# INFORME DE AUDITORÍA Nº 19/2025

*Proyecto:*

**TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN**

*Área Auditada:*

## PROSECRETARÍA DE INFORMÁTICA

Al Señor Rector de la
Universidad Nacional de Córdoba
Mgter. Jhon Boretto
S / D

DICIEMBRE/2025

TABLA DE CONTENIDOS

UNC UAI Universidad Nacional de Córdoba

# INFORME EJECUTIVO

Proyecto: **TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN**
Informe Nº **19/2025**
Área Auditada: **PROSECRETARÍA DE INFORMÁTICA**

## Informe Ejecutivo

El presente informe tiene por objeto sintetizar el resultado de las tareas llevadas a cabo a fin de verificar el cumplimiento de la normativa referida al Control Interno para Tecnología de la Información, en particular lo relacionado con Ciberseguridad. La labor de auditoría fue realizada de acuerdo con las Normas de Auditoría Interna Gubernamental, aplicándose los procedimientos allí enumerados. Las labores de campo se llevaron a cabo durante el mes de noviembre y primera quincena de diciembre en la Prosecretaría de Informática.

El presente informe se encuentra referido a las observaciones y conclusiones sobre el objeto de análisis mencionado precedentemente y no contempla la eventual ocurrencia de hechos posteriores que puedan modificar su contenido.

A continuación, se detallan las principales observaciones detectadas:

**POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN**

**ORDENANZA Nº 3/08 HCS**

**NORMAS DE CONTROL INTERNO PARA TECNOLOGÍA DE LA INFORMACIÓN**

**Res. SGN N° 87/22**

Si bien hay un procedimiento de realización de backup de todos los sistemas, bases datos, máquinas virtuales, etc., no existe un procedimiento de restauración selectivo de los mismos. Además, no se dispone de un plan de tratamiento ante contingencias que garantice la continuidad operativa de los distintos sistemas.

De las Observaciones detalladas se desprenden las siguientes Recomendaciones:

Se deberá desarrollar y documentar un plan de pruebas que permita verificar la integridad y confiabilidad de las copias de seguridad. Este plan debe garantizar que los datos puedan ser recuperados correctamente ante un escenario de restauración, prever la realización de un plan de contingencia que contemple

las acciones necesarias para asegurar la continuidad operativa en situaciones críticas o de emergencia.

## Conclusión

Como conclusión de la presente Auditoría, se puede apreciar que en las distintas áreas entrevistadas, la Ordenanza H.C.S. Nº 3/08 Política de Seguridad de la Información de la Universidad Nacional de Córdoba y de la Res. SGN N° 87/22 Normas de Control Interno Para Tecnología De La Información; se cumplen correctamente brindando seguridad y garantizando un seguro desempeño en los sistemas y servicios que brinda de la Universidad Nacional de Córdoba a través de la Prosecretaría de Informática. En cuanto al cumplimiento de la normativa referida al Control Interno para Tecnología de la Información, en particular lo relacionado con Ciberseguridad se considera necesario cumplimentar las observaciones mencionadas.

Córdoba, 19 de diciembre de 2025

# INFORME ANALÍTICO

Proyecto: **TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN**
Informe Nº **19/2025**
Área Auditada: **PROSECRETARÍA DE INFORMÁTICA**

**Informe Analítico**

## I- OBJETO

Verificar el cumplimiento de la normativa referida al Control Interno para Tecnología de la Información, en particular lo relacionado con Ciberseguridad y la protección de los activos de información.

## II- ALCANCE

La tarea se llevó a cabo en la Prosecretaría de Informática, abarcando temas esenciales a la información referida al cumplimiento de la Ordenanza H.C.S. Nº 3/08 Política de Seguridad de la Información. Res. SGN 87/2022 Normas de Control Interno para Tecnología de la Información. La tarea de campo se realizó durante el mes de noviembre y primera quincena de diciembre de 2025. El universo correspondió al 100% de los datos del sistema.

El presente informe se encuentra referido a las observaciones y conclusiones sobre el objeto de la tarea por el período precedentemente indicado y no contempla la eventual ocurrencia de hechos posteriores que puedan modificar su contenido.

## III- MARCO DE REFERENCIA

El presente Informe se presenta en el marco del Plan de Trabajo del año 2025, y del desarrollo de Auditorías sobre áreas de apoyo, correspondiente al Proyecto Sistemas Informáticos. La Auditoría se llevó a cabo en la Prosecretaría de Informática en las áreas de Servicios, Redes e Infraestructura.

La Prosecretaría de Informática tiene como misión contribuir con las funciones de docencia, investigación y extensión de la Universidad Nacional de Córdoba, coordinando el uso de los recursos relacionados con la informática; mediante la formulación y ejecución de políticas relacionadas con las Tecnologías de Información y Comunicaciones (TICs); adquisición y administración de sistemas de información; planificación y administración de la infraestructura de red y servicios informáticos.

**Marco Normativo**

Para la realización de la Auditoría se aplicó la Res. SGN 87/2022 Normas de Control Interno para Tecnología de la Información y Ordenanza H.C.S. Nº 3/08 Política de Seguridad de la Información de la Universidad Nacional de Córdoba.

## IV- TAREAS REALIZADAS Y PROCEDIMIENTOS APLICADOS

- Reunidos en la PSI (Prosecretaría de Informática) con el responsable del Área de Infraestructura y Servicios, nos informa sobre las distintas áreas y los directores responsables técnicos de los mismos, organizando reuniones para continuar con las entrevistas.

- Reunidos con el Director del Área de Ciberseguridad de la PSI nos informa que cuenta con cierta infraestructura y herramientas de gestión de incidentes (IRIS, Wazuh, OWASP ZAP), que cuesta conseguir y mantener al personal especializado. La disponibilidad de la red es crítica, y aunque existen guías y procesos basados en NIST, aún falta consolidar un plan integral de contingencias y completar la identificación de activos y amenazas.

- Mediante una reunión de Meet, el Director del área de Despliegue SIU nos informa que cuenta con herramientas modernas de monitorización y automatización (Kuma, Grafana, Ansible), que realiza backups diarios y tiene documentación técnica de recuperación. Sin embargo, la prioridad de sistemas críticos depende del contexto del periódo de actividades de la UNC y las decisiones de otras direcciones, los tiempos de recuperación no están formalmente definidos, y la UNC dispone de la nube de la PSI como alternativa ante contingencias.

- Mediante una reunión de Meet grupal con distintas áreas; el Director del área de Redes nos informa que atiende la infraestructura crítica de la UNC con un equipo colaborativo de técnicos, que la documentación de procedimientos se encuentra desactualizada, que dependen de proveedores y falta de procedimientos formales. El director del área de Servicios sostiene la infraestructura académica y administrativa crítica de la UNC. Se destaca la automatización y seguridad de los backups, y que falta sistematizar pruebas periódicas de recuperación de configuraciones. Ante una contingencia, la falta de redundancia generalizada puede representar un riesgo para la continuidad operativa. La respuesta a incidentes está organizada de forma colaborativa, con responsables por subárea y protocolos de recuperación. El Área de Infraestructura cumple un rol estratégico en la continuidad operativa de la PSI. Si bien existen avances en la automatización y redundancia, es necesario prever la actualización de procedimientos, la eficiencia en

backups y la cobertura integral de planes de contingencia. La prioridad inmediata es fortalecer la integridad del DataCenter y optimizar los procesos de respaldo para garantizar la seguridad y disponibilidad de la información.

- Mediante una reunión de Meet, con el encargado de Proyectos Especiales, nos informa que el Sistema GDE cuenta con una estructura clara y cuenta con mecanismos básicos de respaldo (backups diarios y snapshots). Tienen falta de documentación formal de contingencias y dificultades para actualizar a nuevas versiones. Se recomienda priorizar la formalización de procedimientos, fortalecer la estrategia de contingencia y asegurar la asistencia técnica necesaria para la evolución del sistema.

- Mediante una reunión de Meet, el Director del área de la administración de Google Workspace en la UNC, nos informa que es una área crítica que combina seguridad, gestión de usuarios y soporte a la operación académica y administrativa. Que lidera un equipo reducido de colaboradores clave con alta responsabilidad y discreción. Hay una nueva área de inteligencia artificial trabajando en mejorar las consultas al sistema Digesto, representando una oportunidad estratégica para modernizar el acceso a dicho sistema. La gestión de incidentes y la seguridad continúan siendo los principales desafíos del área.

No se analizaron en los procesos verificados, acciones u omisiones que implican “Costos de la No Calidad”.

## V – OBSERVACIONES, OPINIÓN DEL AUDITADO Y RECOMENDACIONES

### POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

### ORDENANZA Nº 3/08 HCS

### NORMAS DE CONTROL INTERNO PARA TECNOLOGÍA DE LA INFORMACIÓN

### Res. SGN N° 87/22

1. De las entrevistas realizadas a los encargados y directores de las distintas áreas como Servicios, Redes e Infraestructuras, se desprende que no existe un procedimiento documentado, actualizado y aprobado por las autoridades de la Prosecretaría para: el tratamiento y respuestas de Gestión de Incidentes de Seguridad, y para la Gestión de Contingencias que garantice la continuidad operativa de los distintos sistemas.

Impacto: Medio

2. Si bien hay un procedimiento de realización de backup de todos los sistemas, bases datos, máquinas virtuales, etc., no existe un procedimiento documentado aprobado por las autoridades para la realización de resguardo y recuperación de la información.

   Impacto: Medio

**OPINION DEL AUDITADO**

Las Observaciones planteadas fueron aceptadas por los funcionarios responsables comprometiéndose a la implementación de las soluciones según consta en nota NO-2025-01067049-UNC-NOC#PSI.

**RECOMENDACIONES**

1 - Se deberá prever la realización de un procedimiento aprobado por las autoridades de la PSI para el tratamiento y respuesta a Incidentes de Seguridad de las áreas de Ciberseguridad y de Servicio de Google Workspace; como así también disponer de un procedimiento aprobado por las autoridades de la PSI para la Gestión de Contingencias de las áreas de: Despliegue SIU, Servicios, Infraestructura, Proyectos Especiales (GDE) y Redes que contemple las acciones necesarias para asegurar la continuidad operativa en situaciones críticas o de emergencia.

2 - Se deberá actualizar un procedimiento documentado aprobado por las autoridades de la PSI, que permita verificar la integridad y confiabilidad de las copias de seguridad. Este plan debe garantizar que los datos puedan ser recuperados correctamente ante un escenario de restauración. Se podría instrumentar pruebas parciales de restauración de algunos sistemas que lo permitan y repetirlos en un determinado tiempo con el fin de ir adquiriendo automatización de la pruebas.

## VI - CONCLUSIONES

Como conclusión de la presente Auditoría, se puede apreciar que en las distintas áreas entrevistadas, la Ordenanza H.C.S. Nº 3/08 Política de Seguridad de la Información de la Universidad Nacional de Córdoba y de la Res. SGN N° 87/22 Normas de Control Interno Para Tecnología De La Información; se cumplen correctamente brindando seguridad y garantizando un seguro desempeño en los sistemas y servicios que brinda de la Universidad

Nacional de Córdoba a través de la Prosecretaría de Informática. En cuanto al cumplimiento de la normativa referida al Control Interno para Tecnología de la Información, en particular lo relacionado con Ciberseguridad se considera necesario cumplimentar las observaciones mencionadas.

Córdoba, 19 de diciembre de 2025

Universidad Nacional de Córdoba
2025

**Hoja Adicional de Firmas**
**Informe Gráfico Firma Conjunta**

**Número:** IF-2025-01088648-UNC-UAI#REC

CORDOBA, CORDOBA
Viernes 19 de Diciembre de 2025

**Referencia:** INFORME DE AUDITORIA N° 19/2025

---

El documento fue importado por el sistema GEDO con un total de 11 pagina/s.

Digitally signed by GDE UNC
DN: cn=GDE UNC, c=AR, o=Universidad Nacional de Cordoba, ou=Prosecretaria de Informatica, serialNumber=CUIT 30546670623
Date: 2025.12.19 09:58:51 -03'00'

Sergio Ruben Diaz
Auditor Senior
Auditores Unidad de Auditoría Interna
Universidad Nacional de Córdoba

Digitally signed by GDE UNC
DN: cn=GDE UNC, c=AR, o=Universidad Nacional de Cordoba, ou=Prosecretaria de Informatica, serialNumber=CUIT 30546670623
Date: 2025.12.19 10:25:17 -03'00'

Liliana Bosaz
Auditora Interna Titular
Unidad de Auditoría Interna
Universidad Nacional de Córdoba

Digitally signed by GDE UNC
DN: cn=GDE UNC, c=AR, o=Universidad Nacional de Cordoba, ou=Prosecretaria de Informatica, serialNumber=CUIT 30546670623
Date: 2025.12.19 10:22:36 -03'00'