UADER FCyT

TP N°13 ESTÁNDAR ISO27000

LIC. EN SISTEMAS DE INFORMACIÓN

ASIGNATURA: INGENIERÍA DE SOFTWARE 2

ALUMNO:

GONZALEZ IGNACIO

TP13 Estándar ISO27000
1. Utilice como punto de partida el documento de ISO27000 (2018) y realice un relevamiento bibliográfico adicional para identificar las normas detalladas que integran el “ecosistema” normativo denominado ISO 27000. Obtenga resúmenes de los mismos. Formule un resumen:
• Enumere todas las normas formantes.
• Versión resumida de su alcance.
• Principales conceptos abordados.
• Principales diferencias entre la versión 2018 y 2022.

1. Normas que integran la familia ISO 27000

Núcleo general:

- **27000:** visión general y vocabulario.
- **27001:** requisitos del SGSI (certificable).
- **27002:** controles y buenas prácticas.
- **27003:** guía de implementación del SGSI.
- **27004:** métricas y evaluación.
- **27005:** gestión de riesgos.

Extensiones y guías:

- **27011:** telecomunicaciones.
- **27013:** integración con ISO 20000.
- **27014:** gobernanza.
- **27016:** economía organizacional.
- **27017 / 27018:** seguridad y privacidad en la nube.
- **27033:** seguridad de redes.
- **27034:** seguridad de aplicaciones.
- **27035:** gestión de incidentes.
- **27036:** relaciones con proveedores.
- **27040:** seguridad en almacenamiento.
- **27050:** e-Discovery.
- **27799:** salud (información clínica).

2. Alcance

La familia ISO 27000 establece un **marco integral para la gestión de la seguridad de la información (SGSI)**: definición de políticas, gestión de riesgos, controles técnicos y organizativos, y mejora continua.
Cada norma cumple una función: 27001 define qué hacer; 27002 y complementarias explican cómo hacerlo.

3. Principales conceptos

- **SGSI (ISMS):** sistema estructurado para proteger información.
- **Confidencialidad, integridad y disponibilidad.**
- **Riesgo, amenaza, vulnerabilidad, control, activo.**
- **Ciclo PDCA:** planificación, ejecución, verificación y mejora.
- **Gobernanza, métricas, conformidad y respuesta a incidentes.**

4. Diferencias clave 2018 → 2022

- **ISO/IEC 27000:** sigue vigente (última edición 2018).
- **Cambios principales en 27001 y 27002 (2022):**
    - Reestructuración de controles: de 114 a **93 controles** agrupados en 4 dominios.
    - Inclusión explícita de **ciberseguridad y privacidad.**
    - **Controles nuevos:** seguridad en la nube, amenazas físicas, preparación ante incidentes, etc.
    - Enfoque más **flexible y basado en resultados.**
    - Annex A de 27001 actualizado para alinearse con 27002:2022.

Conclusión:
ISO/IEC 27000:2018 sigue siendo la base conceptual y terminológica. La versión 2022 renovó el enfoque operativo del SGSI, adaptándolo a un entorno digital y de ciberamenazas más complejo.

2. Evalúe el grado de criticidad de los siguientes activos de información en el contexto de una organización proveedora de educación superior (universitaria).

Parte	Requisito	Fuente
Estudiantes	Protección de PI, acceso a Learning Management System (LMS) 24x7	Ley 25.326 / Contratos nube
Docentes	Integridad de calificaciones, disponibilidad	Normativa interna
Ministerio/CONICET	Confidencialidad de investigación	Convenios
Proveedores nube	SLA, cifrado, logs	Contrato/SLA

1. Estudiantes

- Archivos asociados: datos personales, historial académico, accesos al LMS.
- Requisitos: protección de datos (Ley 25.326), disponibilidad 24x7 del sistema de gestión educativa.
- Criterios:
    - Confidencialidad: *Alta* — involucra información personal sensible.

    - Integridad: *Alta* — errores afectarían calificaciones y trayectoria académica. Disponibilidad: *Alta* — el LMS es esencial para clases, exámenes y comunicación.
- Criticidad global: Muy alta.
  Una falla afecta directamente la continuidad educativa y el cumplimiento legal.

2. Docentes

- Activos asociados: datos personales, registros de calificaciones, materiales de cátedra.
- Requisitos: integridad de calificaciones, disponibilidad operativa según normativa interna.
- Criterios:
    - Confidencialidad: *Media-Alta* — información laboral y evaluativa.
    - Integridad: *Muy alta* — calificaciones incorrectas generan perjuicio académico y legal.
    - Disponibilidad: *Media* — necesario para dictado y carga de notas.
- Criticidad global: Alta.
  Afecta legitimidad académica y cumplimiento institucional.

3. Ministerio / CONICET

- Archivos asociados: proyectos de investigación, datos científicos, convenios.
- Requisitos: confidencialidad de investigación, cumplimiento de convenios y estándares de publicación.
- Criterios:
    - Confidencialidad: *Muy alta* — posible información sensible o patentable.
    - Integridad: *Alta* — resultados deben mantenerse inalterables.
    - Disponibilidad: *Media* — acceso controlado, pero crítico para continuidad investigativa.
- Criticidad global: Muy alta.
  Compromete propiedad intelectual, reputación y financiamiento.

4. Proveedores de nube

- Activos asociados: infraestructura, almacenamiento, copias de seguridad, registros de auditoría (logs).
- Requisitos: cumplimiento de SLA, cifrado, custodia de logs (según contrato).
  Criterios:
    - Confidencialidad: *Alta* — manejan datos institucionales y personales.
    - Integridad: *Alta* — errores impactan en servicios dependientes.
    - Disponibilidad: *Muy alta* — su interrupción paraliza plataformas críticas.
- Criticidad global: Muy alta.
  Son el pilar tecnológico del ecosistema educativo y de investigación.

Conclusión:

Los activos más críticos son **los datos de estudiantes**, **los proveedores de nube** y **la información científica institucional**, ya que combinan alta sensibilidad legal, necesidad operativa continua y valor estratégico.

3. Haga una evaluación detallada desde el punto de vista de SGSI sobre los componentes (actores, procesos, herramientas, información, etc.) involucrados en el dictado de educación superior en formato remoto/virtual.

A. Actores

- Estudiantes y docentes: usuarios principales; riesgo de credenciales débiles o mal uso de LMS
- Administradores IT: responsables del mantenimiento y control de accesos; riesgo de privilegios excesivos.
- Proveedores de nube: manejas datos institucionales; riesgo de fallos en SLA o exposición de información.

B. Procesos Críticos:

- Gestión académica: inscripción, calificaciones, certificación. Requiere integridad y trazabilidad.
- Accesos al LMS y aulas virtuales: demanda disponibilidad continua.
- Evaluaciones y comunicaciones: exigen autenticidad e integridad de la identidad y resultados.
- Respaldo y recuperación: mitigación ante pérdida o corrupción de datos.

C. Herramientas:

- LMS (Moodle, Canvas, etc): núcleo del servicio; debe tener cifrado logs y control de roles.
- Videoconferencias (Zoom, Meet): requiere gestión segura de sesiones.
- Sistema de almacenamiento y nube: protección cifrado y autenticación multifactor.

D. Información:

- Datos personales y académicos: requieren confidencialidad.
- Investigaciones y materiales docentes: alta sensibilidad intelectual.
- Logs y registros: soporte para auditorías y respuesta a incidentes.

E. Evaluación SGSI:

- Amenazas: fuga de datos, suplantación de identidad, indisponibilidad del servicio.
- Controles prioritarios (ISO 27001/27002): gestión de accesos, seguridad en la nube, respaldo, concientización y respuesta a incidentes.
- Nivel de criticidad: alto, por el impacto académico, legal y reputacional ante una brecha o interrupción.

4. Realice una evaluación de riesgo teniendo en cuenta los factores expresados en la siguiente tabla.

ID	Activo/Proceso	Amenaza	Vuln.	Prob.	Imp.	Riesgo	Notas
R-01	DB alumnos	Ransomware	Parches atrasados				Crítico; planes BRS/backup
R-02	LMS	DDoS	Sin Firewall				Mitigar con Firewall
R-03	Email	Phishing	Conciencia baja				Campañas + 2FA + DMARC(1)
R-04	SIU	Interrupción eléctrica	Redundancia limitada				UPS + generador
R-05	Doc repositorio	Fuga PII	Acceso laxo				RBAC(2) + DLP(3) + clasificación

(1) Domain-based Message Authentication, Reporting, and Conformance, es un protocolo de seguridad de correo electrónico que previene el suplantación de dominio (spoofing) y ataques de phishing (2) Control de Acceso Basado en Roles (del inglés, Role-Based Access Control) (3) Data Loss Prevention (Prevención de Pérdida de Datos), un conjunto de herramientas y estrategias de ciberseguridad que identifican y protegen la información confidencial dentro de una organización para evitar su uso, uso compartido o transferencia indebida, ya sea intencionada o accidental, a usuarios no autorizados

ID	**Activo / Proceso**	**Amenaza**	**Vulnerabilidad**	**Prob.**	**Imp.**	**Riesgo**	**Notas / Medidas de mitigación**
R-01	DB alumnos	Ransomware	Parches atrasados	Alta	Muy alta	Critico	Aplicar actualización regular, backups verificados, plan BRS y restauración probada.
R-02	LMS	DDos	Sin Firewall	Media	Alta	Alto	Implementar firewall, balanceador de

							carga, monitoreo de tráfico y CDN
R-03	Email	Pishing	Concien cia baja	Alta	Medio	Alto	Capacitación continua, autenticación 2FA, políticas DMARC/ SPF/DKIM
R-04	SIU	Interrupcion electrica	Redundancia limitada	Media	Alta	Alto	Implementar UPS, generador y respaldo geográfico.
R-05	Doc repositorio	Fuga PII	Acceso laxo	Media	Muy alta	Critico	Aplicar RBAC, DLP, clasificación de información y cifrado en reposo.

Formule

• Asignación estimativa de valores de

- o Probabilidad 1 Muy baja (≤1 vez/5 años)… 5 Crítica (≥1/mes)
- o Impacto 1 Menor (sin impacto)… 5 Catastrófico (masiva ≥1 semana)

• Mapa de calor teniendo en cuenta que los criterios a ser aplicados y los umbrales respectivos serán

- o Perfil de riesgo aceptable (Apetito de riesgo)
  - -Riesgo aceptable ≤6
  - -Riesgo tolerable 7–12 con PTR

-Riesgo inaceptable ≥15 (accionar inmediato)

• Realice una evaluación de riesgo teniendo en cuenta los factores expresados en la siguiente tabla.

Escala	Probabilidad (P) – Frecuencia estimada	Impacto (I) – Consecuencia esperada
1	Muy baja (≤ 1 vez cada 5 años)	Menor (sin impacto relevante)
2	Baja (1 vez cada 2–5 años)	Limitado (afecta parcialmente un área)
3	Media (1 vez por año)	Moderado (interrupción <1 día o datos no críticos)
4	Alta (1 vez por trimestre)	Grave (afecta servicios principales por varios días)
5	Crítica (≥1 vez por mes)	Catastrófico (interrupción ≥1 semana o fuga masiva)

Riesgo = P × I

Umbrales de apetito de riesgo:

- ≤ **6** → Aceptable
- **7–12** → Tolerable (requiere Plan de Tratamiento de Riesgo - PTR)
- ≥ **15** → Inaceptable (acción inmediata)

ID	Activo / Proceso	Amenaza	Vulnerabilidad	P	I	R = P× I	Nivel	Acción / Medidas
r-01	DB alumnos	Ransomware	Parches atrasados	4	5	**20**	**Inaceptable**	Aplicar parches, backup 3-2-1, pruebas de restauración, segmentación de red.
r-02	LMS	DDoS	Sin firewall	3	4	**12**	**Tolerable (PTR)**	Implementar firewall, CDN, monitoreo y mitigación automática.

r-03	Email	Phishing	Conciencia baja	4	3	**12**	**Tolerable (PTR)**	Capacitación, 2FA, filtros antiphishing, DMARC/SPF/DKIM.
r-04	SIU	Corte eléctrico	Redundancia limitada	2	4	**8**	**Tolerable (PTR)**	UPS, generador, redundancia geográfica, monitoreo energético.
r-05	Repositorio documental	Fuga de PII	Acceso laxo	3	5	**15**	**Inaceptable**	RBAC, DLP, cifrado, clasificación de datos, revisión de permisos.

Impacto →	**1**	**2**	**3**	**4**	**5**
Prob. 5 (Crítica)	5	10	15	20	25
Prob. 4 (Alta)	4	8	12	**16**	**20**
Prob. 3 (Media)	3	6	9	12	**15**
Prob. 2 (Baja)	2	4	6	8	10
Prob. 1 (Muy baja)	1	2	3	4	5

Colores:

- Verde ≤ 6 → Aceptable
- Amarillo 7–12 → Tolerable (PTR)
- Rojo ≥ 15 → Inaceptable

Síntesis final

- **Riesgos inaceptables:** r-01 (ransomware), r-05 (fuga de PII).
- **Riesgos tolerables:** r-02 (DDoS), r-03 (phishing), r-04 (interrupción eléctrica).
- **Ningún riesgo aceptable sin tratamiento.**

Conclusión:
El SGSI debe priorizar la mitigación inmediata de ransomware y fugas de información personal, seguidos por mejoras preventivas en ciberdefensa, capacitación y resiliencia operativa.

5. Utilizando los aprendizajes reflejados en https://www.urmconsulting.com/blog/lessons-learnt-from-early-iso-27001-2022 transitions. Elabore un resumen de los principales problemas que debe cuidar una organización durante el proceso de re-certificación en estándar ISO27000.

Principales problemas en la re certificación ISO 27001:2022

A. **No usar correctamente iso 27002:2022;** riesgo de implementar controles obsoletos.
B. **Sistemas y proceso desalineados;** aplicar procesos antiguos sin adaptación genera vacíos o duplicidades.
C. **SoA desactualizado;** auditor puede considerar la transición incompleta.
D. **Documentación antigua;** políticas y registros refiere a cláusulas o controles previos.
E. **Falta de integración con otros sistemas;** esfuerzos duplicados y perdida de coherencia.
F. **Calendario de transición insuficiente;** riesgo de errores por prisa.
G. **Formación insuficiente;** personal clave no entiende los cambios del estándar.
H. **Descuidar la conformidad con la versión anterior;** vulnerabilidades durante la transición.
I. **Subestimar cambios sutiles;** implementación superficial que no cumple requisitos.
J. **Evidencias insuficientes;** auditorías detectan falta de registros y pruebas de implementación.

Recomendación:
Actualizar SoA, políticas y procedimientos; formal al personal; mantener la versión anterior hasta completar la transición; generar evidencias claras y planificar tiempos.

6. Utilice el “Caso de Estudio TIC” para identificar los costos y beneficios que afronta una organización de base tecnológica al implementar ISO 27000. Produzca un resumen del caso e identifique que aspectos del mismo mas contribuyen a su comprensión de las motivaciones estratégicas que puede movilizar a una organización en el emprendimiento de una hoja de ruta sobre éste tema.

Costos asociados a la implementación

- **Inversión inicial:** Costos de consultoría, formación y auditoría externa.
- **Tiempo de dedicación:** horas de personal para adaptar procesos y documentación.
- **Recursos tecnológicos:** adquisición de herramientas para monitoreo y control.

Beneficios obtenidos

- **Mejora en la reputación:** certificación reconocida que genera confianza en clientes y socios.
- **Reducción de incidentes de seguridad:** implementación de controles efectivos que disminuyen riesgos.
- **Cumplimiento normativo:** adecuación a estándares internacionales que facilita su entrada a nuevos mercados.
- **Mejora continua:** proceso sistemático de revisión y mejora de la seguridad de la información.

Motivaciones estratégicas para implementar ISO 27000

- **Competitividad:** diferenciación frente a competidores mediante la certificación.
- **Confianza del cliente:** garantía de protección de datos sensibles.
- **Acceso a nuevos mercados:** cumplimiento de requisitos de seguridad exigidos por clientes internacionales.
- **Gestión de riesgos:** identificación y mitigación proactiva de amenazas a la seguridad de la información.

Este caso demuestra que, aunque la implementación de ISO 27000 implica costos iniciales, los beneficios a largo plazo, como la mejora de la reputación, la reducción de riesgos y el cumplimiento normativo, justifican la inversión.