Caso	Activos Críticos	Amenaza	Vulnerabilidades	Impacto	Probabilidad	Nivel de Riesgo	Medidas de Tratamiento
1. Robo de credenciales por phishing	Credenciales de usuarios, sistema académico, información académica	Suplantación vía phishing	Falta de 2FA Falta de filtros anti-spam Ausencia de capacitación	Alto (modificación de datos académicos)	Alta	Crítico	Implementar 2FA Filtros de spam y análisis de enlaces Campañas de concientización Monitoreo de accesos sospechosos
2. Ransomware en clínica odontológica	Datos clínicos, administrativos y financieros	Malware (ransomware)	Antivirus caducado Sin copias de seguridad Red no segmentada	Muy Alto (pérdida operativa y legal)	Alta	Crítico	Políticas de respaldo automático Software antivirus actualizado Segmentación de red Capacitación al personal
3. Acceso no autorizado a cámara IP	Imágenes de vigilancia, sistema de monitoreo	Acceso no autorizado remoto	Contraseñas por defecto Firmware desactualizado Falta de autenticación segura	Alto (violación de privacidad y reputación)	Media	Alto	Cambiar contraseñas por defecto Actualizar firmware periódicamente Usar HTTPS y autenticación segura Activar

							alertas y logs
4. Uso indebido de información personal	Datos personales de ciudadanos	Uso indebido por personal interno	Sin auditoría de accesos Sin control de privilegios Sin clasificación de información	Muy Alto (sanciones legales, pérdida de confianza)	Media	Alto	Implementar registros de auditoría Gestión de accesos por roles Clasificación y protección de datos sensibles Acuerdos de confidencialidad
5. Corte de servicio por ataque DoS	Sitio web institucional, plataforma de inscripciones	Ataque de denegación de servicio (DoS)	Sin WAF ni protección DoS Infraestructura sin redundancia Falta de monitoreo en tiempo real	Alto (interrupción de servicios críticos)	Alta	Crítico	Implementar WAF y protección anti-DoS Arquitectura con alta disponibilidad Sistemas de monitoreo 24/7 Plan de respuesta ante incidentes