Universidad Nacional Mayor de San Marcos

Facultad de Ingeniería de Sistemas e Informática
Unidad de POSTGRADO
Maestría de Ingeniería de Sistemas e Informática
Mención en Ingeniería de Software

Examen: EXAMEN PARCIAL

Curso: Ciberseguridad en la Ingeniería de Software
Docente: JORGE ERNESTO PISCOYA PRÍNCIPE
Fecha: 28.06.25
Alumno: Lino Ever, Ramos Maiz
Código de alumno: 24207219

Instrucciones Generales:

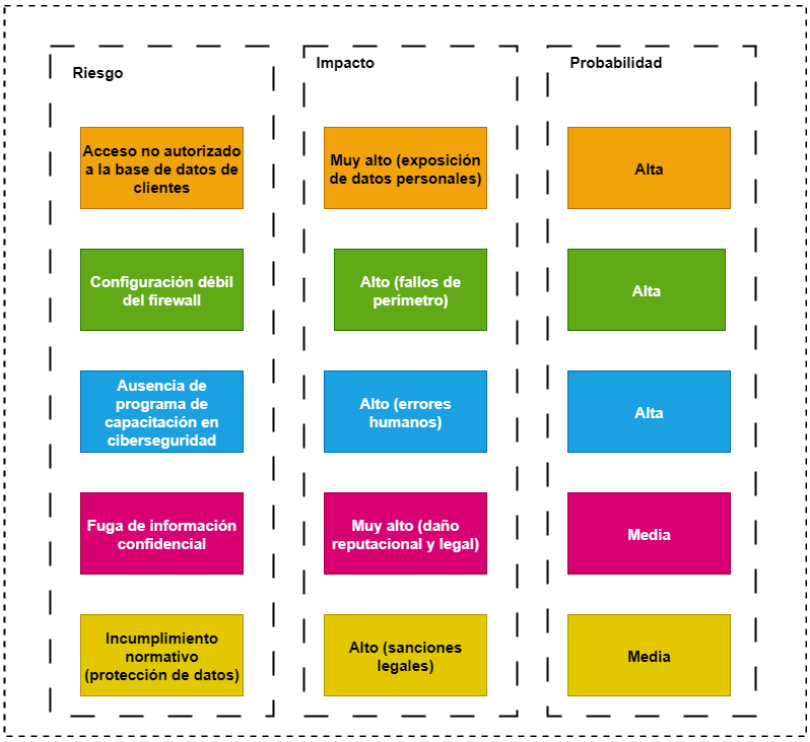
1. Lea cuidadosamente cada pregunta antes de responder.
2. Responda de forma clara y precisa.
3. Justifique sus respuestas cuando se indique.
4. Este examen tiene un total de **20 puntos**.
5. El examen debe ser enviado a **jorge.piscoya1@unmsm.edu.pe** con el asunto "EXAMEN PARCIAL – *CÓDIGO_DE_ALUMNO – NOMBRE_COMPLETO*"

Universidad Nacional Mayor de San Marcos

CASO 1: GlobalSecure SAC (4 puntos)

1. Identificación y evaluación de riesgos

Riesgos identificados (5):



Aplicación del Anexo A de la ISO/IEC 27001:2022:

El **Anexo A** incluye controles que ayudan a mitigar estos riesgos, por ejemplo:

- **A.5.10** Política de seguridad de la información
- **A.5.23** Concienciación, educación y formación en seguridad
- **A.8.20** Configuración segura
- **A.8.28** Protección de la información en aplicaciones
- **A.8.25** Control de acceso a la información

Controles clave según la ISO/IEC 27002:2022:

Capítulo 7 – Seguridad en recursos humanos:

7.2.2 Capacitación en seguridad de la información

7.3.1 Responsabilidades después de la terminación o cambio de empleo

Capítulo 8 – Gestión de activos:

8.3.1 Gestión de activos de información

8.8.1 Gestión de la configuración

Matriz de aceptación de riesgos:

Riesgo	Impacto	Probabilidad	Nivel	Aceptación
Acceso no autorizado a BD	Muy alto	Alta	Crítico	No aceptable
Configuración débil de firewall	Alto	Alta	Critico	No aceptable
Falta de capacitación	Alto	Alta	Critico	No aceptable
Fuga de información	Muy alto	Media	Alta	No aceptable
Incumplimiento normativo	Alto	Media	Alto	No aceptable

2. Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI)

Plan propuesto:

Controles seleccionados:

A.5.10, A.5.23, A.8.20, A.8.25, A.8.28 (ISO 27001)

Cap. 7 y Cap. 8 (ISO 27002)

Actividad	Cronograma	Recursos tecnológicos	Recursos humanos
Implementar firewall de nueva generación y reglas específicas	1 semana	Firewall físico/virtual, reglas actualizadas	Equipo TI
Establecer política formal de seguridad y plan SGSI	2 semanas	Herramientas de documentación	Jefe de seguridad, legal
Configurar controles de acceso según roles	1 semana	Gestor de identidades IAM	Administrador TI
Implementar programas de capacitación (e-learning)	3 semanas	Plataforma LMS	RRHH, experto en ciberseguridad
Realizar auditoría de seguridad inicial	2 semanas	Software de auditoría	Consultor externo

3. C

Universidad Nacional Mayor de San Marcos

Basado en el Capítulo 7 de ISO 27002:2022

Temas clave:	Periodicidad:	Medición de efectividad:
Políticas internas de seguridad	Inducción obligatoria al ingresar	Cuestionarios con puntajes mínimos
Phishing y amenazas comunes	Refuerzo trimestral	Métricas de participación
Contraseñas seguras y MFA	Simulacros de phishing semestrales	Reportes de incidentes post-entrenamiento
Protección de datos personales		Resultados de simulacros de phishing
Buenas prácticas de navegación		

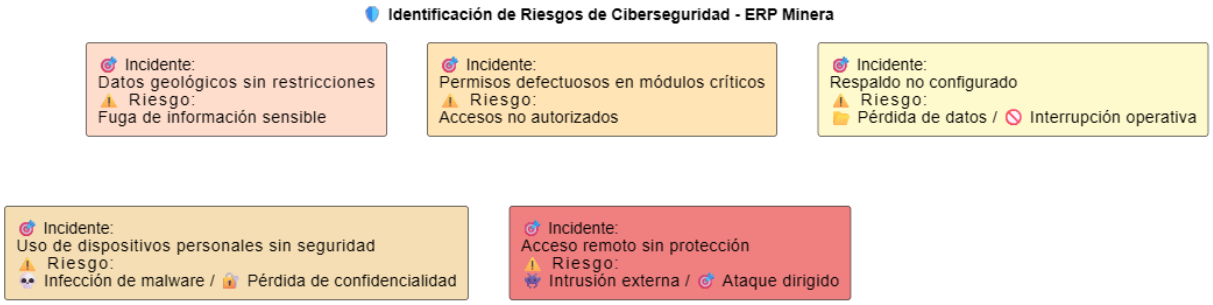
CASO 2: Desarrollo de un ERP para la Empresa Minera "Minerales del Sur S.A." (4 puntos)

1. Reconocimiento de activos críticos

Incidente	Activos críticos afectados	Posibles impactos
Exposición de datos geológicos sensibles	Base de datos de reservas minerales y ubicación de yacimientos	Espionaje industrial, pérdida de ventaja competitiva
Acceso no controlado a módulos críticos	Módulos financieros, de producción y RRHH	Manipulación de datos, fraudes internos, errores operativos
Falta de respaldo de datos	Servidor principal, turnos de trabajo, producción semanal	Interrupción operativa, pérdida de productividad
Uso de dispositivos personales no autorizados	Credenciales de usuarios, red corporativa, datos accedidos desde dispositivos inseguros	Fugas de información, malware, suplantación de identidad
Interfaces de acceso remoto vulnerables	Interfaces de administración remota, direcciones IP expuestas	Ataques externos, acceso no autorizado, manipulación del ERP

Universidad Nacional Mayor de San Marcos

2. Identificación de riesgos de ciberseguridad



3. Controles recomendados (según ISO/IEC 27032)

Gestión de accesos y roles de usuario

- Definir roles estrictos y mínimos privilegios.
- Implementar control de acceso basado en rol (RBAC).
- Autenticación multifactor (MFA).

b. Respaldo y recuperación de datos

- Política formal de respaldos automáticos (backup diario / incremental).
- Verificación periódica de integridad de respaldos.
- Pruebas regulares de recuperación (disaster recovery).

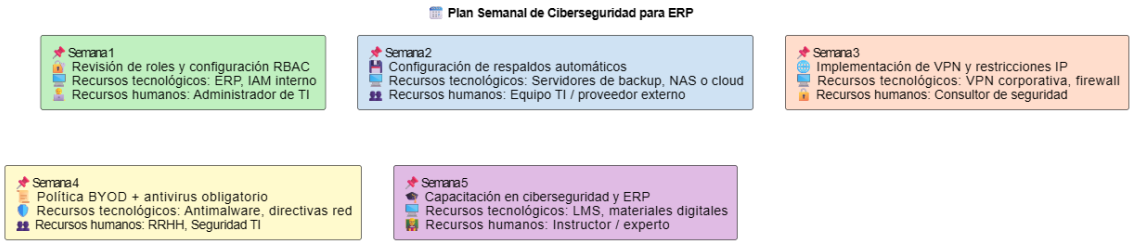
c. Seguridad en conexiones remotas

- Uso de VPN cifrada y restricciones de IP.
- Firewall robusto para interfaces de desarrollo.
- Auditoría y control de accesos remotos.

d. Sensibilización de usuarios y BYOD

- Políticas claras para uso de dispositivos personales (BYOD).
- Autenticación MFA y antivirus obligatorio para dispositivos móviles.
- Capacitación continua sobre amenazas (phishing, malware)

4. Plan de implementación



CASO 3: ITSEC COMMERCE – EVALUACIÓN DE CONTROLES ISO 27001 EN UNA EMPRESA DE COMERCIO ELECTRÓNICO (4 puntos)

Control	Nombre del control	¿Aplica?	Justificación	Estado de cumplimiento	Observaciones / Acciones
A.5.7	Contacto con autoridades	Sí	La empresa gestiona datos personales, por lo tanto debe coordinar con la Autoridad de Protección de Datos	No implementado	Designar responsables de contacto con INDECOPI y APDP
A.5.10	Política de seguridad de la información	Sí	No existe política formal; es esencial para iniciar el SGSI	No implementado	Redactar y aprobar política de seguridad integral
A.5.23	Concienciación y formación en seguridad	Sí	No hay programa de capacitación; los usuarios usan cuentas compartidas	Parcial	Establecer programa formal de capacitación continua
A.5.24	Gestión de incidentes de seguridad	Sí	No hay proceso documentado para gestionar incidentes	No implementado	Diseñar y formalizar el procedimiento de respuesta a incidentes

A.8.16	Gestión de acceso privilegiado	Sí	El personal de desarrollo accede innecesariamente a datos de clientes	Parcial	Limitar accesos, usar MFA y registro de auditoría
A.8.28	Protección de datos en aplicaciones	Sí	No hay revisión periódica de vulnerabilidades	No implementado	Implementar pruebas periódicas y usar WAF
A.8.29	Seguridad en interfaces de usuario	Sí	El portal web carece de controles contra ataques web	Parcial	Integrar revisión de código y mecanismos anti-inyección
A.8.31	Protección de datos personales e información confidencial	Sí	Hay acceso excesivo a bases de datos sin control	Parcial	Aplicar controles de acceso por roles y cifrado
A.8.35	Gestión de backup	Sí	La empresa terceriza backups sin contrato de SLA	Parcial	Formalizar contratos de respaldo y establecer controles de revisión
A.8.16	Gestión de cuentas compartidas	Sí	Se detectaron usuarios compartidos en herramientas administrativas	No implementado	Eliminar cuentas compartidas y establecer trazabilidad individual

Acciones recomendadas

1. Crear una política de seguridad formal y validarla con la alta dirección (A.5.10).
2. Capacitar regularmente al personal sobre seguridad, acceso, phishing, protección de datos (A.5.23).
3. Eliminar cuentas compartidas e implementar registros de auditoría (A.8.16).
4. Establecer revisión periódica del portal web con pruebas de vulnerabilidad y WAF (A.8.28).

5. Contratar formalmente el servicio de backups con SLA definidos (A.8.35).
6. Diseñar un proceso de gestión de incidentes documentado y probado (A.5.24).
7. Aplicar control de acceso por roles para limitar exposición de datos (A.8.31).

CASO 4: "SECURITY 360° – CIBERSEGURIDAD MULTICAPA" (6 puntos)

Diagnóstico por capa:

Capa	Controles existentes	Riesgos asociados	Brechas evidenciadas
Perímetro	Firewall básico, sin IPS configurado	Caídas por ataques DDoS	Falta de protección avanzada y mitigación automatizada
Red Interna	Segmentación parcial	Movimientos laterales de amenazas	IDS ausente, segmentación débil
Dispositivos	Antivirus instalado, sin EDR	Malware por phishing	No hay cifrado de discos ni control de dispositivos USB
Identidades	Usuarios privilegiados sin MFA	Accesos no autorizados	Gestión de privilegios débil
Aplicaciones	API mal configurada, sin WAF	Exposición pública	Ausencia de revisión de código seguro
Monitorización	SOC tercerizado, sin SIEM propio	Falta de correlación de eventos	No se almacenan ni correlacionan registros clave
Nube	Acceso a la nube sin controles robustos	Fuga de datos	Deficiencias en configuración y monitoreo
Incidentes	Sin plan de respuesta	Lenta reacción ante ataques	No se han realizado simulacros en 18 meses
Formación	Nula capacitación reciente	Errores humanos	Ausencia de concienciación y simulacros

Gobernanza	No certificado en ISO 27001	Falta de cumplimiento normativo	No hay política formal ni auditorías periódicas

Medidas propuestas por capa

Capa	Preventivas	Detectivas	Reactivas
Perímetro	Implementar IPS y reglas anti-DDoS	Monitoreo de tráfico con alertas	Activación de mitigación automatizada DDoS
Red Interna	Segmentar por VLAN y zonas de confianza	Instalar IDS internos	Respuesta automatizada ante amenazas internas
Dispositivos	EDR corporativo y cifrado de discos	Alertas por acceso no autorizado	Desconexión automática de dispositivos externos
Identidades	MFA obligatorio y gestión por roles (RBAC)	Auditoría de accesos	Revocación inmediata de cuentas comprometidas
Aplicaciones	Revisiones de código seguro, API Gateway	WAF activo y registros de acceso	Parcheo rápido ante vulnerabilidades descubiertas
Monitorización	SIEM centralizado integrado al SOC	Correlación en tiempo real	Manual de acciones ante eventos críticos
Nube	Políticas IAM estrictas y cifrado en tránsito	Análisis de configuraciones en la nube (CSPM)	Aislamiento de servicios expuestos
Incidentes	Plan de respuesta formalizado y comunicado	Registro y clasificación de incidentes	Procedimientos de recuperación probados
Formación	Programa anual de capacitación + simulacros	Evaluaciones periódicas	Retroalimentación y mejora continua
Gobernanza	Certificación ISO 27001 en 12 meses	Auditorías internas semestrales	Plan de mejora continua basado en hallazgos

Universidad Nacional Mayor de San Marcos

Hoja de ruta de implementación:

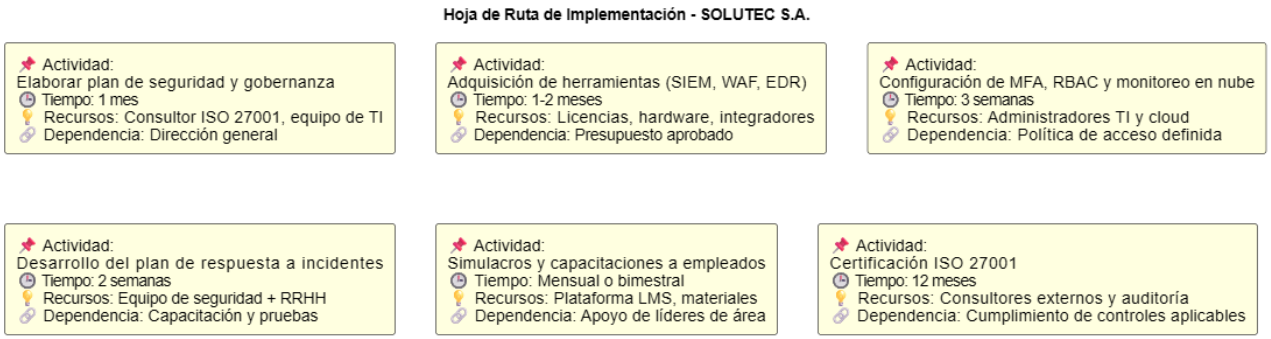
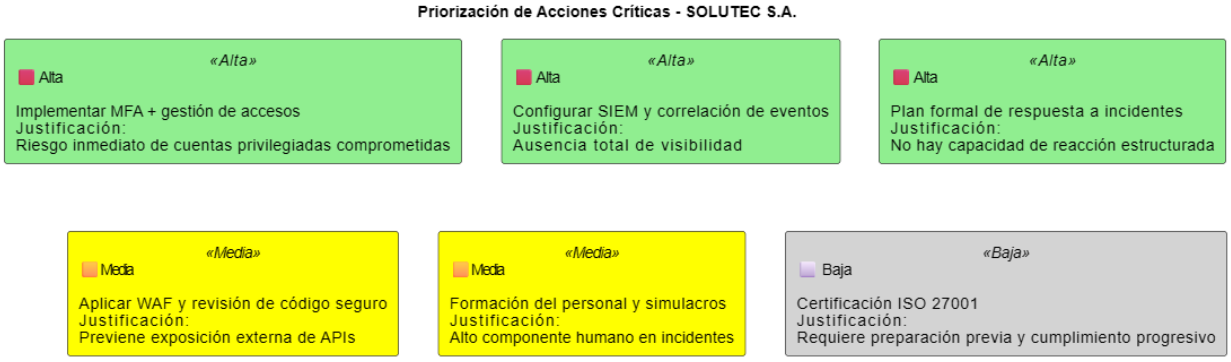
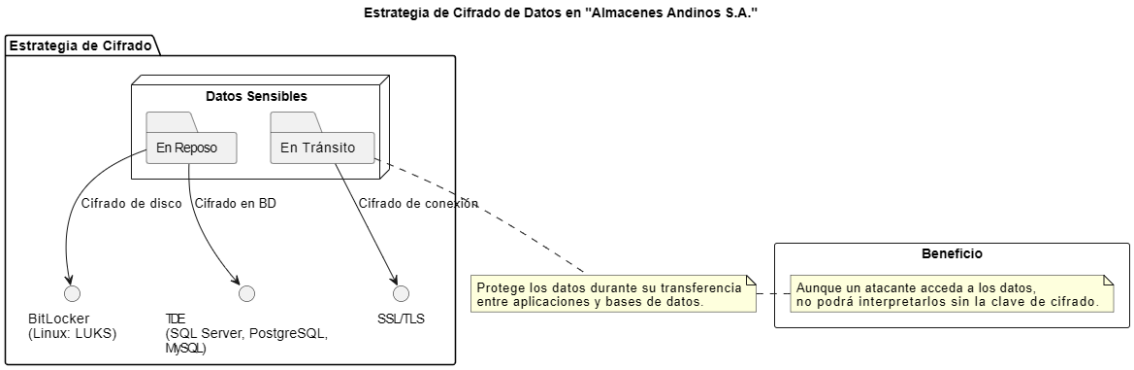


Tabla de priorización (por criticidad):



CASO 5: Protección de Datos en "Almacenes Andinos S.A." (2 puntos)

1. Cifrado de Datos



2. Control de Acceso

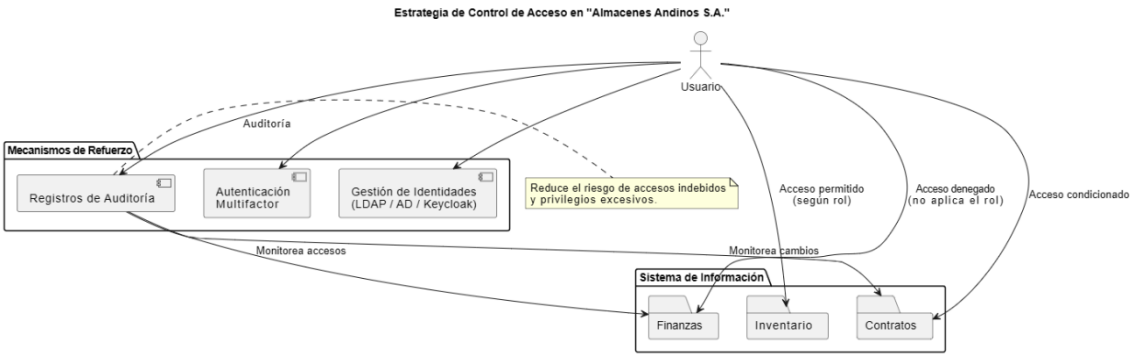
Propuesta:

- Implementar control de acceso basado en roles (RBAC) para asegurar que cada usuario acceda solo a la información que necesita.
- Mecanismos adicionales:

  Autenticación multifactor (MFA).

  Gestión centralizada de identidades mediante servicios como LDAP, Active Directory o Keycloak.

  Registros de auditoría para rastrear accesos y modificaciones a la base de datos.
- Beneficio: Minimiza el riesgo de accesos indebidos o privilegios excesivos.



3. Seguridad Física

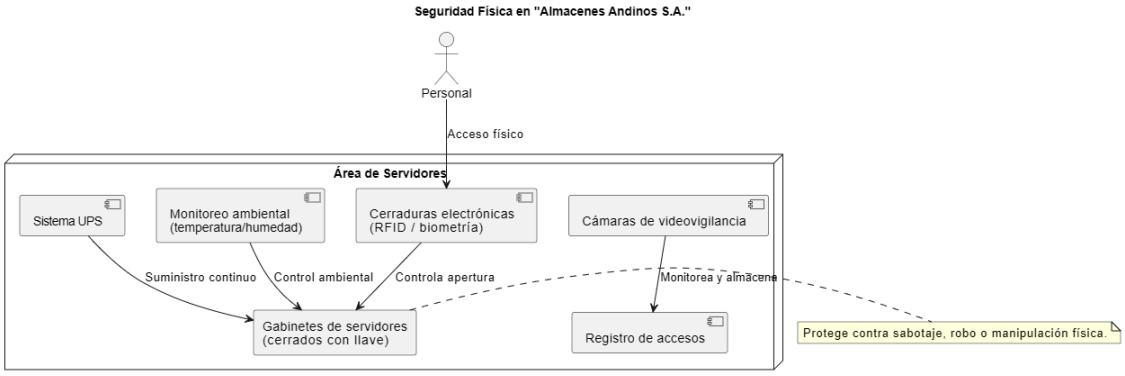
Propuesta:

- Controles de acceso físico al área del servidor:

  Uso de cerraduras electrónicas con tarjetas RFID o biometría.

  Cámaras de videovigilancia y registro de entradas/salidas.

  Políticas estrictas para personal autorizado en zonas sensibles.
- Implementación de gabinetes de servidores cerrados con llave.
- Sistemas de alimentación ininterrumpida (UPS) y monitoreo ambiental (temperatura/humedad).
- Beneficio: Se reduce la probabilidad de sabotaje, robo o manipulación directa del hardware.



4. Segmentación de Datos

Propuesta:

- Separar lógicamente los tipos de datos en bases de datos diferentes o tablas con niveles de acceso diferenciados.

  Base de datos 1: registros financieros.

  Base de datos 2: registros logísticos.

  Base de datos 3: datos operacionales en tiempo real.

- Aplicar etiquetado de sensibilidad (confidencial, interno, público).
- Aplicar políticas de respaldo diferenciadas para cada segmento.
- Beneficio: En caso de una brecha, el impacto se limita solo al segmento afectado y no a toda la información corporativa.