Gobernanza y ciberseguridad en la universidad pública.*

Julio García Muñoz
Director de la Unidad de Control Interno

Óscar González Martín
Auditor Interno de Sistemas de Información

Auditores Certificados de Sistemas de Información CISA
Universidad de Castilla-la Mancha

Revista Auditoría Pública nº 86
Diciembre 2025. Páginas: 179-186

Resumen: La universidad pública vive hoy una auténtica revolución silenciosa: cada matrícula, cada expediente y cada investigación transitan por redes digitales donde la seguridad se pone a prueba a diario. Este artículo examina cómo gobernanza y ciberseguridad se entrelazan para sostener la credibilidad de la institución en un entorno de riesgos invisibles pero constantes. A partir de ejemplos reales –desde un portátil sospechoso hasta un ataque de ransomware en plena época de exámenes– se muestra cómo la auditoría interna y los órganos de control externo dialogan y se complementan. El análisis pone de relieve el valor de los Controles Básicos de Ciberseguridad como un lenguaje común capaz de convertir amenazas difusas en prácticas verificables. La conclusión es clara: la universidad que quiera seguir siendo referente de conocimiento debe reforzar no solo su tecnología, sino también su cultura de seguridad y rendición de cuentas. Porque, en la era digital, lo que no se controla acaba controlándote.

Palabras Clave: Gobernanza, Ciberseguridad, Universidad pública, Auditoría interna, Controles básicos.

Abstract: Public universities are undergoing a silent revolution: every enrollment, academic record, and research project flows through digital networks where security is constantly tested. This article explores how governance and cybersecurity intersect to sustain institutional credibility in a landscape of invisible but persistent risks. Drawing on real-life examples –from a suspicious laptop to a ransomware attack during exam season– it highlights the interplay between internal audit and external oversight bodies. The analysis underscores the relevance of the Basic Cybersecurity Controls as a shared language that transforms abstract threats into verifiable practices. The message is clear: universities that aspire to remain trusted hubs of knowledge must strengthen not only their digital infrastructure but also their culture of security and accountability. In the digital era, what goes unchecked eventually takes control.

Keywords: Governance, Cybersecurity, Public university, Internal audit, Basic controls.

* *El contenido de este artículo, o parte del mismo, se basa en una comunicación presentada en los XVI Encuentros Técnicos de los OCEX (Córdoba, 2025).*

1. *Universidad digital: lo que permanece y lo que se transforma.*
2. *Normas, gobernanza y responsabilidades: el viaje de la norma al campus.*
3. *De la estrategia a la gestión tecnológica. Controles bajo una doble mirada.*
4. *Ciberseguridad en primera persona: los controles básicos como relato de campus.*
   - *CBCS 1. El dispositivo desconocido.*
   - *CBCS 2. El software malicioso.*
   - *CBCS 3. La vulnerabilidad no tratada.*
   - *CBCS 4. La llave maestra olvidada.*
   - *CBCS 5. El servidor mal configurado.*
   - *CBCS 6. El registro que nadie revisó.*
   - *CBCS 7. El ransomware y la última defensa.*
   - *CBCS 8. La visita de norma.*
5. *The (not so) new normal. Ideas finales: el día a día digital y el control externo.*

Bibliografía y referencias.

1. Universidad digital: lo que permanece y lo que se transforma.

Quien visite hoy un campus universitario comprobará que sus habituales quehaceres no se reducen a las tradicionales aulas y bibliotecas. En cada esquina, estudiantes consultan su matrícula en el móvil, investigadores acceden desde casa a repositorios científicos, administrativos procesan expedientes electrónicos y profesores corrigen trabajos en plataformas virtuales.

La misión universitaria[1] –enseñar, investigar, transferir conocimiento– sigue intacta. Lo que ha cambiado es el ecosistema donde se desarrolla. Hoy el expediente académico de un estudiante ya no está en un archivador, sino en un servidor. La publicación de un artículo no se hace solo en papel, sino en repositorios digitales abiertos a todo el mundo. Un proceso de selección de plazas se resuelve en plataformas electrónicas, con notificaciones automáticas y acceso telemático para candidatos y tribunales.

En este nuevo paisaje digital, los riesgos han mutado. Un clic en un enlace equivocado puede filtrar credenciales de miles de alumnos. Una vulnerabilidad sin parchear puede paralizar el sistema de becas en plena campaña. Un fallo en la nube puede bloquear investigaciones internacionales financiadas con fondos europeos.

El auditor interno universitario vive estos escenarios desde dentro: observa los procesos, detecta grietas y propone soluciones. Pero la foto no está completa hasta que los **OCEX autonómicos** revisan la película completa: ¿se ha gestionado bien el dinero público invertido en tecnología?, ¿las medidas aplicadas garantizan transparencia y seguridad?, ¿la universidad está en línea con lo que exige la normativa y con lo que hacen otras instituciones?

2. Normas, gobernanza y responsabilidades: el viaje de la norma al campus.

Las universidades navegan en un profuso maremágnum normativo. La **LOSU**[2] obliga a digitalizar y garantizar accesibilidad. La **Ley 39/2015** y la **40/2015** convirtieron los expedientes en trámites electrónicos obligatorios. El **Esquema Nacional de Seguridad (ENS)** exige mínimos de ciberseguridad. El **RGPD** y la **LOPDGDD** ponen reglas estrictas al tratamiento de datos personales. La **Directiva NIS 2** refuerza el papel de las universidades como operadores esenciales.

1 ORTEGA Y GASET, J. 1930 *Misión de la Universidad.* Revista de Occidente.

2 Ley Orgánica 2/2023, de 22 de marzo, del Sistema Universitario.

Traducir estas normas básicas de funcionamiento no es un ejercicio teórico. Veamos algunos casos donde postulamos un reparto de controles de responsabilidades en materia de ciberseguridad entre auditores internos y externos.

Por ejemplo, cuando un estudiante solicita una **beca online**, el sistema debe estar cifrado y ser interoperable. El auditor interno debe comprobar si las plataformas cumplen con el ENS; el OCEX puede revisar si la universidad ha diseñado el proceso con garantías de seguridad y legalidad.

En un **concurso de plazas de profesorado**, las notificaciones electrónicas deben ser seguras y verificables. El auditor interno examina la trazabilidad de los registros; el OCEX fiscaliza si se aplicaron de forma uniforme los principios de igualdad y transparencia.

En un **repositorio de investigación**, el RGPD exige que los datos se almacenen con garantías. El auditor interno vigila las medidas técnicas; el OCEX evalúa si la universidad, como institución pública, aplica la normativa igual que lo haría cualquier otra administración.

El viaje de la norma al campus, en definitiva, es el territorio compartido donde se encuentran auditores internos y externos: unos observan desde la inmediatez de la gestión diaria, otros desde la perspectiva de la rendición de cuentas pública.

Este viaje ya ha sido iniciado, por ejemplo, por la Sindicatura de Comptes de la Comunitat Valenciana[3], en sus auditorías de la gobernanza de las TI y de la ciberseguridad de 5 universidades públicas de la región.

Esta auditoría planteaba a las universidades auditadas, de manera general, las siguientes preguntas:

- ¿Dispone de un marco de gobernanza de las TI adecuado a sus características y a las buenas prácticas en la materia?
- ¿Tiene implantados sistemas de gestión de la seguridad de la información acordes con lo establecido en el Esquema Nacional de Seguridad?
- ¿Ha cumplido con las principales normas en materia de seguridad de la información?

Centrada en los elementos fundamentales para la existencia de una adecuada gobernanza y no habiendo realizado pruebas sobre la situación y eficacia de los controles de ciberseguridad desplegados por las universidades, concluye con una serie de fortalezas y debilidades de cada una ellas que sirven como punto de partida para futuros trabajos de la propia Sindicatura.

Además, este guante lanzado desde la Comunidad Valenciana, sin duda, es muy necesario que recojan a la mayor brevedad posible el resto de OCEX para auditar el nivel de ciberseguridad de las universidades públicas de sus autonomías. E, igualmente, los servicios de control interno universitarios deben emprender auditorías similares, bien con medios internos, bien con la contratación de expertos externos.

3. De la estrategia a la gestión tecnológica. Controles bajo un a doble mirada.

Tal y como nuestro sistema parasimpático trabaja de madrugada para regular el ritmo cardiaco, gestionar la tecnología en una universidad es como dirigir una ciudad que no duerme. Hay infraestructuras críticas (servidores, redes, sistemas de almacenamiento) que deben estar latiendo continuamente y al ritmo adecuado, siempre disponibles. Ademas, la transversalidad de la tecnología en la gestión económico–administrativa de la universidad obliga a un panorama en el que los servicios evolucionan constantemente para responder a una comunidad diversa y exigente.

Este dibujo trae mucho trabajo asociado. PDCA puede ser un buen marco de juego. Plan–Do–Check–Act. Todo debe comenzar con la consideración estratégica, Programa Electoral del que se derive la **Estrategia de (Gobierno y Gestión de la) Servicios TI** de la Universidad y se detalle el **Plan Director de Sistemas de Información**.

Para el auditor interno, empezar la casa por los cimientos es clave. El Plan Director es un instrumento fundamental, y constituye el mapa de riesgos que señala dónde mirar. Para el OCEX, supone la brújula que indica si la universidad avanza en la dirección que prometió en su estrategia digital.

Ejemplifiquemos con sencillos casos prácticos del día a día universitario cómo sería la debida coordinación entre controles internos y externos se coordinen.

3 Sindicatura de Comptes de la Comunitat Valenciana. Nota Informativa: La gobernanza de las TI y de la ciberseguridad en las universidades públicas valencianas. Situación a 30 de junio de 2024 - Sindicatura de Comptes

De una parte, ante procesos de **matriculación online**, el auditor interno podría verificar cifrado y registros inalterables. El OCEX revisa si existen pruebas de continuidad ante caídas del sistema.

Por otro lado, en la **compra de licencias científicas**, el auditor interno revisa que las credenciales no se compartan y que haya soporte contratado. El OCEX evalúa si las compras son eficientes y si se controla adecuadamente el inventario TIC.

Por último, en la **gestión documental electrónica**, el auditor interno comprueba trazabilidad de modificaciones. El OCEX analiza si la universidad cumple con las obligaciones del Esquema Nacional de Interoperabilidad.

Huelga decir que tanto auditores internos como los externos podrían intercambiar los controles sugeridos siempre que contasen con la debida capacitación (o músculo externo contratado).

Teniendo como vector principal el riesgo, ningún control sobra. Bueno sí. Sobra el control estéril, el estético, el solapado, el ineficiente. Algo que deberá tener en cuenta el control TI n+1. Partir de lo ya realizado. Evaluar el nivel de riesgo, y diseñar un nuevo control de ciberseguridad que no redunde, que sea práctico y que aporte valor.

Y este mantra vale para ambos, auditores internos y OCEX. Ambos deben tener una mirada clara: un diseño de controles que revise el detalle, pero que parta del cuadro completo. Juntos construyen un relato coherente sobre cómo la universidad planifica, gestiona y rinde cuentas en su transformación digital.

4. Ciberseguridad en primera persona: los controles básicos como relato de campus.

Seamos francos, el nivel de ciberseguridad de las administraciones públicas tiene mucho trabajo por delante. Los casos de ramsomware, por ejemplo, nos lo recuerdan a diario a golpe de titular informativo. Ministerios, ayuntamientos, hospitales son victimas usuales. Y la universidad no es una excepción.

Una buena noticia en este apremiante contexto, donde achicar la brecha entre el nivel de seguridad y la expansión del nivel de amenazas es tarea titánica, es la **Guía Práctica de Fiscalización de los OCEX (GPF-OCEX 5313)**, que propone 8 **Controles Básicos de Ciberseguridad (CBCS)** como marco común.

Quédense con estos titulares: la guía es muy útil. Es técnicamente robusta, pues se parte de los controles de referencia internacional (CIS Controls[4]), y se alinea con el marco español (ENS[5]). Y luego lo da todo *mascadito* para seguir la "p" con la "a", con sencillos programas de trabajo que un auditor no avezado en el mundo tecnológico puede seguir.

Para organizaciones en las que no se ha realizado nunca un trabajo de auditoría sobre la ciberseguridad, seas auditor interno o externo, permite dar un (re)paso inicial de gran valor para, al menos, tener el statu quo (spoiler: la cosa suele estar mal) del que partir.

Lo dicho. Una guía, en el sentido de utilidad y ayuda que el diccionario le reputa a la palabra.

Sin embargo, y siendo de fácil seguimiento como decimos, queremos hablar de los controles básicos de ciberseguridad con un estilo diferente. Pensamos que la ciberseguridad universitaria se cuenta mejor con historias reales. Y detrás de cada uno de estos controles hay escenas reconocibles en cualquier campus.

8 controles, 8 historias. Los controles básicos de ciberseguridad en la Universidad.

La universidad actual no consiste únicamente en aulas, bibliotecas, laboratorios o unidades administrativas; es también una amplia comunidad donde conviven estudiantes con sus portátiles y teléfonos móviles, profesores que imparten docencia (presencial o virtual) o realizan investigaciones y gestores que tratan con datos sensibles de miles de personas. Cada matrícula, cada expediente, cada investigación es información valiosa.

En la mayoría de los casos, los integrantes de la comunidad universitaria utilizan los servicios informáticos que la institución pone a su disposición sin pararse a pensar en la cantidad de riesgos cibernéticos que siempre acechan: ordenadores desconocidos que se conectan a la red informática, aplicaciones descargadas sin control, correos sospechosos, vulnerabilidades sin parchear, accesos indebidos a expedientes, logs que nadie revisa o copias de seguridad que no funcionan cuando más se necesitan.

4 Center of Internet Security. Organización de reconocido prestigio internacional. Define un marco de seguridad que establece un conjunto priorizado de controles orientados a mitigar los ataques más comunes y dañinos.

5 Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Las ciberamenazas son un riesgo invisible que nunca descansa.

Para hacer frente a esos riesgos, la universidad debe contar con ocho escudos de protección: los Controles Básicos de Ciberseguridad. Cada uno de estos controles tiene su misión particular, y entre todos tienen como misión custodiar nuestra información y nuestros sistemas.

CBCS 1. EL DISPOSITIVO DESCONOCIDO.

Imagina una mañana cualquiera en la Universidad. El campus despierta y miles de dispositivos se encienden: portátiles y teléfonos móviles de estudiantes y profesores, ordenadores de administración, servidores de investigación, y hasta cámaras de seguridad conectadas a la red.

Entre todos estos elementos aparece un dispositivo sospechoso. Es un ordenador desconocido, conectado a la red de un laboratorio. Nadie sabe de dónde ha salido ni quién lo controla. Podría ser un portátil con malware de un alumno, o quizá un atacante externo lo ha introducido para espiar comunicaciones.

Estos "fantasmas digitales" constituyen un riesgo dentro de la red de comunicaciones. Pueden usarse para robar credenciales, capturar datos personales de expedientes académicos o incluso detener servicios críticos como la plataforma de matrícula online.

Aquí entra en juego el primer control básico de ciberseguridad: Inventario y control de dispositivos físicos.

Su objetivo es sencillo: disponer de un "censo digital" de todos los equipos autorizados. Cada portátil, cada servidor, cada switch debe estar registrado, con datos básicos como identificador del dispositivo (número de serie, dirección MAC, IP), persona o unidad responsable, estado o ubicación.

Este inventario no es un simple documento Excel olvidado en un cajón: debe ser una herramienta viva, actualizada y automatizada, que refleje la realidad de lo que está conectado en ese momento.

Para implementar este control, se utilizan herramientas que permiten vigilar la red en tiempo real y comprobar si alguien intenta conectarse sin estar autorizado.

Este control se apoyará en herramientas NAC (Network Access Control) que permiten gestión del acceso a la red, herramientas de escaneo de red y descubrimiento de activos, o herramientas de ticketing para la gestión de altas y bajas del inventario.

El papel del auditor será comprobar que el control funciona de verdad, buscando evidencias de que el inventario existe y está actualizado, que se revisa y monitoriza y que los dispositivos tengan un responsable asignado.

No se puede proteger lo que no se conoce.

CBCS 2. EL SOFTWARE MALICIOSO.

En la facultad de química, un profesor está evaluando los trabajos de sus alumnos. Uno de ellos presenta la documentación en un formato "raro" y decide convertirlo a PDF. Para ello se instala un programa que encuentra en internet: un "conversor gratuito de PDF". Parece inofensivo y muy útil.

Lo que este usuario no sabe es que el software trae escondido un regalo envenenado: un malware capaz de abrir una conexión remota y permitir a un atacante externo moverse por la red universitaria. Ese pequeño gesto, un clic inocente, puede convertirse en un agujero por el que robar expedientes académicos, datos de investigación o incluso las credenciales de acceso a la intranet.

Este software no autorizado constituye un nuevo riesgo. En una universidad, donde conviven miles de dispositivos, la instalación libre de programas es una tentación constante. Y lo que parece un recurso necesario puede convertirse en una amenaza.

En este caso actúa el segundo control básico: el control del software autorizado.

Para implementar este control se pueden usar herramientas como SCCM e Intune que permiten desplegar el software autorizado en los equipos, o Applocker que bloquea el software que no está en la lista blanca.

Gracias a este control, la universidad no depende de la buena fe de los usuarios, sino de controles automáticos que evitan sorpresas.

La unidad de auditoría tiene nuevas tareas: comprobar la existencia y control del inventario de software autorizado y los procedimientos de altas, bajas y revisiones de los componentes del mismo.

CBCS 3. LA VULNERABILIDAD NO TRATADA.

En pleno inicio de curso, el campus digital estaba al máximo rendimiento. Los estudiantes se conectaban a la plataforma de matrícula, los investigadores consultaban convocatorias de proyectos y el personal administrativo trabajaba en la gestión de becas.

Todo funcionaba correctamente. Pero bajo esa normalidad, un problema acechaba.

En el servidor principal del sistema que gestiona la matrícula un parche de seguridad crítico llevaba semanas pendiente de instalarse. No era mala fe ni descuido grave: simplemente, "no había tiempo" y el sistema era demasiado sensible como para apagarlo unos minutos en ese momento. El equipo de TI pensaba: *"lo haremos después del periodo de matriculación."*

Aparece un nuevo riesgo: una vulnerabilidad sin corregir. Puede no pasar nada, pero basta con que algún ciberdelincuente la detecte y decida explotarla.

La amenaza se hizo real cuando, esa misma mañana, apareció un intento de conexión desde el exterior que trataba de explotar precisamente esa brecha conocida. El ataque falló, pero dejó al descubierto la fragilidad de la situación.

Para evitar situaciones como esta disponemos del tercer control: la gestión de vulnerabilidades.

El auditor deberá comprobar que existen procedimientos y herramientas que permitan la identificación, priorización y corrección de las vulnerabilidades que puedan afectar a los sistemas de la universidad.

CBCS 4. LA LLAVE MAESTRA OLVIDADA.

En la secretaría de alumnos, el equipo administrativo cerraba expedientes y procesaba notas. Durante el alta de permisos de un nuevo trabajador, alguien se percata de la existencia de una cuenta de usuario cuyo propietario se había jubilado meses atrás. Además, era una cuenta con acceso completo a expedientes académicos, nóminas y servidores de datos.

El riesgo era enorme: una "llave maestra" olvidada que podía abrir todas las puertas digitales de la universidad. Si un atacante la encontraba, podría manipular calificaciones, robar información confidencial o paralizar sistemas enteros.

Para estos casos tenemos el cuarto control: el control de privilegios. Una gestión continua de las cuentas de usuario, sobre todo las que disponen de privilegios elevados. La labor del auditor consistirá en asegurar que las cuentas con permisos de acceso "elevados" están bajo control, que se usan solo en caso necesario y que la actividad de estos usuarios queda registrada.

CBCS 5. EL SERVIDOR MAL CONFIGURADO.

El grupo de investigación de bioquímica acababa de recibir un servidor nuevo, potente, que iba a almacenar datos de experimentos financiados con proyectos europeos. El técnico lo instaló rápido: enchufar, encender y dejarlo funcionando para que los investigadores pudieran empezar cuanto antes.

Nadie se fijó en que el servidor tenía la configuración por defecto: Usuario "admin" y contraseña "1234", servicios innecesarios abiertos, puertos sin restricción.

Todo funcionaba y los investigadores empezaron a trabajar, ya podían subir sus datos. Pero lo que no sabían es que ese servidor era ahora la puerta más débil de la universidad. Bastaba con que un atacante escaneara la red para encontrarlo, probar la contraseña por defecto y acceder a información crítica.

Tenemos un nuevo riesgo: configuraciones inseguras, descuidos que convierten un sistema en una entrada libre para los atacantes.

Aquí entra en juego el quinto control: las configuraciones seguras. Ningún equipo debe ponerse en producción sin aplicar medidas de fortalecimiento de la configuración (hardening). Existen guías específicas, basadas en las normas del CCN-STIC, muy útiles para apoyar este control.

El papel del auditor no será reconfigurar este equipo a un estado más seguro, sino comprobar que existen procedimientos (y que se siguen) de bastionado del hardware y software antes de su puesta en producción.

CBCS 6. EL REGISTRO QUE NADIE REVISÓ.

Era viernes por la noche en la universidad. Los edificios estaban vacíos, pero los sistemas seguían vivos: servidores de matrícula, nóminas, correo electrónico… todos trabajando en silencio.

A las 23:47, alguien desde una dirección IP extranjera intentó acceder al sistema de nóminas. Introdujo contraseñas al azar, una y otra vez. El sistema lo anotó en sus registros (logs), pero no saltó ninguna alerta. Nadie estaba mirando. El intento pasó desapercibido. Al día siguiente, todo seguía funcionando y nadie se dio cuenta de lo ocurrido.

Ese es el riesgo: registros que existen, pero que no se revisan. Como cámaras de seguridad que graban todo, pero cuyas cintas nunca son observadas.

Para evitar este riesgo tenemos el sexto control: la supervisión de registros y monitorización continua.

El área de TI implantó un SIEM (Security Information and Event Management): un sistema que centraliza y analiza todos los logs. Configuraron alertas: si alguien intentaba entrar al sistema de nóminas fuera del horario laboral, el

sistema enviaba una alarma.

La siguiente vez que el atacante lo intentó, a las dos de la madrugada, la alerta sonó en el móvil del responsable de seguridad. En pocos minutos, bloquearon la dirección sospechosa y revisaron los accesos. El ataque no prosperó.

En este caso, el auditor comprobará que existen registros de la actividad de los usuarios, su almacenamiento, centralización y revisión y la existencia de herramientas de análisis y alerta.

CBCS 7. EL RANSOMWARE Y LA ÚLTIMA DEFENSA.

Era plena temporada de exámenes en la universidad. La plataforma de docencia virtual estaba a rebosar: profesores subiendo materiales, estudiantes descargando apuntes, foros llenos de mensajes.

De pronto, un lunes a primera hora, todo se detuvo. Archivos cifrados, mensajes de error en pantalla y un aviso aterrador:

"Sus datos han sido secuestrados. Si quiere recuperarlos, pague en criptomonedas."

El campus digital estaba paralizado. La universidad había sufrido un golpe devastador: un ataque de ransomware.

Los profesores no podían subir exámenes, los alumnos no podían entregar trabajos, y la tensión se extendía como un incendio. Todos miraban al área de informática, esperando una respuesta.

Fue entonces cuando se activó el séptimo control: las copias de seguridad.

La universidad contaba con un plan de respaldo robusto: copias diarias automáticas, almacenadas tanto en servidores locales como en la nube con *Azure Backup*. Además, cada mes se realizaban restauraciones de prueba para asegurar que funcionaban.

Había que dar las gracias a la auditoría que se había realizado el año anterior en la que se revisó la política de copias de seguridad y se recomendaron pruebas de recuperación para detectar errores.

CBCS 8. LA VISITA DE NORMA.

La universidad vivía en un periodo de calma. El curso había arrancado con normalidad y los niveles de estrés habían bajado considerablemente. Pero la alegría dura poco en la casa del pobre. Había llegado un correo con un asunto serio: "Inicio de auditoría".

En el área de informática estaban tranquilos, tenían todo bajo control: sistemas actualizados, red vigilada, copias de seguridad al día… Pero cuando Norma, la auditora, pidió las políticas y procedimientos firmados, las actas del comité de seguridad y la declaración de aplicabilidad del ENS, nadie sabía de qué estaba hablando. El incumplimiento normativo no desactiva los sistemas, pero destruye reputaciones.

La universidad entendió entonces que la seguridad no termina en el firewall, sino que también vive en los documentos que la sostienen. Lo que empezó como un susto se convirtió en una oportunidad. Se elaboró la política de seguridad de la información, se constituyó un comité de seguridad, se asignaron roles y se empezó a mantener actualizado no solo lo técnico, sino también lo formal.

La universidad, al final, salió reforzada. No solo protegía sus sistemas, también podía demostrar que lo hacía.

Como epílogo a este conjunto de historias universitarias, recalcamos la noción básica de que los riesgos no son teóricos: ocurren asiduamente, desde un ordenador infectado en un despacho hasta un servidor crítico sin parches. Pero con los controles básicos de ciberseguridad activos, la Universidad dispone de un sistema de defensa robusto, aunque requiere vigilancia, disciplina y cultura.

El papel del auditor es esencial: verificar que los controles no se limitan a buenas intenciones, sino que están en funcionamiento, documentados y probados.

5. The *(not so)* new normal. Ideas finales: el día a día digital y el control externo.

La universidad que describíamos al inicio, con estudiantes conectados desde cualquier lugar, investigadores trabajando en repositorios globales y administrativos gestionando expedientes electrónicos, es la misma que llega hasta estas líneas finales. La universidad sigue siendo un lugar de conocimiento y servicio público, pero ahora necesita guardianes digitales y auditores que sean eficaces en los contextos digitales del siglo XXI. Solo así podrá cumplir su misión clásica en este presente no tan nuevo, donde cada clic importa y cada control cuenta.

El futuro digital de la universidad ya no se anuncia, se vive a diario en el campus. Los retos emergentes –inteligencia artificial, nube y teletrabajo– no son escenarios hipotéticos, sino escenas cotidianas que ponen a prueba los mecanismos de control.

Un profesor prueba un sistema de **IA** para detectar plagios en los exámenes. Los estudiantes protestan al sentirse evaluados por un algoritmo. El auditor interno comprueba si el sistema deja trazabilidad y supervisión humana. El OCEX analiza si la universidad cumple el RGPD y respeta los derechos de los estudiantes frente a decisiones automatizadas.

Un grupo de investigación decide volcar sus datos en un **servidor en la nube** contratado por rapidez. Solo después descubren que está alojado fuera de la UE. El auditor interno detecta la vulnerabilidad y plantea soluciones. El OCEX evalúa si la universidad incumplió el ENS y si adoptó garantías contractuales adecuadas para proteger datos sensibles.

Un administrativo, tras la pandemia, tramita expedientes desde su casa. Lo hace desde un portátil personal, sin VPN ni autenticación multifactor. El auditor interno observa la brecha inmediata. El OCEX revisa si la universidad ha diseñado políticas claras de teletrabajo, alineadas con la normativa laboral y de protección de datos.

Estos relatos muestran que la transformación digital universitaria no es un discurso abstracto, sino un mosaico de decisiones concretas, tomadas cada día por estudiantes, docentes, investigadores y gestores. Y que estas decisiones tienen consecuencias que deben ser acompañadas por controles, primero internos y después externos.

Aquí radica la importancia del **diálogo entre auditoría interna y OCEX autonómicos**. El auditor interno aporta cercanía, conoce las rutinas y detecta vulnerabilidades a pie de campus. El OCEX ofrece una visión independiente, compara universidades y fija estándares homogéneos de seguridad y transparencia. Entre ambos se construye una narrativa coherente: una universidad que no solo enseña e investiga, sino que lo hace con seguridad, transparencia y confianza.

En este viaje, los **Controles Básicos de Ciberseguridad** son un ejemplo de ese lenguaje compartido: convierten riesgos invisibles en prácticas medibles, y casos cotidianos en criterios de fiscalización. Pero los CBCS son mucho más que medidas técnicas: son relatos cotidianos del campus, escenas reconocibles en cualquier facultad, desde un portátil sospechoso hasta un ransomware en época de exámenes. Y detrás de cada historia está siempre la misma moraleja: lo que no se controla, acaba controlándote.

En definitiva, en un entorno académico cada vez más digital y vulnerable, la colaboración entre control interno y externo no es un lujo, sino la clave de bóveda que sostiene la credibilidad, la seguridad y la transparencia de la universidad pública.

Bibliografía y referencias.

- Directiva (UE) (NIS 2. Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).
- Guía Práctica de Fiscalización (GPF-OCEX 5313): Controles Básicos de Ciberseguridad.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley Orgánica 2/2023, de 22 de marzo, del Sistema Universitario.
- Ley Orgánica 3/2018, de Protección de Datos Personales.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Reglamento (UE) 2016/679, Reglamento General de Protección de Datos (RGPD).