UNIVERSIDAD TECNOLOGICA DEL PERU
Gestión de Riesgos Informáticos
Segunda Evaluación

APELLIDOS Y NOMBRES: DAVIDH GABRIEL DIONICIO LAZO – U22242342

PREGUNTA 1:

Tomando de referencia la Segunda Exposición Grupal, resuma las Conclusiones y/o Recomendaciones en base al título de su exposición.

Gestión de riesgos en el sector salud peruano: protección de historias clínicas electrónicas y ciberseguridad hospitalaria bajo ISO 27005

Conclusiones:

- El sector salud peruano es uno de los más vulnerables a ciberataques debido a la naturaleza altamente sensible de los datos que gestiona (historias clínicas, diagnósticos, datos personales de pacientes) y a la acelerada digitalización de procesos asistenciales como la telemedicina, recetas electrónicas y sistemas HIS

- La aplicación de ISO 27005 permite identificar de forma estructurada los activos críticos del sector salud —como servidores de historias clínicas electrónicas (HCE), bases de datos de pacientes, equipos biomédicos conectados a red y plataformas de citas en línea—, evaluar las amenazas específicas (ransomware hospitalario, acceso no autorizado a datos clínicos, phishing dirigido a personal médico)

- Existe una sinergia obligatoria entre ISO 27005 y la normativa peruana, particularmente con la Ley N° 29733 (Ley de Protección de Datos Personales) y la NTP-ISO/IEC 27005:2018 adoptada por INACAL. Los hospitales y clínicas que gestionan datos sensibles de salud están obligados a implementar medidas técnicas y organizativas que la gestión de riesgos bajo ISO 27005 facilita de forma natural.

- La investigación aplicada en Perú confirma la efectividad de ISO 27005 en el sector salud. Estudios como el del Hospital Regional de Lambayeque (usando ISO 27005 + MAGERIT) y la evaluación de la OGITT del Instituto Nacional de Salud demuestran que la identificación y valoración de riesgos permite priorizar controles y reducir la exposición a amenazas críticas.

RECOMENDACION:

- Implementar un SGSI alineado a ISO 27001 con gestión de riesgos basada en ISO 27005 en todos los establecimientos de salud que gestionen historias clínicas electrónicas, priorizando la clasificación de activos según su criticidad (confidencialidad de datos del paciente, disponibilidad de sistemas de emergencia, integridad de recetas electrónicas)

- Establecer un Plan de Continuidad del Negocio (BCP) integrado con la gestión de riesgos para garantizar que, ante un incidente grave (ej.: ransomware), los procesos críticos de atención médica puedan continuar operando con procedimientos alternativos (registros manuales, backups offline, comunicación redundante)

- Designar un Comité de Seguridad de la Información con participación de la alta dirección del centro de salud, el área de TI, el responsable de datos personales y representantes clínicos, para que la gestión de riesgos no sea un ejercicio aislado de tecnología sino una decisión estratégica institucional.

- Cumplir con la normativa peruana de protección de datos (Ley N° 29733) asegurando que todo tratamiento de datos clínicos tenga consentimiento informado, que se implementen controles de acceso basados en roles y que se notifiquen las brechas de seguridad a la Autoridad Nacional de Protección de Datos Personales.

- Utilizar la NTP-ISO/IEC 27005:2018 como marco de referencia nacional, complementándola con metodologías probadas como MAGERIT u OCTAVE para adaptar el análisis de riesgos al contexto específico de cada institución de salud peruana.

PREGUNTA 2:

En el marco de la norma ISO 27005:2008, se requiere un proceso continuo de evaluación y tratamiento de riesgos. ¿Cómo debe una empresa realizar un análisis de riesgos informáticos para cumplir con los requisitos de la norma, y qué pasos específicos debería seguir para identificar, evaluar y tratar un riesgo relacionado con la pérdida de datos confidenciales debido a un ciberataque? Proporciona un ejemplo de cómo podría llevarse a cabo cada uno de estos pasos.

I. Primero seria establecimiento del contexto.

Se define el alcance, los criterios de evaluación y el apetito de riesgo de la organización.

Ejemplo:

Una empresa de telecomunicaciones peruana define que el alcance del análisis incluye su base de datos de clientes (5 millones de registros con nombres, DNI, direcciones y datos de facturación). Establece escalas de probabilidad (Rara vez / Posible / Probable / Casi seguro) e impacto (Bajo / Medio / Alto / Crítico), y determina que cualquier riesgo con nivel ≥ Alto requiere tratamiento inmediato.

II. IDENTIFAICAION DE RIESGOS

Se identifican los activos, las amenazas, las vulnerabilidades y las consecuencias.

Ejemplo:

Elemento	Descripción
Activo	Base de datos de clientes servidor SQL en data center propio)
Amenaza	Ciberataque tipo *SQL Injection* o *ransomware* dirigido
Vulnerabilidad	Software de base de datos sin parches de seguridad actualizados; ausencia de WAF (Web Application Firewall)
Consecuencia	Exfiltración de 5 millones de registros con datos personales → multas por incumplimiento de la Ley N° 29733, pérdida de confianza de clientes, demandas legales

IV. EVALUACION DE RIESGOS

Se compara el nivel de riesgo obtenido con los criterios de aceptación definidos en el priemero.

Ejemplo:

El riesgo obtuvo una puntuación de 16 (Crítico), superando ampliamente el umbral de aceptación de la empresa (≤ 6). Por lo tanto, este riesgo **no es aceptable** y requiere tratamiento prioritario e inmediato. Se ubica en la esquina superior derecha del mapa de calor (zona roja).

V. TRATAMIENTO DE RIESGOS

Se selecciona una estrategia de tratamiento: mitigar, transferir, evitar o aceptar.

Ejemplo para mitigar:

Control	Descripción	Responsable
Parcheo y hardening	Implementar un programa mensual de actualización de parches y configuración segura de servidores	Equipo de infraestructura
WAF + IDS/IPS	Instalar un Web Application Firewall y sistema de detección/prevención de intrusiones	Equipo de ciberseguridad
Cifrado de datos	Cifrar la base de datos en reposo (AES-256) y en tránsito (TLS 1.3)	DBA + Seguridad
Segmentación de red	Aislar el servidor de base de datos en una VLAN dedicada con acceso restringido	Redes
Backup y DRP	Respaldos diarios cifrados con pruebas de restauración mensuales	Operaciones TI
Concienciación	Capacitación trimestral al personal en phishing, ingeniería social y manejo de datos	RRHH +Seguridad
Transferencia parcial	Contratar un ciberseguro que cubra costes de notificación y respuesta a incidentes	Gerencia de Riesgos

VI. ACEPTACION DEL RIESGO RESIDUAL

Tras aplicar los controles, se recalcula el riesgo residual y la alta dirección lo acepta formalmente.

EJEMPLO:

Después de implementar los controles, la probabilidad baja a Posible (2) y el impacto a Alto (3). El riesgo residual = 2 × 3 = 6 (Moderado), que se encuentra dentro del umbral de aceptación de la empresa. La Gerencia General firma el acta de aceptación del riesgo residual.

VII. MONITORIE Y REVISION Y COMUNICACIÓN CONTINUA

Ejemplo:

Se programa una revisión trimestral de vulnerabilidades (escaneo con Nessus/Qualys), se realizan pruebas de penetración anuales, se revisan los indicadores de incidentes y se reporta al Comité de Seguridad de la Información. Si surge una nueva amenaza (ej.: un zero-day en el motor de base de datos), se reinicia el ciclo desde la identificación.

PREGUNTA 3:

Análisis de riesgos y Matriz de Riesgos (Matriz de Calor)

Una empresa de comercio electrónico está experimentando un aumento en el número de intentos de ataque de phishing a sus clientes. Utilizando una matriz de riesgos (matriz de calor), ¿cómo identificarías y clasificarías el riesgo de un ataque exitoso de phishing? Explica cómo la probabilidad de ocurrencia y el impacto del riesgo afectan su clasificación en la matriz, y qué acciones específicas debería tomar la empresa para mitigar este riesgo.

I. Identificación del riesgo

Elemento	Descripción
Riesgo	Ataque exitoso de phishing que suplanta la identidad de la empresa para robar credenciales y datos de pago de clientes
Amenaza	Ciberdelincuentes que envían correos/SMS/sitios web falsos imitando la marca de la empresa
Vulnerabilidad	Falta de autenticación multifactor (MFA) en cuentas de clientes; ausencia de campañas de concienciación al usuario final; dominio sin protección DMARC/DKIM/SPF

Consecuencia	Robo de datos de tarjetas de crédito, fraude financiero, pérdida de confianza del cliente, sanciones regulatorias, caída de ventas

II. Definición de escalas (Matriz 5×5)

Escala de Probabilidad:

Nivel	Valor	Descripción
Rara vez	1	Menos de 1 vez cada 5 años
Improbable	2	1 vez cada 1-5 años
Posible	3	1 vez al año
Probable	4	Varias veces al año
Casi seguro	5	Ocurre frecuentemente (mensual o más)

Escala de Impacto:

Nivel	Valor	Descripción
Insignificante	1	Sin afectación significativa
Menor	2	Pérdida financiera menor, pocos clientes afectados
Moderado	3	Pérdida financiera considerable, decenas de clientes afectados
Mayor	4	Gran pérdida financiera, cientos de clientes afectados, cobertura mediática
Catastrófico	5	Pérdida masiva, miles de clientes afectados, sanciones regulatorias graves, daño reputacional severo

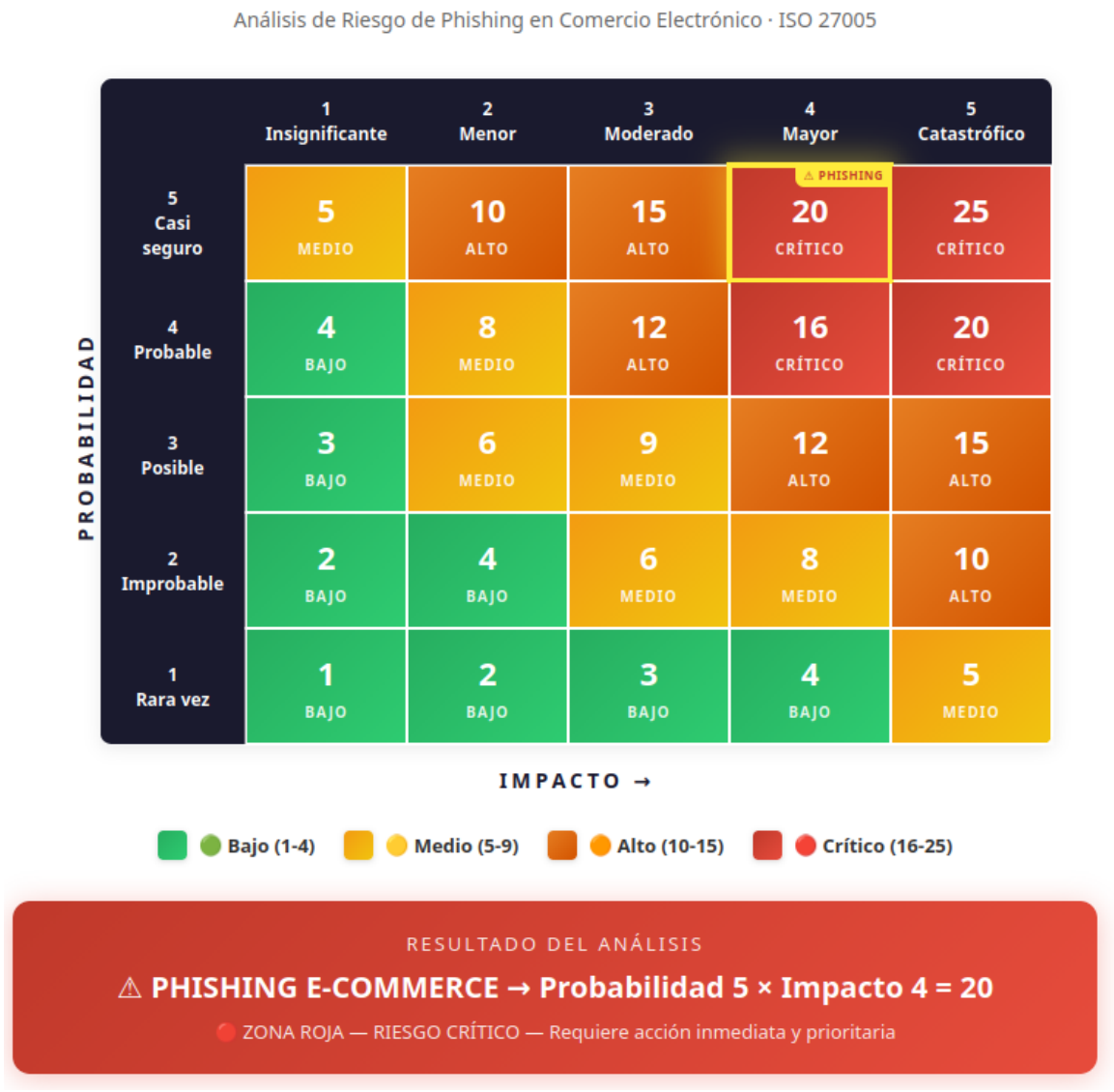
III. Evaluación y clasificación en la Matriz de Calor

Para el caso de la empresa de e-commerce con **aumento de intentos de phishing**:

- **Probabilidad = Casi seguro (5):** Los intentos de phishing son cada vez más frecuentes (ocurren semanalmente), y dado que la empresa no tiene MFA ni protección de dominio robusta, la probabilidad de un ataque **exitoso** es muy alta.
- **Impacto = Mayor (4):** Un ataque exitoso podría comprometer datos de pago de cientos de clientes, generar contracargos masivos, multas regulatorias y pérdida de confianza en la plataforma.

Nivel de Riesgo = 5 × 4 = 20 → RIESGO EXTREMO

IV. Mapa de Calor (Matriz 5×5)



V. ¿Cómo afectan la probabilidad y el impacto a la clasificación?

- **La probabilidad alta** (5) ubica el riesgo en la fila superior de la matriz, lo que significa que es un evento que se espera que ocurra con alta frecuencia. En el caso del phishing, el aumento constante de intentos y la sofisticación de las técnicas de suplantación (URLs similares, correos personalizados con datos reales del cliente) elevan la probabilidad al nivel máximo.
- **El impacto alto** (4) ubica el riesgo hacia la derecha de la matriz, reflejando consecuencias graves: pérdida financiera por fraude con tarjetas, costes de notificación a clientes afectados, posibles sanciones de INDECOPI y la SBS, y deterioro de la imagen de marca en un mercado altamente competitivo.

- **La combinación de ambos factores** (5 × 4 = 20) coloca el riesgo en la **zona roja (crítica)** del mapa de calor, lo que indica que requiere **acción inmediata y prioritaria**. [piranirisk.com], [templarcib...uridad.com]

VI. Acciones específicas de mitigación

Nº	Acción	Descripción	Prioridad
1	**Implementar MFA obligatorio**	Autenticación multifactor para todas las cuentas de clientes (OTP por SMS/app)	Inmediata
2	**Configurar DMARC, DKIM y SPF**	Proteger el dominio de correo para evitar que los atacantes suplanten la identidad de la empresa en emails	Inmediata
3	**Desplegar un sistema anti-phishing**	Herramienta de detección y takedown automático de sitios web y dominios falsos que suplanten la marca	Inmediata
4	**Campaña de concienciación a clientes**	Enviar comunicaciones periódicas educando a los clientes sobre cómo identificar correos/sitios falsos; incluir banner permanente en la web/app	Alta
5	**Monitoreo de marca en internet**	Contratar servicios de brand monitoring y threat intelligence para detectar nuevos dominios de phishing en tiempo real	Alta
6	**Canal de reporte de phishing**	Habilitar un botón o correo dedicado (ej.: reportephishing@empresa.com) para que los clientes reporten intentos sospechosos	Media
7	**Certificado EV SSL y sello de confianza**	Usar certificado SSL de validación extendida y sellos de seguridad visibles para que el cliente identifique el sitio legítimo	Media
8	**Simulacros internos de phishing**	Realizar ejercicios de phishing simulado al personal interno para fortalecer la primera línea de defensa	Alta
9	**Revisión periódica y mejora continua**	Evaluar trimestralmente la eficacia de los controles, actualizar la matriz de riesgos y ajustar estrategias según nuevas amenazas	Media

7. Riesgo residual esperado tras la mitigación

Después de implementar los controles:

- **Probabilidad baja a:** Posible (3) — se reducen significativamente los ataques exitosos
- **Impacto baja a:** Moderado (3) — el MFA y la detección temprana limitan el daño
- **Riesgo residual = 3 × 3 = 9** — dentro del umbral aceptable