación valida la robustez del modelo en un contexto de alta seguridad, donde la confidencialidad es el activo más crítico.

5.3.1 Contextualización y diagnóstico inicial (el problema)

Una entidad encargada de controlar el cumplimiento de la normativa (parecida a un órgano de control) sufría constantes filtraciones de información a la prensa antes de que los actos administrativos con las resoluciones administrativas fueran oficializados, con la consiguiente

merma de la autoridad institucional y los riesgos legales por vulneraciones de los derechos del procedimiento.

Diagnóstico: Se disponía de información que hacía sospechar que pudiera existir fuga interna de información. La falta de controles y garantías permitían que no se pudiera identificar a los responsables.

5.3.2 Aplicación metodológica (intervención)

Se verificaron de forma estricta los dominios 1.12 (clasificación de la información) y 1.17 (seguridad de la información).

Auditoría de Accesos (IAM): Se comprobó que el 80% del personal tenía privilegios "Administrador" en la red, lo que quebrantaba el principio de "Menor Privilegio" (Least Privilege).

Trazabilidad (Logging): Los sistemas no generaban ningún tipo de registro de la persona que visualizaba o descargaba los expedientes en pdf.

5.3.3 Resultados y evidencia de mejora

Se desarrolla arquitectura de seguridad por roles (RBAC) y soluciones DLP (Data Loss Prevention).

- **Integridad:** Se desarrolló una trazabilidad del 100% de los accesos.
- **Disuasión:** Con el conocimiento de que se estaba auditando, las filtraciones se detuvieron completamente en el periodo de observación posterior.

- **Validación:** Confirma que la auditoría técnica es clave para avalar la seguridad jurídica y la ética pública.

Al practicar un Benchmarking de las tres verificaciones, emergen patrones estructurales que validan la universalidad del modelo de auditoría que propone la tesis.

5.3.4 Patrones de Hallazgos Comunes

La brecha de gobernanza: En los tres casos, el problema no era la inexistencia de las herramientas tecnológicas (Hardware), sino la inexistencia de la gestión (Management) con la desconexión entre los objetivos del negocio (educar, recaudar, fiscalizar) y la estrategia de TI como la causa raíz común.

El factor humano: La resistencia al cambio y las insuficiencias de competencias digitales del personal administrativo fueron siempre una barreras, validadas por el dominio 1.22 (capacitación).

Reactividad vs. proactividad: Las instituciones públicas peruanas solían invertir en seguridad post incidente crítico, lo que pone de relieve una baja madurez en la gestión de riesgos.

5.3.5 Conclusión de la Validación

El análisis cruzado indica que el Modelo de Auditoría diseñado en los Capítulos 1-4 es:

- **Flexible:** Para cumplir objetivos en materia de disponibilidad (Universidad), o de usabilidad (Municipio), o de confidencialidad (Agencia).
- **Predictivo:** Capaz de anticipar crisis de reputación antes de que ocurran.
- **Eficaz:** Las medidas derivadas de la auditoría generaron mejoras en la calidad del servicio en todos los casos.

CAPÍTULO VI

6 RESULTADOS, IMPACTO Y NIVEL DE MADUREZ INSTITUCIONAL

El presente capítulo materializa la síntesis integral y el análisis crítico de los resultados generados como producto de la intervención de auditoría y la ejecución piloto del Plan de Mejoras en la Universidad Nacional Autónoma de Chota (UNACH); el principal objetivo de este apartado es medir el "Delta de Mejora" (Δ) y para ello, la diferencia cuantitativa y cualitativa entre el estado de situación inicial de la gobernanza tecnológica (ex-ante) y el estado de situación actual (ex-post). Para poder objetivar dicha medida se hace uso del Modelo de Madurez de Capacidades (CMMI) y de los dominios de madurez de COBIT 2019, las cuales se pueden utilizar para medir el hecho de que esa institución haya sido capaz de pasar de un nivel de gestión "Ad-Hoc" o "Caótico" a uno "Definido" y "Gestionado". La presente evaluación va más allá de las métricas técnicas tradicionales (el uptime de servidores, por ejemplo) y lo que hace es correlacionar ambos aspectos con el incremento que puedan tener en la Calidad del Servicio Educativo, validando de este modo empíricamente la hipótesis que articula la investigación, que es que la madurez tecnológica como tal constituye un predictor causal directo de la eficiencia administrativa y la satisfacción estudiantil en el sector ti público (ISACA, 2018; CMMI Institute, 2020).

Por otro lado, el capítulo amplía la discusión, transcendiéndola al caso en concreto y colocando las brechas estructurales de TI del sector público peruano; sobre ello se realizan consideraciones respecto a los

resultados de la investigación y a partir de los informes de la OCDE sobre Gobierno Digital en el Perú y la Ley de Gobierno Digital, estableciendo las barreras sistémicas que encuentran la rigidez presupuestal, la brecha de talento humano y la resistencia cultural al cambio; finalmente se sistematizan las Lecciones Aprendidas bajo un fundamento de Gestión del Conocimiento, trasformando así la experiencia de la auditoría institucional en capital intelectual institucional. El presente análisis no sólo establece una hoja de ruta para la sostenibilidad de las mejoras realizadas en la UNACH, sino un modelo de referencia que se puede replicar para otras entidades que pertenezcan al sistema universitario nacional que busque cumplir con las Condiciones Básicas de Calidad que exige la SUNEDU y como forma de garantizar la pertinencia social y académica de la inversión tecnológica (Organisation for Economic Cooperation and Development OECD, 2020).

6.1 Nivel de cumplimiento por norma

La parte 6.1 desglosa la progresión que ha tenido la universidad en tres dominios normativos críticos que fueron auditados, siguiendo una escala de madurez de 0-5.

6.1.1 Evolución en seguridad de la información (ISO/IEC 27001)

La evolución de la postura de seguridad de la información en el estándar ISO/IEC 27001 no es únicamente una actualización tecnológica, sino una transformación estructural que cambia la visión del contexto de protección emergente, reactiva y fragmentada a un Sistema de Gestión de Seguridad de la Información (SGSI) vivo, preventivo, acorde con la

estrategia de la organización. Esta evolución de la postura se basa epistemológicamente en el ciclo de mejora continua (Planificar-Hacer-Verificar-Actuar) y en la gestión basada en riesgos, lo que permite a la organización pasar de escalones iniciales de control técnico a otros escalones superiores de ciber-resiliencia y gobernanza ágil, manteniendo por tanto la tríada confidencialidad - integridad - disponibilidad como patrimonios intangibles de continuidad y legitimidad institucional (Calder, 2017; Humphreys, 2016).

Diagnóstico inicial (nivel 1 - inicial/ad hoc): la seguridad informática era un proceso inexistente antes de la auditoría, ya que dependía exclusivamente de configuraciones forzadas en cada estación de trabajo (antivirus gratuitos, firewalls desactivados).No se realizaba segregación de las redes (VLANs), de tal forma que un malware existente en una sala de alumnos podía infectar los servidores administrativos. El riesgo de fuga de la información de notas era crítico.

Estado actual (nivel 3 - definido): En esta fase de intervención ya se había aprobado y puesto en circulación la Política de Seguridad de la Información (PSI) mediante la resolución del rector. Se había puesto en marcha un Directorio Activo (AD) para la gestión centralizada de las identidades y accesos, eliminando así las cuentas genéricas. Se había segmentado la red lógica, así como se habían puesto en funcionamiento protocolos de cifrado de las bases de datos sensibles de la universidad.

Resultado cuantitativo: El grado de cumplimiento de los controles del Anexo A de ISO 27001 pasó del 15% al 65% en un plazo de seis meses.

6.1.2 Evolución en continuidad del negocio (ISO 22301)

La maduración de la capacidad de continuidad de la Universidad Nacional Autónoma de Chota (UNACH) no representa solo una mejora en la calidad de los mecanismos de respaldo de datos, sino que es un cambio de paradigma desde la gestión de la recuperación ante desastres DR (Disaster Recovery) centrada en la restauración tecnológica de los servidores hacia la gestión de la continuidad del negocio BCM (Business Continuity Management) entendida como un enfoque global de la resiliencia organizacional.

De acuerdo con la norma ISO 22301:2019, esta maduración implica el paso de una visión reactiva y de contingencia a una estructura centrada en el análisis de impacto en el negocio BIA (Business Impact Analysis) que permite a la institución poder identificar sus procesos críticos y dar continuidad a la operatividad mínima aceptable ante interrupciones disruptivas. Este salto cualitativo transforma la continuidad de un "artilugio seguro" a un imperativo estratégico garantizador de la sostenibilidad del servicio educativo y de la confianza de las partes interesadas (Al Hour, A, 2012; International Organization for Standardization ISO, 2019).

Diagnóstico inicial (nivel 0 - inexistente): En la universidad no existía red de seguridad.Las copias de seguridad (backups) se realizaban de forma manual en discos duros externos, sujetas a fallos físicos o robo, y en ningún caso se había realizado ninguna prueba de restauración. El Tiempo de Recuperación (RTO) ante un desastre era indeterminado y la culminación del semestre académico quedaba en peligro.

Estado actual (nivel 2 - repetible): Se automatizó el proceso de backup, aplicando la regla 3-2-1 (3 copias, 2 medios, 1 fuera de sitio/nube). Se ejecutó el primer simulacro de recuperación de datos críticos y fue posible restaurar el Sistema de Gestión Académica en un tiempo controlado.

Resultado cuantitativo: Reducción del RTO de "Indeterminado" a 4 horas para servicios críticos.

6.1.3 Evolución en gestión de servicios (ISO/IEC 20000 / ITIL)

La maduración de la capacidad de continuidad de la gestión de los servicios de TI ITSM (Information Technology Service Management) implica el abandono de un paradigma tecnocéntrico clásico del éxito del uptime del hardware, aun cuando el mismo se orientará hacia una con la creación de valor alineado a la estrategia del negocio, de acuerdo con ISO/IEC 20000-1:2018 e ITIL 4 conforme lo indica el marco. Este tránsito evolutivo reconfigura al departamento de TI, del centro de costos operativo a compañero estratégico del ciclo de vida del servicio desde la demanda hasta el valor entregado al estudiante. La introducción de un SGI (sistema de gestión de incidencias) estandarizado permite el tránsito de la gestion artesanal de incidencias a una cultura del proceso de mejora continua y eficacia procesal, donde la calidad se cuantifica mediante los acuerdos de nivel de servicio SLA (service level agreement) y la satisfacción final del usuario es la medida indicadora del desempeño institucional (Agutter, 2019; Axelos, 2019).

Diagnóstico inicial (nivel 1 - reactivo): El soporte técnico era informal; las solicitudes se realizaban por pasillo o WhatsApp personal de los

técnicos, sin registro de las mismas y sin priorización. Esto suponía una percepción de "favoritismo" y desinterés en el usuario final.

Estado actual (nivel 3 - definido): Ya se había creado una Mesa de Asistencia (Service Desk) oficial con una herramienta de Ticketing y también se habían creado Catálogos de Servicios y Acuerdos de Nivel de Servicio (SLA) explícito para los docentes y administrativos.

Resultado cuantitativo: Se logró la capacidad de la trazabilidad del 100% de los incidentes, lo cual permite identificar patrones de fallas recurrentes de forma más eficiente.

6.2 Indicadores institucionales posteriores a la intervención

Bajo esta subsección, se muestra mediante estadística la correlación entre la mejora técnica (Causa) y la satisfacción del estudiante (Efectos).

6.2.1 Indicadores de Eficiencia Operativa (KPIs Técnicos)

La medición del rendimiento de la infraestructura tecnológica de la UNACH no debe sustentarse en sensaciones subjetivas, sino en métricas cuantitativas rigurosas a las que comúnmente se les denomina KPIs (*Key Performance Indicators*). Dentro del área de la gestión de servicios de TI (ITSM), un KPI técnico se puede definir como una brújula de navegación que recoge la «salud fisiológica» de los sistemas para poder distinguir la disponibilidad nominal de la disponibilidad real del servicio.

Siguiendo las líneas de ITIL 4, la evaluación se llevará a cabo para indicadores de rezago (*lagging*) y de tendencia (*leading*); en este sentido, los más significativos para el ámbito universitario son los siguientes:

1. **MTTR (*Mean Time to Restore*):** Tiempo medio para restaurar este es el tiempo medio que le lleva al equipo de TI restablecer un servicio tras una caída. Un MTTR alto indica que, para el tipo de fallos, la empatía necesaria para la detección y tratamiento de ellos no se adopta.
2. **MTBF (*Mean Time Between Failures*):** Tiempo medio entre fallos el tiempo medio entre dos fallos consecutivos. Este indicador hace referencia a la fiabilidad y estabilidad de la arquitectura que subyace.
3. **Disponibilidad del servicio (%):** proporción entre el tiempo que el sistema (por ejemplo, aula virtual) está activo por el tiempo que se pactó.

La adopción por parte del entorno universitario aleja a la gestión de TI de un enfoque con un carácter artesanal a otro, basado en evidencia, es decir, en el que se pueden justificar las decisiones respecto a la inversión sobre el mantenimiento desde la aritmética (Axelos, 2019; Marr, 2012).

Estos indicadores informan del rendimiento "duro" de la infraestructura tecnológica.

Disponibilidad del sistema de matrícula:

Línea base: 85% (interrupciones acumuladas de 12 horas en semana crítica).

Post-auditoría: 99.8% (interrupciones menores a 15 minutos). Esto se logró mediante la optimización de consultas SQL y balanceo de carga web.

Tiempo Medio de Resolución (MTTR):

Línea base: Desconocido (estimado empíricamente en >48 horas).

Post-Auditoría: 4 horas para incidentes de prioridad alta según lo establecido en el SLA.

6.2.2 Indicadores de Percepción de Calidad (NPS y SERVQUAL)

Los indicadores de percepción de calidad (NPS y SERVQUAL) juegan un papel esencial en esta etapa, el hecho es que los KPIs que evalúan la calidad objetiva (lo que hace la máquina), los indicadores de percepción de calidad evalúan la calidad subjetiva (lo que siente el usuario). Al auditar los servicios educativos, muchas veces el resultado es una "disonancia cognitiva" en la que los sistemas funcionan técnicamente bien (KPIs en verde), pero tanto los estudiantes como los docentes tienen una sensación de insatisfacción. Para tratar de objetivar esto, se recurre a modelos psicométricos estandarizados.

El modelo por el que se inclinan los autores es el SERVQUAL parametrizado por los autores Parasuraman, Zeithaml y Berry. Este modelo teórico descompone la calidad del servicio en la distancia (*Gap*)

entre las expectativas del usuario (lo que espera el estudiante del uso de la tecnología universitaria) y la percepción que tiene del servicio recibido. Se puede concluir que el uso de estos instrumentos permite a la UNACH auditar no solo la infraestructura, sino que también es posible auditar la "Experiencia del Usuario" (UX), es decir se puede identificar las carencias en la producción de valor percibido independientemente de que la tecnología posea altos niveles de solución técnicamente (Parasuraman y otros, 1988; Van Grembergen & De Haes, 2018).

Realización de encuesta de satisfacción post-intervención a una muestra representativa de estudiantes para medir el efecto en la "calidad percibida".

6.2.3 Net Promoter Score (NPS) Tecnológico

El Net Promoter Score (NPS) que es originalmente un concepto comercial de fidelidad, se ha adaptado en la gestión de la TI actual (*eNPS o Tech*-NPS) para medir la fidelidad y satisfacción que tiene el usuario interno. La base de la metodología que desarrolló Reichheld se apoya en una única pregunta clave: "En una escala del 0 al 10, ¿qué tanto recomendaría este servicio tecnológico a un compañero para realizar su trabajo?".

En lo que respecta a la UNACH, el NPS clasifica a la comunidad universitaria en tres fracciones:

- **Detractores (0-6):** Son las personas que deben usar el servicio tecnológico, pero están frustradas con el mismo, lo que los lleva a

hablar del servicio en términos denigrantes, lo que genera un riesgo reputacional para el área de TI.

- **Pasivos (7-8):** Personas que están satisfechas con el servicio, pero lo hacen en términos indiferentes y expuestos a utilizaciones de un servicio alternativo.
- **Promotores (9-10):** Personas que consideran que se cuenta con un servicio informático de calidad, y terminarán siendo embajadores del cambio tecnológico.

El cálculo del indicador:

$$NPS = \%Promotres - \%Detractores$$

Este es un indicador que permite una métrica ejecutiva de alto nivel con relación directa con el uso del TI y la madurez digital institucional (Reichheld, 2003; Satmetrix, 2021).

El índice pasó de una zona crítica de -20 (Detractores > Promotores) a una zona positiva de +35: los estudiantes destacan ahora "estabilidad" y "rapidez" como principales atributos del servicio.

6.2.4 Dimensión de tangibilidad

La dimensión tangible (tangibles) dentro del SERVQUAL resulta ser paradójica en las TI porque el software en sí mismo es, por definición, intangible. Sin embargo, la misma dimensiona la "evidencia física" del servicio. En la operacionalización de la auditoría informática universitaria, la tangibilidad está constituida por una serie de elementos visibles con los que los propios usuarios asocian la calidad técnica.

Esto es, la apariencia y ergonomía de los laboratorios de cómputo, la modernidad de las (UI) de los portales académicos, la velocidad de carga visible; y, por último, la apariencia profesional y el equipamiento del personal de soporte técnico. Los estudiantes, a partir de las señales visibles citadas, asocian la competencia técnica "invisible" del departamento de sistemas con la teoría de la evidencia de servicio. Una infraestructura física descuidada, interfaces obsoletas o simplemente poco agradables dan una rápida señal de incompetencia aun cuando el código que se ejecuta sea robusto (Parasuraman y otros, 1991; Zeithaml y otros, 2009).

El 85% de los encuestados afirman que la nueva interfaz del Portal del Estudiante y la estabilidad del Aula Virtual mejoran su experiencia de aprendizaje y disminuyen la ansiedad durante los exámenes, y brechas estructurales de TI en la administración pública.

Este subtema incrementa el tono académico de la tesis, considerando las barreras sistémicas que impiden la sostenibilidad de los logros del Estado.

6.2.5 La Brecha de Talento Digital (Human Capital Gap)

La Brecha de Talento Digital se entiende como la diferencia estructural entre las capacidades tecnológicas que una determinada organización necesita para materializar su estrategia de transformación digital y las competencias efectivas que tiene la plantilla de personal en el presente. En el sector público universitario, esta problemática presenta un riesgo estratégico más serio que la obsolescencia de la infraestructura informática.

El análisis de la brecha se articula a partir de marcos de referencia de competencias como el SFIA (*Skills Framework for the Information Age*). La auditoría suele poner de manifiesto que, si bien la universidad adquiere tecnologías punteras (Nube, Big Data), la relación entre la capacidad humana y la técnica se encuentra estancada en paradigmas de mantenimiento de legados. Esa diferencia produce "un retorno de la inversión negativo", en el cual las herramientas homologadas quedan infrautilizadas por falta de expertise. Reducir la brecha no se produce solo a partir de la contratación, sino que también se lleva a cabo a partir de estrategias muy agresivas de *Reskilling* (reciclaje profesional) y *Upskilling* (perfeccionamiento), ajustando el perfil del personal de TI al de la Educación 4.0 (SFIA Foundation, 2021; World Economic Forum, 2020).

A pesar de las mejoras en cuanto a infraestructura, la auditoría hizo patente una fragilidad del recurso humano. El régimen laboral del sector público y los topes salariales dificultan la permanencia de especialistas en ciberseguridad o arquitectos de datos, que se pasan al sector privado.

Implicancia: El riesgo de un retroceso en la madurez es alto si el esfuerzo del personal clave: (Key People Risk) se retira de la institución. La capacitación continua es la única medida de mitigación posible en el corto plazo.

6.2.6 La rigidez del sistema nacional de presupuesto

Se certificó una distorsión en la inversión tecnológica. El sistema público favorece la inversión en hardware (Activos Fijos / CAPEX)

porque es tangible y auditable, pero restringe el gasto en software, soporte y capacitación (Gasto Corriente / OPEX).

Implicancia: Lo que provoca la creación de "cementerios tecnológicos", servidores nuevos que funcionan con software obsoleto o pirata, por no contar con presupuesto para licencia o mantenimiento (OECD, 2020).

6.2.7 Silos de información y cultura organizacional

La resistencia al cambio fue el hallazgo transversal más complejo. Distintas facultades mantenían sus propios registros en hojas de cálculo ("Shadow IT"), por desconfianza en el sistema central, o deseo de mantener cuotas de poder.

Implicancia: La tecnología, por sí sola, no resuelve problemas políticos. La interoperación técnica (conectar sistemas) requiere de la interoperabilidad política (voluntad de compartir datos)

6.3 Lecciones aprendidas

Sistema de la experiencia, una forma de transformar la auditoría en un activo del conocimiento institucional.

1. La tecnología debe seguir a la estrategia: El estudio de la realidad tuvo como resultado que la compra de tecnología sin comprobar antes cómo iban los trámites administrativos no sirve para nada, ya que solo automatiza el caos. Las mejoras más importantes en la matrícula no fueron a base de comprar más servidores, luego por simplificar el flujo del trámite administrativo.

2. El liderazgo del rectorado es el factor crítico de éxito: Las políticas de seguridad no se cumplen si no son impulsadas por la alta dirección. La dirección del área informática no podría imponer controles sobre docentes y decanos si no está el detrás político del rector.
3. La comunicación es parte de la solución técnica: Aprendimos que gestionar las expectativas del estudiante es tan importante como gestionar los servidores. Por ejemplo, la automatización de alertas tempranas y comunicados sobre mantenimientos produjeron una reducción del 60% de quejas relacionadas en las redes sociales, mejorando la imagen institucional de la universidad.
4. De la auditoría puntual a la auditoría continua: Debemos abandonar el actual modelo de auditorías anuales con el fin de adaptarnos a la velocidad de la tecnología. Debemos pasar a un modelo de monitoreo continúo automatizado para mantener el nivel de madurez alcanzado.

CONCLUSIONES DEL TOMO II

En la UNACH, la gestión tecnológica presenta una discordancia estructural entre la creciente demanda de servicios digitales y una oferta institucional signada por la obsolescencia técnica y la ausencia de gobernanza. Esta brecha va más allá de lo técnico y se convierte en una limitante para el cumplimiento de las Condiciones Básicas de Calidad (CBC), consignadas en la Ley Universitaria, que a su vez afecta la competitividad institucional. En el ámbito académico, se observa consenso en que existe una relación positiva entre la madurez del Gobierno TI y la calidad del servicio, lo que hace necesaria la adopción de marcos internacionales como COBIT o ISO que incidan en tiempos de respuesta y satisfacción de usuarios.

La investigación concluye en que la vulnerabilidad institucional no está dada por la falta de hardware, sino que responde a una débil gobernanza de TI caracterizada por la desalineación del Rectorado con el área tecnológica y la existencia de silos de información y *Shadow IT*. En el presente, la universidad concibe umbrales primitivos de madurez ("Ad hoc" o "Repetible") en la operación, lo que propicia un riesgo residual inusitadamente elevado, inconveniente que expone la información académica a amenazas incesantes o latentes. Por lo cual, se plantea la vigencia de un modelo proactivo; un Plan de Mejoras que encuentre su base en los estándares de calidad ISO 9001 y en las metodologías PMI.

En el plano operativo, la seguridad de la información se presenta como un inquebrantable precepto legal que formula el establecimiento de un SGSI bajo la norma ISO 27001, el cual salva los registros y los datos de

carácter personal. Igualmente, la resiliencia institucional depende de la forja de Planes de Recuperación de Desastres (DRP's) con RTO's establecidos, las cuales evitan paradas para evitar los riesgos del calendario académico.Se concluye, una vez más, que la ausencia de arquitectura de datos y clasificación de la información contraviene las buenas prácticas de DAMA-DMBOK, poniendo a la entidad en riesgo de fugas críticas de la integridad.

La calidad considerada por el usuario final está directamente relacionada con la eficacia del helpdesk bajo el marco de ITIL y la estabilidad del software, lo que significa que depende de un ciclo de vida de desarrollo (SDLC) riguroso y de controles de calidad (QA) que impidan la deuda técnica. Las inversiones en la infraestructura a la hora de tomar decisiones se deben realizar desde el enfoque del Costo Total de Propiedad (TCO) y no solo considerando el precio, garantizando la necesaria estandarización para el soporte técnico. El paso de un monitoreo reactivo a uno proactivo permitirá prevenir y resolver cuellos de botella antes de que eso impacte a la persona que estudia y garantizar la disponibilidad de los servicios de mayor impacto.

Por último, la hipótesis general queda confirmada: existe una relación positiva, significativa y de causalidad entre el incremento de la madurez de los controles de TI y la mejora en la calidad del servicio percibida. La modernización de la gestión documental a través de la firma digital y el cierre de la brecha de competencia digital del personal son habilitadores de la política de "Cero Papel" y la protección de los activos. En conclusión, la auditoría de TI se valida como una inversión estratégica esencial para la competitividad y la legitimación de la

universidad pública del siglo XXI, mejorando los KPI críticos, como la satisfacción del alumnado (NPS).

GLOSARIO

Acuerdo de Nivel de Servicio (SLA - Service Level Agreement): Contrato o un compromiso formalmente registrado entre el proveedor de los servicios de TI (Dirección de TI) y el usuario (Estudiante/Docente) donde se especifican las métricas de calidad como pueden ser, los tiempos de respuesta y la disponibilidad mínima del sistema.

Activos de información: Cualquier información o recursos que pueden ser, datos software, hardware, personas, etc. y que tienen responsabilidad para la organización y que deben ser protegidos.

Auditoría Basada en Riesgos (Risk-Based Audit): Es la metodología de auditoría que prioriza la opinión hacia áreas o procesos de mayor riesgo en cuanto a los objetivos estratégicos de la institución, optimizando así la utilización de los recursos de auditoría.

Arquitectura de información: Organización de los sistemas de información que permite definir cómo clasificar, etiquetar y relacionar los datos de forma que se facilite la búsqueda y la gestión.

Backup (copia de seguridad): Práctica que permite tener copias de los datos originales con el fin de permitir la recuperación de los mismos en caso de pérdida o daño de los datos originales como puede ser su

deterioro por un ataque cibernético. Deberá seguir la regla 3-2-1 (tres copias, dos medios, uno fuera de lugar).

Balanced scorecard (cuadro de mando integral): Herramienta de gestión estratégica que deja a la postre disponer el control de la organización (o del plan de mejoras) mediante los indicadores financieros, de clientes, de procesos internos y de aprendizaje.

Brecha de Capital Humano (Human Capital Gap): Desajuste entre las habilidades digitales de que dispone el personal actual y las que la organización necesita para la correcta operatividad de la tecnología.

Causa raíz: La razón básica o raíz de un problema o desviación, a diferencia de los síntomas, que si se elimina no vuelve a ocurrir.

CMMI (Capability Maturity Model Integration): Modelo de referencia que pretende ayudar a las organizaciones a mejorar sus procesos y que los categoriza en función del nivel de madurez (5 niveles) (Inicial, Gestionado, Definido, Cuantitativamente gestionado, Optimizado).

COBIT 2019: Marco de referencia para el gobierno y la gestión de la información y la tecnología empresarial, destinado a la alineación de la TI con los objetivos comerciales.

Condiciones Básicas de Calidad (CBC): estándares mínimos que impone la SUNEDU del Perú que las Universidades tienen que cumplir para el debido licenciamiento institucional.

Confidencialidad: propiedad de la seguridad de la información que garantiza que la misma no sea puesta a disposición ni revelada a individuos, entidades o procesos no autorizados.

Data Loss Prevention (Prevención de Datos DLP): Conjunto de herramientas y procedimientos para detectar y prevenir escapes, pérdidas o uso no autorizado de datos sensibles (como notas o datos personales) que se transmiten fuera de la red corporativa.

Deuda técnica: Coste que tiene una solución fácil y rápida en el ámbito del desarrollo de software o de infraestructuras, debido al esfuerzo adicional de re-trabajo que se podría haber ahorrado si se hubiera elegido un enfoque más adecuado que llevara más tiempo.

Diagrama de Ishikawa (Espina de Pescado): Herramienta visual para identificar y listar las posibles causas de un hallazgo, clasificándolas en personas, procesos, tecnología y entorno.

Disponibilidad: Garantía de que los sistemas, aplicaciones y datos están disponibles y en funcionamiento cuando los usuarios autorizados los necesitan. Se mide generalmente en porcentaje de tiempo activo (Uptime).

Escalabilidad: Capacidad de un sistema computacional para gestionar una cantidad creciente de trabajo (ej. más alumnos que se matriculan) añadiendo recursos al sistema.

Estudio de caso: Método de investigación que implica un estudio en profundidad y detallado de un fenómeno específico (la gestión de IT) en su contexto real (la universidad pública).

Firma digital: Tipo de firma electrónica que usa criptografía asimétrica para asegurar la autenticidad, integridad y no repudio de un documento digital, con plena validez jurídica (Ley de Gobierno Digital).

Firewall (Cortafuegos): Sistema de prevención y detección de intrusiones basado en redes informáticas que permite controlar y gestionar el tráfico de la red de acuerdo a las políticas de seguridad previamente definidas.

Gap Analysis (Análisis de Brechas): Técnica de evaluación que compara la situación actual de la organización (As-Is) con la situación deseada definida por un estándar (To-Be) (ej. ISO 27001).

Gobernanza de TI: El sistema mediante el cual se dirige y controla el uso de la tecnología de la información existente y futura que se implementa en dirección a una estrategia institucional. Incluye la evaluación y el control de los planes de TI para que respalden la estrategia institucional y el seguimiento de su cumplimiento.

Gobierno digital: Uso estratégico de las tecnologías digitales y de la información y los datos por parte del gobierno para proporcionar valor público, mejorar el servicio al ciudadano y optimizar la administración interna.

Hallazgo de auditoría: Resultado de la evaluación de la evidencia de auditoría obtenida frente a los criterios de auditoría. Puede ser conforme, no conforme u oportunidad de mejora.

Integridad: Propiedad que permite garantizar que la información no ha sido cambiada ni alterada de ningún modo no permitido, manteniéndose exacta y completa.

Interoperabilidad: Capacidad que tienen diferentes sistemas de información y organizaciones para poder colaborar entre sí (intercambiar información) sin las restricciones que condicionan las restricciones de acceso o de implementación.

ISO/IEC 27001: Norma internacional para especificar los requisitos para establecer, implementar, mantener y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información (SGSI).

ITIL (Information Technology Infrastructure Library): Conjunto de buenas prácticas para la gestión de servicios de TI, que se ocupa de la forma en la que los servicios tecnológicos pueden acompasarse con las necesidades del negocio.

KPI (Key Performance Indicator): Indicador clave de desempeño, es una métrica que podemos cuantificar y que se asigna a identificar qué tan bien la organización está logrando sus objetivos clave.

Ley 29733 (Ley de Protección de Datos Personales): Normativa nacional que protege el derecho fundamental de las personas a la

protección de la información personal y regula el tratamiento de la información por parte de entidades tanto públicas como privadas.

Materialidad: Concepto de auditoría relacionado con la importancia relativa de una información o error. Un error es material cuando su supresión o equivocación podría incidir indirectamente en los dictámenes tomados por el usuario de esa información correspondiente.

Matriz RACI: Herramienta de asignación de responsabilidades que permite determinar quién es Responsable (Responsible), quién es Rinde Cuentas (Accountable), quién es Consultado (Consulted) y quién es Informado (Informed) en cada una de las tareas.

Mesa de ayuda (Service Desk): Punto único de contacto entre el proveedor de servicios de TI y el usuario en el que se ocupan de gestionar incidentes y solicitudes de servicio.

Monitoreo continuo: Proceso automatizado de monitorización permanente acerca de los diferentes controles y riesgos de TI, lo que permite la detección casi en tiempo real de cualquier anomalía.

Net Promoter Score (NPS): Métrica utilizada para valorar la lealtad y satisfacción del cliente (estudiante) a partir de la probabilidad de que el usuario recomiende el servicio a otras personas.

No Conformidad (NC): Incumplimiento justificado de los requisitos establecidos en una norma o estándar para un producto. Intervención o cambio interno deducido que puede ser mayor (sistémico), o menor (aislado).

No repudio: Garantía jurídica y técnica que asegura que el emisor de un mensaje o firma no puede negar posteriormente haberlo enviado o firmado.

PMBOK (Project Management Body of Knowledge): Guía de estándares y mejores prácticas para la dirección de proyectos publicada por el Project Management Institute (PMI).

Plan de Continuidad de Negocio (BCP): Documento que describe la forma en la que la organización seguirá operando durante y después de una interrupción no planificada.

Quick Wins (Victorias Tempranas): Mejoras que se pueden implementar de forma rápida, de bajo coste y con un alto impacto visible, utilizadas para ganar confianza y tracción para un proyecto de cambio.

Riesgo inherente: Se entiende como el grado de riesgo propio de una actividad o proceso de no considerar los controles internos establecidos.

Riesgo residual: Indica el riesgo residual que se conserva tras la aplicación de los controles y medidas de mitigación.

RTO (Recovery Time Objective): El Tiempo Objetivo de Recuperación. El tiempo máximo que un sistema puede estar fuera de servicio, tras un desastre, antes de causar un daño considerado inaceptable.

SERVQUAL: El modelo multidimensional para medir la calidad del servicio a través de la evaluación de la brecha existente entre las expectativas del cliente y su percepción en cinco dimensiones: fiabilidad, capacidad de respuesta, seguridad, empatía y elementos tangibles.

Shadow IT (TI en la Sombra): Uso de sistemas, dispositivos, software, aplicaciones y servicios de TI, dentro de una organización, sin la aprobación explícita, del correspondiente departamento de TI.

Silos de información: Cuando los sistemas de gestión de información no están abiertos a la comunicación con otros sistemas, y los datos quedan restringidos a un departamento o facultad.

TCO (Total Cost of Ownership): Costo Total de Propiedad. Presupuesto que recoge no solo el importe de adquisición de un activo informático, sino también los costes de operación, mantenimiento y baja a lo largo de su vida útil.

Trazabilidad: Capacidad de un elemento (dato o activo) de determinar su frecuencia de uso, aplicación o ubicuidad de él (identificación mediante identificaciones registradas -Logs-).

Triangulación: Estrategia metodológica que hace uso de distintas fuentes de datos o métodos para estudiar un mismo fenómeno donde se incrementa la validez y confiabilidad de las conclusiones.

Usabilidad (UX): Facilidad con la cual las personas pueden utilizar una herramienta concreta o cualquier otro objeto fabricado por humanos a

los efectos de llegar a una finalidad concreta, y en software, esta usabilidad se refiere a la experiencia del usuario al utilizar la interfaz.

Vulnerabilidad: Debilidad en un activo o control que es susceptible de explotación por una o varias amenazas (por ejemplo, software desactualizado, contraseñas de usuario débiles).

BIBLIOGRAFÍA

Agutter, C. (2019). ITIL 4 Essentials: Your essential guide for the ITIL 4 Foundation exam and beyond. IT Governance Publishing. https://doi.org/https://www.amazon.com/ITIL%C2%AE-Essentials-essential-Foundation-beyond/dp/1787782182

Al Hour, A. (2012). Business Continuity Management: Choosing to survive. itgp. https://doi.org/https://www.amazon.com/-/es/Abdullah-Al-Hour/dp/B01JXS46ZY

Arcotel. (2023). Arcotel. Resolución de Comité Informático ARCOTEL-2023-0147. Agencia de Regulación y Control de las Telecomunicaciones.: https://www.arcotel.gob.ec/wp-content/uploads/downloads/2023/08/resolucio%CC%81n_de_comite_informa%CC%81tico_arcotel-2023-0147-signed.pdf

Arens, A. A., Elder, R. J., & Beasley, M. S. (2017). Auditing and assurance services: An integrated approach (16.ª ed.). Pearson. https://doi.org/https://digilib.stekom.ac.id/assets/dokumen/ebook/feb_44bac1dd499213de626e2f232c01e8542ffef3bc_1652001111.pdf

Auditool. (2025). Auditool. ¿Qué es un Comité de Auditoría y por qué es clave en el gobierno corporativo? : https://www.auditool.org/blog/control-interno

Axelos. (2017). Managing successful projects with PRINCE2 (6.ª ed.). TSO (The Stationery Office): https://www.axelos.com/certifications/prince2/prince2-6th-edition

Axelos. (2019). ITIL Foundation: ITIL 4 Edition. TSO (The Stationery Office). https://www.axelos.com/certifications/itil-service-management/itil-4-foundation

Beyer, B., Jones, C., Petoff, J., & Murphy, N. R. (2016). Site reliability engineering: How Google runs production systems. O'Reilly Media: https://sre.google/sre-book/table-of-contents/

Business Beam s.f. (2019). Business Beam. IT Governance Implementation using COBIT & ISO 38500: https://businessbeam.com/consulting/it-governance-implementation-using-cobit-iso-38500/

Calder, A. (2017). Nine steps to success: An ISO 27001 implementation overview (3rd ed.). IT Governance Publishing: https://hightable.io/product/iso-27001-templates/?gad_source=1&gad_campaignid=23005960220&gbraid=0AAAACbxnjrqQNTLrnnE8t2NunYiKp2Wo&gclid=Cj0KCQiA9OnJBhD-ARIsAPV51xO_QGzP-B3vGPD9PUeQcqlxijBFoDx56R2mGG34rNv6PcbyGpBnu7IaArr1EALw_wcB

Calle García, A. J., Mendoza Chila, G. Y., Ronquillo Morán, H. K., & Rivera Piloco, B. M. (2023). Auditoría de la gestión de tecnologías de la información en el sector público. Ciencia y Desarrollo, 27(1), 381-391. https://doi.org/10.21503/cyd.v27i1.2575

Center for Internet Security. (2021). CIS Controls Version 8. CIS.

Checklist Fácil. (2023). Checklist Fácil. Indicadores de gestión pública: cómo mejorar la transparencia en el sector público: https://es.checklistfacil.com/blog/indicadores-de-gestion-publica/

CIO Index s.f. (2025). CIOIndex. IT Governance Frameworks: An In-Depth Analysis Of COBIT, ISO/IEC 38500, ITIL, And More: https://cioindex.com/magazine/it-governance-frameworks-in-depth-analysis/

CMMI Institute. (2018). CMMI for Services, Version 2.0. CMMI Institute: https://www.cmmiinstitute.com/products/cmmi-old/dev-old

Committee of Sponsoring Organizations of the Treadway Commission COSO. (2017). Enterprise risk management: Integrating with strategy and performance. COSO.

Connolly, T., & Begg, C. (2015). Database systems: A practical approach to design, implementation, and management (6.ª ed.). Pearson. https://doi.org/https://www.academia.edu/41779665/Database_Systems_A_Practical_A_Thomas_Connolly

Consortium for Service Innovation. (2017). KCS v6 methodology. Consortium for Service Innovation. Consortium for Service Innovation: https://www.serviceinnovation.org/kcs/

Contraloría General del Estado GCE. (2023). Contraloría General del Estado Quito Ecuador. Acuerdo No. 004-CG-2023: Normas de Control Interno para las Entidades, Organismos del Sector Público y de las Personas Jurídicas de Derecho Privado que dispongan de recursos públicos.

Coombs, T. W. (2014). Ongoing crisis communication: Planning, managing, and responding (4.ª ed.). IEEE TRANSACTIONS ON PROFESSIONAL COMMUNICATION, 53(2), 174-178. https://doi.org/0.1109/TPC.2010.2046099

COSO ERM. (2017). Committee of Sponsoring Organizations of the Treadway Commission. Enterprise risk management: Integrating with strategy and performance: https://www.scirp.org/reference/referencespapers?referenceid=4072896

DAMA International. (2017). DAMA International. DAMA-DMBOK: Data management body of knowledge (2.ª ed.). Technics Publications: https://dama.org/content/body-knowledge

Dempsey, K., Chawla, N. S., Johnson, A., Johnston, R., Jones, A. C., Orebaugh, A., Scholl, M., & & Stine, K. (2011). Information security continuous monitoring (ISCM) for federal information systems and organizations (NIST Special Publication 800-137). U.S. Department of Commerce, 800-137. https://doi.org/https://doi.org/10.6028/NIST.SP.800-137

Denzin, N. K. (2012). Triangulation 2.0. Journal of Mixed Methods Research, 6(2), 80-88. https://doi.org/https://doi.org/10.1177/1558689812437186

DNV. (2017). Separation of duties and IT security. https://www.dnv.com/article/separation-of-duties-and-it-security-182590/

Dumas, M., La Rosa, M., Mendling, J., & Reijers, H. A. (2018). Fundamentals of Business Process Management (2nd ed.). Springer.

Elliott, D., Swartz, E., & Herbane, B. (2025). Business continuity management: A crisis management approach. . Routledge, 338. https://doi.org/https://www.academia.edu/127841310/Business_Continuity_Management_A_Crisis_Management_Approach

Ellram, L. M. (1995). Total cost of ownership: An analysis approach for purchasing. International Journal of Physical Distribution & Logistics Management, 8(25), 4-23. https://doi.org/10.1108/09600039510099928

Engebretson, P. (2013). The basics of hacking and penetration testing: Ethical hacking and penetration testing made easy (2.ª ed.). Syngress. https://doi.org/https://wqreytuk.github.io/Patrick+Engebretson+The+Basics+of+Hacking+and+Penetration+Testing,+Second+Edition+%282013%29.pdf

ETSI. (2016). Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates (EN 319 411-1 V1.1.1). European Telecommunications Standards Institute: https://www.etsi.org/deliver/etsi_en/319400_319499/31941101/01.01.01_60/en_31941101v010101p.pdf

EY Switzerland. (2025). EY. CISO Governance: Choosing the optimal Line of Defense: https://www.ey.com/en_ch/insights/cybersecurity/where-should-your-ciso-sit-in-the-three-lines-of-defense-model

Fowler, M. (2019). Refactoring: Improving the design of existing code (2.ª ed.). Addison-Wesley Professional. https://doi.org/https://dl.ebooksworld.ir/motoman/Refactoring.Improving.the.Design.of.Existing.Code.2nd.edition.www.EBooksWorld.ir.pdf

Gartner. (2020). IT Key Metrics Data 2021: Executive Summary. Gartner, Inc: https://www.gartner.com/en/documents/3994656

Grajek, S. (2020). 2020 Top 10 IT Issues: The Drive to Digital Transformation Begins. EDUCAUSE Review: https://er.educause.edu/articles/2020/1/top-10-it-issues-2020-the-drive-to-digital-transformation-begins

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 3(7). https://doi.org/https://doi.org/10.1016/j.heliyon.2017.e00346

Hadnagy, C. (2018). Social engineering: The science of human hacking (2.ª ed.). Wiley. https://doi.org/http://repo.darmajaya.ac.id/4637/1/Social%20Engineering_%20The%20Science%20of%20Human%20Hacking%20%28%20PDFDrive%20%29.pdf

HDI. (2028). The state of technical support in 2018. HDI: https://www.thinkhdi.com/

Heldman, K. (2021). PMP: Project management professional exam study guide (10.ª ed.). Sybex. https://doi.org/https://www.amazon.com/Project-Management-Professional-Study-Guide/dp/1119658977

Humphreys, E. (2016). Implementing the ISO/IEC 27001:2013 ISMS standard (2nd ed.). Artech House: https://www.newhorizons.edu.pe/cursos-y-certificaciones-internacionales/ciberseguridad/gad_source/1/gad_campaignid/22370597676/gbraid/0aaaaa-3cxlks2jeynjngu4dqydjgmdevd/gclid/cj0kcqia9onjbhd-arisapv51xoahkg1qe2gkppulabwwj2swv3bbqstfdmcxwmyummiuprjggpsxqka

International Federation of Accountants IFAC. (2018). International standard on auditing 320: Materiality in planning and performing an audit. IFAC: https://www.ibr-ire.be/docs/default-source/fr/documents/reglementation-et-publications/normes-et-recommandations/isa/isa-english-version/isa-320_en.pdf?sfvrsn=e927e4d9_1

International Organization for Standardization ISO. (2015). Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements (ISO/IEC Standard No. 17021-1:2015). https://www.iso.org/standard/61651.html

International Organization for Standardization ISO. (2017). Information technology — IT asset management — Part 1: IT asset management systems — Requirements (ISO/IEC Standard No. 19770-1:2017). https://www.iso.org/standard/68535.html

International Organization for Standardization ISO. (2018). Information technology — Service management — Part 1: Service management system requirements (ISO/IEC Standard No. 20000-1:2018). https://www.iso.org/standard/70636.html

International Organization for Standardization ISO. (2019). Quality management — Guidelines for competence management and people development (ISO Standard No. 10015:2019). https://www.iso.org/standard/69458.html

International Organization for Standardization ISO. (2020). Project, programme and portfolio management — Context and concepts (ISO Standard No. 21500:2021). Project, programme and portfolio management — Context and concepts (ISO Standard No. 21500:2021): https://www.iso.org/standard/50003.html

International Organization for Standardization ISO. (2022). ISO/IEC. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. International Organization for Standardization.

ISACA. (2018). COBIT 2019 Framework: Governance and Management Objectives. ISACA.

ISACA. (2019). Framework: Governance and Management Objectives. Information Systems Audit and Control Association. COBIT. https://doi.org/https://cyberranges.com/whitepaper-download-understanding-cyber-ranges-from-hype-to-reality/?utm_source=google&utm_medium=search&utm_campaign=ecso-white-paper&utm_id=general-ecso&gad_source=1&gad_campaignid=22362881191&gbraid=0AAAAACyrLDqPmC5Gkm6FmR01duVi

Joint Task Force Transformation Initiative. (2012). Guide for conducting risk assessments (NIST Special Publication 800-30 Rev. 1). U.S. Department of Commerce: https://doi.org/10.6028/NIST.SP.800-30r1

Kaplan, R. S., & Norton, D. P. (1996). he Balanced Scorecard: Translating Strategy into Action. Harvard Business School Press: https://www.google.com/aclk?sa=L&ai=DChsSEwirlLP3w7aRAxUWpFoFHS1nAxUYACICCAEQAhoCdnU&ae=2&co=1&ase=2&gclid=Cj0KCQiA9OnJBhD-ARIsAPV51xNSzCv9h10acYoO91lJr-NuETXTsDK0bvrp0VHOOp3YSwx-qTOFNUMaArGvEALw_wcB&cid=CAASuwHkaJVw2ds9dQN0aDn07DKLXziwKPrVqTUtbS-w7IUK_O8

Kaushik, A. (2013). Web analytics 2.0: The art of online accountability and science of customer centricity. Sybex. https://doi.org/https://nashnw.myqnapcloud.com:8083/download/43/pdf/43.pdf

Kerzner, H. (2022). Project management: A systems approach to planning, scheduling, and controlling (13.ª ed.). Wiley. https://doi.org/https://www.academia.edu/123134596/Project_management_a_systems_approach_to_planning_scheduling_and_controlling

Kirkpatrick, J. D., & Kirkpatrick, W. K. (2016). Kirkpatrick's four levels of training evaluation. ATD Press. https://doi.org/https://www.amazon.com/Kirkpatricks-Four-Levels-Training-Evaluation/dp/1607280086

Kotter, J. P. (2012). Leading change. Harvard Business Review Press: https://www.scirp.org/reference/referencespapers?referenceid=2233874

Laudon, K. C., & Laudon, J. P. (2020). Management information systems: Managing the digital firm (16.ª ed.). Pearson. https://doi.org/https://www.scirp.org/reference/referencespapers?referenceid=3794844

Laudon, K. C., & Traver, C. G. (2021). E-commerce 2021-2022: Business, technology, society (16.ª ed.). Pearson. https://doi.org/https://www.pearson.com/en-us/subject-catalog/p/e-commerce-2021-business-technology-and-society/P200000001390/9780136931829

Laudon, K. C., & Traver, C. G. (2021). E-commerce 2021-2022: Business, technology, society (16.ª ed.). Pearson. https://doi.org/https://www.pearson.com/en-us/subject-catalog/p/e-commerce-2021-business-technology-and-society/P200000001390/9780136931829

Limoncelli, T. A., Chalup, S. R., & Hogan, C. J. (2014). The practice of cloud system administration: Designing and operating large distributed systems. Addison-Wesley. https://doi.org/https://ptgmedia.pearsoncmg.com/images/9780321943187/samplepages/9780321943187.pdf

Loeliger, J., & McCullough, M. (2012). Version control with Git (2.ª ed.). O'Reilly Media. https://doi.org/https://www.oreilly.com/library/view/version-control-with/9781449345037/

Marr, B. (2012). Key Performance Indicators (KPI): The 75 measures every manager needs to know. Pearson UK.

Meredith, J. R., Shafer, S. M., & Mantel, J. (2017). Project management: A managerial approach (10.ª ed.). Wiley. https://doi.org/https://www.academia.edu/8973287/Project_Management_A_Managerial_Apprach_Jack_R_Meredith_and_Samuel_J_Mantel_Wiley_

Miller, D. R., Harris, S., & Harper, A. (2021). Gray Hat Hacking: The Ethical Hacker's Handbook (6.ª ed.). McGraw-Hill. https://doi.org/https://pages.cs.wisc.edu/~ace/media/gray-hat-hacking.pdf

Ministerio del Trabajo. (2024). Ministerio del Trabajo. Plan Estratégico Institucional: https://www.trabajo.gob.ec/wp-content/uploads/2024/01/plan-estrategico.pdf

Monczka, R. M., Handfield, R. B., Giunipero, L. C., & & Patterson, J. L. (2020). Purchasing and supply chain management (7.ª ed.). Cengage Learning. https://doi.org/https://www.cengage.com/c/purchasing-and-supply-chain-management-7e-monczka-handfield-giunipero-patterson/9780357442142/

Murugesan, S., & Gangadharan, G. R. (2012). Harnessing Green IT: Principles and practices. Wiley. https://doi.org/https://onlinelibrary.wiley.com/doi/book/10.1002/9781118305393

National Institute of Standards and Technology (NIST). (2020). Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53 Revision 5). U.S. Department of Commerce, 800-53. https://doi.org/https://doi.org/10.6028/NIST.SP.800-53r5

Noe, R. A. (2017). Employee training and development (7.ª ed.). McGraw-Hill Education. https://doi.org/10.1002/hrdq.21333

Organisation for Economic Cooperation and Development OECD. (2020). The OECD Digital Government Policy Framework: Six dimensions of a Digital Government. OECD Public Governance Policy Papers: https://doi.org/10.1787/f64fed2a-en

OWASP . (2021). OWASP Top 10:2021. OWASP Foundation (Open Web Application Security Project): https://owasp.org/Top10/

Parasuraman, A. P., Zeithaml, V. A., & Berry, L. L. (1988). SERVQUAL: A multiple-item scale for measuring consumer perceptions of service quality. Journal of Retailing, 64(1), 12-40. https://doi.org/https://www.researchgate.net/publication/200827786_SERVQUAL_A_Multiple-item_Scale_for_Measuring_Consumer_Perceptions_of_Service_Quality

Parasuraman, A., Berry, L. L., & Zeithaml, V. A. (1991). Refinement and reassessment of the SERVQUAL scale. Journal of Retailing, 67(4), 420. https://doi.org/https://www.researchgate.net/publication/304344168_Refinement_and_reassessment_of_the_SERVQUAL_scale

Parasuraman, A., Zeithaml, V. A., & Berry, L. L. (1988). SERVQUAL: A multiple-item scale for measuring consumer perc. of service quality. Journal of Retailing, 1(64), 12-40. https://doi.org/https://www.researchgate.net/publication/200827786_SERVQUAL_A_Multiple-item_Scale_for_Measuring_Consumer_Perceptions_of_Service_Quality

Peltier, T. R. (2026). Information Security Policies, Procedures, and Standards: A Practitioner's Reference. CRC Press. https://doi.org/https://doi.org/10.1201/9780849390326

Power, M. (2007). Organized uncertainty: Designing a world of risk management. Oxford University Press. https://doi.org/10.1111/j.1467-9299.2008.00756_2.x

Presidencia del Consejo de Ministros. (2019). Modelo de Gestión Documental en el marco del Gobierno Digital. PCM - Secretaría de Gobierno Digital. https://www.gob.pe/institucion/pcm/informes-publicaciones/325721-modelo-de-gestion-documental-mgd

Pressman, R. S., & Maxim, B. R. (2020). Software engineering: A practitioner's approach (9.ª ed.). McGraw-Hill Education. https://doi.org/https://www.mheducation.com/highered/product/software-engineering-a-practitioners-approach-pressman.html?viewOption=student

Pressman, R. S., & Maxim, B. R. (2020). Software Engineering: A Practitioner's Approach (9th ed.). McGraw-Hill Education. https://doi.org/https://www.researchgate.net/publication/365946272_Software_Engineering_A_Practitioner's_Approach_9_th_Edition

Project Management Institute (PMI). (2021). A Guide to the Project Management Body of Knowledge (PMBOK® Guide) – Seventh Edition and The Standard for Project Management. Project Management Institute: https://www.pmi.org/pmbok-guide-standards/foundational/pmbok

Project Management Institute. (2021). A guide to the project management body of knowledge (PMBOK guide) (7.ª ed.). Project Management Institute. https://doi.org/https://www.pmi.org/pmbok-guide-standards/foundational/pmbok

Project Management Institute. (2021). A guide to the project management body of knowledge (PMBOK guide) (7.ª ed.). Project Management Institute. https://doi.org/https://tegnum.edu.pe/wp-

content/uploads/2023/09/Project-Management-Institute-A-Guide-to-the-Project-Management-Body-of-Knowledge-PMBOK-R-Guide-PMBOK%C2%AE%EF%B8%8F-Guide-Project-Management-Institute-2021.pdf

Reichheld, F. F. (2003). The One Number You Need to Grow. Harvard Business Review, 81(12), 46-54. https://doi.org/https://hbr.org/2003/12/the-one-number-you-need-to-grow

Rosenfeld, L., Morville , P., & Arango, J. (2015). Information architecture: For the web and beyond (4.ª ed.). O'Reilly Media. https://doi.org/https://e-edu.nbu.bg/pluginfile.php/62325/mod_resource/content/1/Information_Architecture_For_The_Web_And_Beyond_Fourth_Edition.pdf

Santoso, H., Girsang, A. S., & Suroso, J. S. (2017). Analysis of digital signature security on document management system. 2017 International Conference on Information Management and Technology. ICIMTech, 172-176. https://doi.org/https://doi.org/10.1109/ICIMTech.2017.8273531

Satmetrix. (2021). The Net Promoter Score Benchmark Study. Nice Satmetrix.

Schwaber, K., & Sutherland, J. (2020). The Scrum guide: The definitive guide to Scrum: The rules of the game. Scrum: https://scrumguides.org/

Schwalbe. (2019). Information technology project management (9.ª ed.). Cengage Learning. https://doi.org/https://www.cengage.com/c/information-technology-project-management-9e-schwalbe/9781337101356/

SFIA Foundation. (2021). The SFIA Framework 8 reference guide. SFIA Foundation: https://sfia-online.org/

Silic, M., & Back, A. (2014). Shadow IT: A view from behind the curtain. . Computers & Security, 45, 274-283. https://doi.org/https://doi.org/10.1016/j.cose.2014.06.001

Snedaker, S., & Rima, C. (2013). Business continuity and disaster recovery planning for IT professionals (2.ª ed.). Syngress. https://doi.org/https://wqreytuk.github.io/Patrick+Engebretson+The+Basics+of+Hacking+and+Penetration+Testing,+Second+Edition+%282013%29.pdf

Sommerville, I. (2016). Software engineering (10.ª ed.). Pearson. https://doi.org/https://dn790001.ca.archive.org/0/items/bme-vik-konyvek/Software%20Engineering%20-%20Ian%20Sommerville.pdf

Souppaya, M., & Scarfone, K. (2018). Guide to enterprise patch management planning: Preventive maintenance for technology. NIST Special Publication 800-40 Rev. 3. https://doi.org/https://doi.org/10.6028/NIST.SP.800-40r3

Stake, R. E. (2013). Multiple case study analysis. Guilford Press: https://www.guilford.com/excerpts/stake.pdf?srsltid=AfmBOorJyVhIqxgTghQfNNt4QY_aJhuSW88BlEIvSzsdaAhtraQ0sZSM

Stallings, W. (2016). Foundations of modern networking: SDN, NFV, QoE, IoT, and Cloud. Addison-Wesley Professional. https://doi.org/https://ptgmedia.pearsoncmg.com/images/9780134175393/samplepages/9780134175393.pdf

Stallings, W. (2017). Cryptography and network security: Principles and practice (7.ª ed.). Person. https://doi.org/http://staff.ustc.edu.cn/~mfy/moderncrypto/crypto7ed.pdf

Stallings, W. (2019). Computer organization and architecture: Designing for performance (11.ª ed.). Pearson. https://doi.org/https://os.ecci.ucr.ac.cr/ci0114/material/Stallings/Computer-Organization-Architecture-11th.pdf

Stallings, W., & Brown, L. (2018). Computer Security: Principles and Practice. Pearson. https://doi.org/https://unidel.edu.ng/focelibrary/books/Computer%20Security%20_%20Principles%20-%20WILLIAM%20STALLINGS_2089.pdf

Swanson, M., Bowen, P., Phillips, A., Gallup, D., & Lynes, D. (2010). Contingency Planning Guide for Federal Information Systems (NIST Special Publication 800-34 Revision 1). National Institute of Standards and Technology (NIST), 800-34. https://doi.org/https://doi.org/10.6028/NIST.SP.800-34r1

Tanenbaum, A. S., & Wetherall, D. J. (2011). Computer networks (5.ª ed.). Pearson. https://doi.org/https://csc-knu.github.io/sys-prog/books/Andrew%20S.%20Tanenbaum%20-%20Computer%20Networks.pdf

The Institute of Internal Auditors. (2017). International professional practices framework (IPPF). The IIA Research Foundation: https://www.theiia.org/en/standards/international-professional-practices-framework/

Thess, M. (2016). The analytics of power management: Utilizing analytics to support the service desk. Springer: https://www.springerprofessional.de/en/power-of-predictive-intelligence-for-service-desk/23334314

United Nations. (2020). United Nations E-Government Survey 2020: Digital Government in the Decade of Action for Sustainable Development. United Nations: https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2020

Van Grembergen, W., & De Haes, S. (2018). Enterprise Governance of Information Technology, Achieving Strategic Alignment and Value. Springer. https://doi.org/10.1007/978-0-387-84882-2

Vuorikari, R., Kluzer, S., & Punie, Y. (2022). DigComp 2.2: The Digital Competence Framework for Citizens - With new examples of knowledge, skills and attitudes. Publications Office of the European Union. https://doi.org/https://data.europa.eu/doi/10.2760/115376

W3C. (2018). Web content accessibility guidelines (WCAG) 2.1. World Wide Web Consortium: https://www.w3.org/TR/WCAG21/

Watson, A. H., & McCabe, T. J. (1996). Structured testing: A software testing methodology using the cyclomatic complexity metric. NIST Special Publication, 500-235. https://doi.org/https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-235.pdf

Weill, P. D., & Ross, J. W. (2005). IT Governance: How Top Performers Manage IT Decision Rights for Superior Results. Electronic Government Research, 1(4), 63-67. https://doi.org/https://www.researchgate.net/publication/236973378_IT_Governance_How_Top_Performers_Manage_IT_Decision_Rights_for_Superior_Results

Weill, P., & Ross, J. W. (2005). IT Governance: How Top Performers Manage IT Decision Rights for Superior Results. International Journal of Electronic Government Research, 1(4), 63-67. https://doi.org/https://www.researchgate.net/publication/236973378_IT_Governance_How_Top_Performers_Manage_IT_Decision_Rights_for_Superior_Results

Whitman, M. E., & Mattord, H. J. (2021). Principles of information security (7.ª ed.). Cengage Learning. https://doi.org/https://www.cengage.com/c/principles-of-information-security-7e-whitman-mattord/9780357506431/

Whittington , O. R., & Pany, K. (2005). Principios de auditoría. McGraw-Hill Interamericana. https://doi.org/https://es.scribd.com/document/413983592/Principios-de-Auditoria-Winttington-y-Panny-pdf

Whittington, O. R., & Pany, K. (2020). Principles of auditing & other assurance services (22.ª ed.). McGraw-Hill Education.

World Economic Forum. (2020). The Future of Jobs Report 2020. World Economic Forum: https://www.weforum.org/publications/the-future-of-jobs-report-2020/

Yin, R. K. (2018). Case study research and applications: Design and methods (6.ª ed.). SAGE Publications. https://doi.org/https://es.slideshare.net/slideshow/yin-r-k-2018-case-study-research-and-applications-design-andocx/255153005

Zeithaml, V. A., Bitner, M. J., & Gremler, D. D. (2009). Services Marketing: Integrating Customer Focus Across the Firm (5th ed.). McGraw-Hill. https://doi.org/https://www.scirp.org/reference/referencespapers?referenceid=2050901

Tomo II Gestión de tecnologías de la información: una perspectiva del control interno en el sector público, se publicó en el mes de diciembre de 2025.

ISBN: 978-9907-0-0580-6

Grupo Editorial BLR
Ecuador
Cel: +593 98 320 4362
https://grupoblr.com/
publicaciones@grupoblr.com

BIOGRAFÍA DE LOS AUTORES

Raquel Virginia Colcha Ortiz:
Docente Investigadora de la Escuela Politécnica Superior de Chimborazo, Doctora en Gestión Pública y Gobernabilidad, Magíster en Contabilidad y Auditoría con mención en Gestión Tributaria, Magíster en Gestión Empresarial, Licenciada en Contabilidad Superior, Auditoría y Finanzas (CPA). Docente de pregrado y posgrado en varias Universidades Ecuatorianas. Presidenta del Consejo de Profesores y Pedagogos encargados de preparar el examen de selección del Contralor General de la Nación, Reconocimiento como Investigadora Principal, Premio Saber Ser y Ser a la Investigación Científica Nacional e Internacional, Profesional Contable Destacada, Directora y Subdirectora de Proyectos de Investigación y Vinculación con la Sociedad.

Byron Napoleón Cadena Oleas:
Profesor investigador de la Escuela Superior Politécnica de Chimborazo, Ingeniero de Empresas, Técnico en Programación de Sistemas; Doctor en Ciencias Económicas, Magister en Informática Aplicada, Magister en Auditoria Integral, Especialista en Gestión Pública, Diploma Superior en Proyectos y Transferencia de Tecnologías. Profesor Titular en la Escuela Superior Politécnica de Chimborazo en los noveles de Grado y Posgrado. Coordinador Académico de la Carrera de Ingeniería de Empresas – Modalidad Dual en la ESPOCH. Desempeñó varios cargos en el ámbito público, como privado, entre ellos: Alcalde del Cantón Riobamba. Concejal Cantón Riobamba. Tesorero Municipal. Presidente de Empresas Públicas. Presidente del Consejo Cantonal de Planificación de Riobamba. Consejero Provincial en el Gobierno Autónomo Descentralizado Provincial de Chimborazo. Presidente del Consejo Cantonal de Protección de Derechos.

Michael Adrián Erazo Granizo:
Ingeniero en Informática e ingeniero en Contabilidad y Auditoría (CPA), con formación de posgrado en Matemática Aplicada mención en Matemática Computacional, y un MBA. Me desempeño como técnico de apoyo a la investigación en la UNACH (Ecuador), con experiencia en docencia

universitaria, investigación y gestión académica, complementada por asesoría contable y administrativa y énfasis en análisis cuantitativo y modelación matemática.

Alfredo Rodrigo Colcha Ortiz:

Magister en Informática Aplicada, (MCP) Microsoft Certified Professional de Microsoft, Ingeniero de Sistemas, Docente de instituciones de educación superior UNACH y ESPOCH de grado y posgrado, participación en proyectos de investigación, publicaciones científicas ponente en eventos académicos nacionales e internacionales, director de tesis, méritos en proyectos de Smart Cities, consultor independiente.

TOMO II GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN: UNA PERSPECTIVA DEL CONTROL INTERNO EN EL SECTOR PÚBLICO

Estimado lector, en el tomo II es un marco operativo que permite implementar y evaluar el control interno de las Tecnologías de la Información en el sector público, alineando la normativa local con estándares internacionales como ISO y COBIT.

El documento ofrece una metodología completa que abarca desde la creación de indicadores de desempeño (KPI) y la identificación de riesgos hasta la ejecución de planes de mejora divididos en infraestructura, gobernanza y talento humano.

A través de casos prácticos, la obra valida un modelo de gestión orientado a resultados, donde la tecnología actúa como la espina dorsal para la eficiencia administrativa, la seguridad de la información y la continuidad de los servicios ciudadanos.

Agradecemos a todos los lectores que se acercan a esta obra con ánimo de aprender, aplicar y transformar.

Grupo Editorial BLR
Ecuador
Cel: +593 98 320 4362
https://grupoblr.com/
publicaciones@grupoblr.com

ISBN: 978-9907-0-0580-6

GRUPO BLR