UNIVERSIDAD TECNOLÓGICA ISRAEL

SISTEMAS DE LA INFORMACIÓN

SEGURIDAD DE LA INFORMACIÓN

DAYANA CHINCHIN

LESLIE GUAMÁN

TEMA: Taller Repaso Examen

2025

Actividad de Revisión: Taller Integrador de Seguridad de la Información

Objetivo: Consolidar el conocimiento sobre Gobierno de Seguridad de la Información, Continuidad del Negocio y Aspectos Regulatorios mediante la aplicación práctica y análisis crítico.

Instrucciones:

Resolver los siguientes retos:

Parte 1: Gobierno de Seguridad de la Información

1. **Elaboren una matriz RACI para un área de TI ficticia de una empresa mediana (pueden usar la de su empresa si aplica).**

Empresa: Pinatech empresa de servicios tecnológicos

Actividad / Proceso TI	Director General	Director de TI	Administrador de Sistemas	Soporte de Servicio Técnico
Definir estrategia tecnológica anual	I	A	C	C
Implementar políticas de seguridad en TI	I	A	R	C
Administración de servidores y redes	I	C	A/R	I
Desarrollo de software interno (ERP, intranet, etc.)	I	A	C	R
Soporte técnico a usuarios	I	C	C	I
Gestión de licencias y proveedores de TI	I	A	C	I
Copias de seguridad y recuperación ante desastres	I	A	R	I
Capacitación tecnológica al personal	I	C	C	C
Control de presupuestos de TI	I	A	C	I
Evaluación de desempeño del personal TI	I	A	C	C

2. Establezcan 3 políticas de seguridad basadas en las necesidades del negocio y justifiquen su elección.

- Política de Control de accesos a la información interna de la empresa como pueden ser contraseñas, autentificación de doble factor, roles y permisos de usuarios para cada uno de los sistemas.
- Política de uso aceptable de los recursos tecnológicos que establece reglas de la utilización adecuado de equipos, redes, correos e internet
- Política de backup y la recuperación de información ante desastres naturales o cualquier otro acontecimiento, esto regula cuando y donde se realizan las copias de seguridad define responsabilidades y tiempos de recuperación de la información perdida

3. Identifiquen un proceso clave de TI y elaboren una mini matriz de riesgos (activo, amenaza, vulnerabilidad, impacto, respuesta).

ID	Riesgo Identificado	AMENAZA	probabilidad	impacto	Clasificación	mitigacion	Responsable
R1	Falla en la ejecución del respaldo	Error del software de backup o falta de espacio en disco	4	4	Alto	Implementar equipos con mas capacidad para que los equipos donde guardamos los respaldos no se saturen	Oficial de seguridad Informatica
R2	Respaldo incompleto o corrupto	Copia interrumpida o verificación omitida	4	4	Alto	Revision de backups semanalmente donde se garantice que la informacion esta completa	Oficial de seguridad Informatica
R3	Pérdida de soportes físicos o accesos a la nube	Robo, mal manejo o mal control de accesos	4	3	Alto	Realizar una auditoria cada semana parta evitar robos de informacion ademas que plantear una politica de cambios de claves cada cierto tiempo	Oficial de seguridad Informatica

Parte 2: Plan de Continuidad del Negocio (BCP)

1. Proceso crítico

Gestión de tickets (pagos, incidentes y marketing)

Garantizar el registro, priorización, atención y cierre oportuno de requerimientos de servicios de pagos, incidentes y servicios de marketing, asegurando continuidad operativa y comunicación efectiva con las áreas de negocio.

Alcance

- Incluye: apertura de tickets (portal, email, teléfono/IVR, chat), clasificación por prioridad, asignación L1/L2/L3, escalamiento, resolución, cierre con validación, comunicación de incidentes mayores.
- Excluye: compras de hardware/insumos y desarrollos fuera del catálogo.
- Horarios por prioridad:
    - P1 (Centros de Pago): 24×7.
    - P2 (Sistemas/Fallas de equipos): horario laboral ampliado.
    - P3 (Marketing): horario laboral.

RTO y RPO

- Global del proceso: RTO 30 min / RPO 15 min (si cae la herramienta de tickets → Plan B).
- Por prioridad:
    - P1 (Centros de Pago): RTO 15 min / RPO 5 min
    - P2 (Sistemas): RTO 60 min / RPO 30 min
    - P3 (Marketing): RTO 4 h / RPO 60 min

Soporte del RPO: BD de tickets con PITR o réplicas/incrementales ≤ 15 min + exportación diaria a almacenamiento alterno.

Principales recursos

- Personas/Roles:
    - Líder Mesa de Ayuda / Coordinador (SLA, escalamiento, comunicación).
    - Agentes L1 (registro y comunicación).
    - Especialistas L2/L3 (infra, redes, aplicaciones, POS, marketing ops).

      Comunicaciones (incidente mayor), Compras (repuestos críticos).
- Tecnología:
    - Plataforma de ticketing on-prem , CMDB, integraciones (correo, chat, monitoreo).
    - Herramientas remotas, inventario de activos/CMDB.
    - Backups+PITR BD de tickets + exportación diaria a repositorio alterno.

2. Esquema básico de BCP

Objetivos

Mantener la continuidad del proceso dentro de los RTO/RPO definidos, con comunicación clara a negocio.

Específicos

- Responder P1 en ≤ 5 min y restaurar en ≤15 min.
- Activar Plan B si cae la herramienta en ≤30 min.
- Preservar trazabilidad (RPO global ≤15 min) y migrar datos al restablecer.
- SLA mensual ≥90%, reaperturas <3%.

Responsables

- Dirección de Operaciones o Finanzas.
- Dueño del proceso: Coordinador de Mesa de Ayuda.
- Área de TI: Líder de Plataforma.
- Comunicaciones: Responsable de Comunicaciones.
- Seguridad: Responsable de Ciberseguridad.

Fases

FASES	TAREA	ENTREGABLE

Preparación	Inventario de procesos/canales, roles y catálogo con prioridades.	política breve del proceso, Catálogo+SLAs, matriz RACI
BIA y Riesgos	Definir RTO/RPO	BIA, matriz de riesgos con medidas y dueños.
Estrategias y Planes	Plan B kits de repuestos,escalamiento por prioridad y criticidad, guías de comunicación.	planes por escenario, plantillas de mensajes
Implementación	Configurar backups+PITR, automatizaciones, listas de distribución, capacitación L1/L2.	Entregables: evidencias de configuración, manuales de resolución rápida
Pruebas/Simulacros	Tabletop mensual, restauración/traspaso de datos del plan B, simulacro P1 trimestral.	informes con hallazgos y acciones.
Mantenimiento/Mejora	Revisiones trimestrales, actualización de SLAs, métricas y lecciones aprendidas.	Registro de cambios y KPI.

Criterios de activación / desactivación del BCP

- Activación: indisponibilidad del ticketing > 5 min, corrupción de base de datos, caída de pasarela de pagos multi-sede, pérdida de conectividad primaria sin ETA <30 min.
- Desactivación: servicio estable ≥ 60 min, colas normalizadas, datos del Plan B migrados y validados.

Plan B (resumen operativo)

1. Publicar formulario/hoja y correo de contingencia (asunto: [P1|P2|P3]-Sede-Resumen).
2. Numeración temporal y registro mínimo obligatorio (sede, servicio, hora, impacto).
3. Reportes cada 15–30 min en P1.
4. Al restablecer, migrar a la herramienta, reconciliar y cerrar con validación del usuario.

3.Respondan en grupo: ¿Qué lecciones extraen del caso del incendio en la empresa de telecomunicaciones?

- Mantener copias de seguridad externas en otra ciudad o país, según la criticidad del negocio.

- Implementar servidores espejo para los servicios críticos, con mecanismos de conmutación (failover).
- Contratar seguros que cubran equipos críticos y pérdida por interrupción del negocio.
- Contar con un Plan de Recuperación ante Desastres (DRP) actualizado y probado.
- Activar de inmediato los planes previamente ensayados, siguiendo criterios de activación definidos.
- Sostener una comunicación clara y oportuna con colaboradores, clientes y autoridades durante el incidente.

Parte 3: Aspectos Regulatorios

1. Enumeren 3 riesgos legales asociados al mal manejo de datos personales según la legislación nacional.

1. **Riesgo:** La empresa puede recibir multas económicas muy grandes si utiliza almacena o comparte datos personales son el consentimiento del titular o sin cumplir las medidas de seguridad

2. **Riesgo:** Los responsables o encargados pueden enfrentar responsabilidad penal si tratan los datos personales con fines de lucro indebidos o engaños.

3. **Riego:** Un mal manejo de los datos como filtraciones de datos confidenciales de los clientes esto genera perdida de confianza de estos, socios e incluso autoridades máximas afectando la imagen de la empresa en el ámbito de ética y profesionalismo

2. **Propongan 2 controles para cumplir con la Ley Orgánica de Protección de Datos Personales**.

Control 1: Implementar un aviso de Privacidad claro y actualizado

Objetivo: Garantizar que los dueños de los datos conozcan que información se esta recopilando en la empresa con el propósito de que se haga conocer cómo se usan y con quien se comparte dicha información.

Acciones

- Elaborar un aviso de privacidad integral de los datos mediante encuestas.

- Definir una identidad del responsable del tratamiento de los datos

- Definir finalidades del uso de los datos de los clientes
- Incluir Mecanismos para ejercer derechos arco
- Incluir transferencias de datos a terceros
- Capacitar al personal para que conozcan y respete lo establecido según la ley de protección de datos ya implementada en la organización

Control 2: Proteger los datos personales contra perdidas, accesos no autorizados, alteración o destrucción

Acciones

- Definir roles y niveles de acceso en el cual solo personal autorizado pueda consultar y modificar datos que se encuentren dentro de la organización
- Aplicar control técnico como cifrado de base de datos y sacada de respaldos semanalmente
- Aplicar en los sistemas de la organización autentificación doble o multifactor para evitar que cualquier persona pueda entrar a los sistemas
- Aplicar antivirus y firewall actualizados
- Mantener riesgos de incidentes de seguridad y procedimientos de notificación de brechas
- Realizar auditorias mensuales y pruebas de vulnerabilidad para así detectar a tiempo algún incidente o riesgo que puedan tener los sistemas

3. Analicen un caso hipotético de violación de seguridad e identifiquen qué artículos del COIP podrían aplicarse.

Caso Hipotético:

Un técnico del área de soporte accede sin autorización a la base de datos de un cliente importante al extraer la información confidencial de este con el fin de venderla y adquirir un beneficio por un tercero que no pertenece a la empresa, esta violación se detecta cuando el cliente reporta accesos no reconocidos a sus cuentas y se inicia una auditoria interna.

Artículos identificados

Artículo 230 – Acceso no consentido a un sistema informático

"La persona que, sin autorización, acceda total o parcialmente a un sistema informático, telemático o de comunicación, será sancionada con pena privativa de libertad de uno a tres años."

Artículo 231 – Interceptación o apoderamiento de información

“La persona que intercepte, acceda o se apodere de información contenida en un sistema informático sin autorización será sancionada con pena privativa de libertad de tres a cinco años.”

Artículo 232 – Transferencia o difusión de información ilícita

“La persona que difunda, revele o transfiera a terceros información obtenida de forma ilícita será sancionada con pena privativa de libertad de cinco a siete años.”