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: _____
Código de alumno: _____

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)

La empresa GlobalSecure SAC es una organización de comercio electrónico con operaciones internacionales. Recientemente, sufrió un incidente de seguridad en el que un atacante externo accedió a su base de datos, exponiendo información sensible de clientes. Este incidente ocurrió debido a una configuración débil en su firewall y la ausencia de un programa de capacitación en ciberseguridad para empleados.

Como asesor en ciberseguridad, se te ha solicitado diseñar soluciones y estrategias basadas en las normas ISO 27001:2022 e ISO 27002:2022.

Actividad

1. Identificación y evaluación de riesgos

Usando el caso, identifique 5 riesgos principales relacionados con el incidente y evalúe su impacto y probabilidad. Explique cómo el Anexo A de ISO 27001:2022 puede ayudar a gestionar estos riesgos, así mismo trabaje con los controles del capítulo 8 y del capítulo 7 de la ISO 27002:2022 para establecer los controles de seguridad utilizando la matriz de Aceptación.

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

Proponer un plan para implementar los controles seleccionados. El plan debe contener lo siguiente:

- Controles
- Actividades clave
- Cronograma
- Recursos necesarios (tecnológicos y humanos)

3. Capacitación y concienciación en ciberseguridad

Establecer un programa de capacitación en ciberseguridad para los empleados, alineado con los controles establecidos del Capítulo 7: Seguridad en Recursos Humanos de la ISO 27002:2022. Indica los temas clave a incluir, su periodicidad y cómo medir la efectividad de las capacitaciones.

Universidad Nacional Mayor de San Marcos

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

La empresa Minerales del Sur S.A. es una compañía minera peruana con operaciones en diversas regiones del país. Sus actividades incluyen la extracción, procesamiento y exportación de minerales como cobre, zinc y oro. Dado el crecimiento de sus operaciones y la complejidad de sus procesos, la empresa ha decidido desarrollar un ERP personalizado para integrar sus áreas clave:

- Gestión de inventarios.
- Mantenimiento de maquinaria y equipos.
- Gestión de nóminas.
- Finanzas y control de presupuestos.
- Planificación y control de producción.
- Monitoreo ambiental y seguridad industrial.

El desarrollo del ERP está a cargo del equipo interno de TI, en colaboración con el proveedor externo TechMin Solutions, quien se encarga de la configuración de los módulos principales y la infraestructura tecnológica.

En el desarrollo del ERP se detectaron las siguientes incidencias:

1. Exposición de datos geológicos sensibles:
   Durante las pruebas iniciales, se detectó que los datos relacionados con las reservas minerales y la ubicación de yacimientos no contaban con las restricciones adecuadas. Estos datos estaban accesibles desde cuentas de usuarios con roles administrativos generales, lo que expone a la empresa a riesgos de espionaje industrial.

2. Acceso no controlado a módulos críticos:
   Se descubrió que empleados de áreas no relacionadas, como Recursos Humanos, podían acceder a los módulos financieros y de control de producción debido a una configuración inicial defectuosa de los permisos de usuario.

3. Falta de respaldo de datos:
   Un fallo en el servidor principal provocó la pérdida temporal de información sobre los turnos de trabajo y la producción semanal. Esto ocurrió porque los respaldos automáticos no se habían configurado adecuadamente.

4. Uso de dispositivos personales no autorizados:
   Algunos supervisores de campo accedieron al sistema ERP desde dispositivos personales, lo que generó vulnerabilidades al no contar con medidas de protección como autenticación multifactor o conexiones seguras.

5. Ataque simulado por penetración externa:
   Durante una auditoría de seguridad, el equipo de TechMin Solutions simuló un

ataque externo. Descubrieron que las interfaces de acceso remoto utilizadas por los desarrolladores para ajustar el ERP no estaban protegidas por firewalls robustos ni políticas de restricción de IP.

Actividad

1. Reconocimiento de activos:
   Identifique los activos críticos afectados en cada incidente (por ejemplo, datos geológicos, módulos específicos del ERP, servidores, usuarios, etc.). Elabore una lista de los activos críticos y los posibles impactos si se ven comprometidos.
2. Identificación de riesgos:
   Relacione cada incidente descrito en el caso con riesgos de ciberseguridad específicos, como fuga de información sensible, interrupciones operativas, o accesos no autorizados.
3. Propuesta de controles según ISO/IEC 27032:
   Proporcione una lista de controles de la ISO/IEC 27032 recomendados para mitigar los riesgos identificados en el punto 2, considerando:
   - Gestión de accesos y roles de usuario.
   - Respaldo y recuperación de datos.
   - Seguridad en las conexiones remotas.
   - Sensibilización de usuarios y uso de dispositivos personales.
4. Diseño de un plan de implementación:
   Proponga un plan para implementar los controles seleccionados, indicando:
   - Actividades clave.
   - Cronograma.
   - Recursos necesarios (tecnológicos y humanos).

Universidad Nacional Mayor de San Marcos

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

CONTEXTO ORGANIZACIONAL

Nombre de la organización: ITSEC Commerce S.A.C.
Sector: Comercio electrónico y logística
Tamaño: 250 empleados
Sedes: Lima (sede central y datacenter propio) + 4 centros de distribución (Trujillo, Arequipa, Cusco, Piura)
Operación:

- Infraestructura híbrida (servicios locales y en la nube – AWS)
- Portal web de e-commerce, aplicación móvil y sistema de atención a clientes
- ERP y CRM en la nube
- Procesamiento de pagos con tarjetas de crédito/débito (integración con pasarelas externas)
- Cumplimiento parcial con la Ley de Protección de Datos Personales
- No tiene certificación ISO 27001 pero desea prepararse para obtenerla en 12 meses

---

SITUACIÓN DE SEGURIDAD ACTUAL

El equipo de TI ha implementado algunas medidas de seguridad, pero no existe una política formal de gestión de seguridad de la información. Los controles están dispersos entre distintas áreas (TI, Legal, Infraestructura), y la dirección no tiene una visión clara sobre qué se está cumpliendo o no.

Además:

- Se identificaron accesos innecesarios a bases de datos de clientes por parte de personal de desarrollo.
- El portal web no cuenta con revisión periódica de vulnerabilidades ni WAF.
- No hay gestión documentada de incidentes de seguridad.
- La empresa terceriza la gestión de backups en la nube sin contrato de nivel de servicio específico.
- Se han detectado usuarios compartidos en herramientas administrativas.

OBJETIVO DEL CASO

Los estudiantes asumirán el rol de consultores de ciberseguridad encargados de evaluar transversalmente qué controles tecnológicos de la ISO/IEC 27001:2022 se están cumpliendo en la organización y cuáles deben implementarse o mejorar.

Para ello deberán:

1. Realizar un análisis transversal por dominios y cláusulas aplicables.
2. Elaborar el Documento de Aplicabilidad (SoA), indicando:
    - El estado actual de cada control (Aplicable / No aplicable)
    - Justificación
    - Grado de cumplimiento (Implementado / Parcial / No implementado)
    - Observaciones o acciones recomendadas

INSTRUCCIONES PARA LOS ALUMNOS

Entregable principal: Documento de Aplicabilidad (SoA) con análisis de controles tecnológicos de la ISO/IEC 27001:2022 (Anexo A).

Paso 1: Levantamiento de información

Analicen el caso y extraigan información clave para evaluar qué controles del Anexo A pueden aplicar.

Paso 2: Determinación de aplicabilidad

Evaluar cada control y justificar su aplicabilidad según el contexto de ITSEC Commerce.

Paso 3: Estado de cumplimiento

Para cada control aplicable, indicar si:

- Está implementado
- Está parcialmente implementado
- No está implementado

Paso 4: Observaciones y recomendaciones

Incluir observaciones breves y sugerencias de acción (por ejemplo, desarrollar una política, adquirir una solución, formalizar un contrato, etc.)

FORMATO DEL DOCUMENTO DE APLICABILIDAD

Se sugiere una estructura en tabla como la siguiente:

Control	Nombre del Control	¿Aplica?	Justificación	Estado de cumplimiento	Observaciones / Acciones
A.5.7	Contacto con autoridades	Sí	Empresa opera en sector regulado y	No implementado	Definir responsables de contacto con INDECOPI y

Control	Nombre del Control	¿Aplica?	Justificación	Estado de cumplimiento	Observaciones / Acciones
			gestiona datos personales		Autoridad de Protección de Datos
A.8.16	Gestión de acceso privilegiado	Sí	Existen accesos con privilegios a base de datos de clientes	Parcial	Implementar control de sesiones, monitoreo y revisión de cuentas
…	…	…	…	…	…

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

CONTEXTO GENERAL

Nombre de la organización: SOLUTEC S.A.
Sector: Servicios financieros digitales
Tamaño: 320 empleados
Cobertura: Nacional (presencia en las 24 regiones del país)

Infraestructura:

- Sede central en Lima (150 empleados, servicios críticos, servidores físicos y virtualizados)
- 6 sedes regionales con operaciones híbridas
- 80% de los servicios están desplegados en cloud pública (AWS y Azure)
- Aplicaciones principales desarrolladas en arquitectura web y API-first
- Red interna segmentada entre áreas administrativas, TI, desarrollo y atención al cliente
- Cuentan con un SOC tercerizado que opera en modalidad 24/7

En el último año, SOLUTEC S.A. ha vivido los siguientes eventos:

1. **Un ataque DDoS** dirigido al portal principal, generando 4 horas de caída del servicio y daño reputacional.
2. **Robo de credenciales de un usuario privilegiado**, lo que permitió un acceso lateral a varios entornos de prueba.
3. **Una aplicación expuesta públicamente fue comprometida a través de una API mal configurada.**
4. **Un colaborador descargó malware en su laptop corporativa a través de un correo de phishing, lo que provocó una propagación lateral limitada.**

5. Una **auditoría reciente reveló deficiencias** en el control de accesos en la nube, y falta de registros de eventos adecuados.
6. La empresa no ha realizado simulacros de incidentes ni capacitaciones de seguridad en los últimos 18 meses.

Los alumnos deberán identificar **al menos un control por cada capa**, evaluar si está presente, ausente o débil, y **proponer mejoras o nuevas implementaciones** según sea necesario:

1. **Perímetro:** Firewalls | IPS | VPN
2. **Red Interna:** Segmentación | IDS | Protección DDoS
3. **Dispositivos:** Antivirus/EDR | Cifrado de discos | Control de dispositivos externos
4. **Identidades:** IAM | MFA | SSO | Gestión de privilegios
5. **Aplicaciones:** Seguridad API | WAF | Revisión de código seguro
6. **Monitorización:** SIEM | SOC 24/7 | Correlación de eventos
7. **Nube:** Control de accesos | DLP | Configuración segura
8. **Incidentes:** Plan de respuesta | Procedimientos de recuperación | Gestión de crisis
9. **Formación:** Concienciación | Simulacros de phishing | Políticas de uso seguro
10. **Gobernanza:** Cumplimiento normativo (como ISO 27001, Ley de Protección de Datos) | Auditorías periódicas | Política de seguridad formalizada

---

INSTRUCCIONES PARA LOS ALUMNOS

1. **Realizar un diagnóstico capa por capa**, identificando:
    - Controles existentes (si los hay)
    - Riesgos asociados
    - Brechas evidenciadas
2. **Proponer un conjunto de medidas para cada capa**, categorizándolas como:
    - Preventivas
    - Detectivas
    - Reactivas
3. **Plantear una hoja de ruta de implementación** para los controles nuevos o mejorados, considerando:
    - Tiempo estimado
    - Recursos requeridos

- Dependencias

4. **Presentar su propuesta en un documento ejecutivo (máx. 10 páginas)** que incluya:
    - Diagnóstico por capa
    - Tabla de priorización
    - Estrategia integral
    - Anexos técnicos (opcional)

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

Almacenes Andinos S.A. es una empresa dedicada al almacenamiento y distribución de productos industriales. Su centro de operaciones cuenta con un sistema digital integrado que gestiona inventarios, logística y facturación. Este sistema recopila datos sensibles, como información financiera de clientes, contratos con proveedores y registros internos sobre movimientos de mercancías.

Recientemente, la compañía decidió implementar un nuevo almacén automatizado en una ubicación remota. Sin embargo, durante el desarrollo del proyecto, el equipo de TI identificó riesgos potenciales relacionados con la seguridad de los datos almacenados, tanto a nivel físico como digital.

Un empleado reportó la pérdida de acceso a una base de datos crítica utilizada para rastrear el inventario en tiempo real. Tras investigar, el equipo de soporte técnico descubrió que alguien había ingresado sin autorización a un terminal en el almacén y había descargado copias no cifradas de los registros de productos.

La situación fue agravada por la ausencia de una política clara sobre segmentación de datos: los registros financieros y logísticos estaban almacenados en la misma base de datos, aumentando el riesgo de una exposición masiva en caso de un acceso indebido. Además, el sistema carecía de controles efectivos para limitar el acceso según roles, lo que permitió que un usuario sin autorización adecuada pudiera realizar cambios en los registros.

Actividad

Con base en este caso, plantea propuestas para resolver las siguientes áreas críticas:

1. **Cifrado de Datos**: ¿Qué estrategias y herramientas recomendarías para garantizar que toda la información almacenada esté protegida contra accesos no autorizados?
2. **Control de Acceso**: ¿Qué mecanismos podrían implementarse para asegurarse de que solo las personas adecuadas tengan acceso a información específica?

3. **Seguridad Física**: ¿Qué medidas adicionales se podrían tomar para proteger las áreas donde se encuentran los servidores y garantizar que no sean vulnerables a accesos no autorizados?
4. **Segmentación de Datos**: ¿Cómo estructurarías las bases de datos para minimizar el impacto de un posible incidente de seguridad?