Nombre de la empresa	Clínica dental Andental
Descripción	Empresa andaluza dedicada a la prestación de servicios odontológicos y de salud bucodental. Cuenta con 25 trabajadores repartidos en tres clínicas (Córdoba, Málaga y Sevilla)
Fecha documento	15/08/2025
Tamaño de la empresa	25
Cantidad de oficinas	3
Teletrabajo	Administración (1 día a la semana)
Alcance legislativo	RGPD, LOPDGDD, normativa sanitaria española y andaluza
Alcance SGSI	Sistemas de información que soportan gestión de historiales, citas y facturación

Nota: este es un caso práctico sobre el estándar ISO 27001. Los datos son ficticios.

Nombre del activo	Tipo	Oficina	Criticidad	C	I	A	Valor CIA	Comentarios
Servidor central	Hardware	Málaga	3	3	3	3	9	Servidor situado en Málaga
Máquina Rayos X	Hardware	Todas	3	3	3	3	9	Una por clínica
Base de datos clientes (nube)	Información	Todas	3	3	3	3	9	
Terminal de pago	Servicio	Todas	3	2	3	3	8	Para cobro a pacientes. Contactless.
Ordenador recepción	Hardware	Todas	3	2	2	3	7	Para citas, historiales, presupuestos y envío de documentación.
Documentación en papel	Información	Todas	3	3	2	2	7	En recepción especialmente, pero también en despacho.
Personal administrativo	Personas	Todas	3	3	2	2	7	
Puerta de entrada	Infraestructura	Todas	2	3	1	2	6	Sin control de acceso y acristalada. Permite ver el interior incluso cuando está cerrada.
Cliente correo corporativo	Software	Todas	2	3	2	1	6	Windows365
Tablets y ordenador de consulta	Hardware	Todas	2	2	2	1	5	Uso en consulta para apoyo en historiales y explicación de tratamiento a los clientes.
Aplicaciones reuniones	Software	Todas	1	2	1	1	4	Teams
Impresora recepción	Hardware	Todas	1	1	1	1	3	Con funciones WiFi
Wifi sala de espera	Servicio	Todas	1	1	1	1	3	

Nota: este es un caso práctico sobre el estándar ISO 27001. Los datos son ficticios.

Nota: este es un caso práctico sobre el estándar ISO 27001. Los datos son ficticios.

ANÁLISIS DE RIESGOS					
Activo	Amenaza	Vulnerabilidad	Probabilidad	Impacto	**Riesgo**
Servidor central	Desastres naturales	No existe ventilación, protección anti incendios	2	3	**6**
	Difusión de software dañino	Ausencia de periodicidad en backups, falta de actualizaciones, inexistencia de política de uso adecuado	3	3	**9**
	Acceso no autorizado	Acceso físico o por red al servidor.	1	3	**3**
Máquina Rayos X	Fallo técnico	Sobrecarga, error interno, fallo eléctrico, mal uso.	3	2	**6**
	Robo o pérdida de información	Almacenamiento local sin cifrado, ausencia de control de acceso, transmisión sin TLS	2	3	**6**
	Daños físicos	Falta medidas anti incendio, falta vigilancia, control de acceso	2	3	**6**
Base de datos clientes (nube)	Destrucción de información	Dependencia del proveedor, ausencia de plan de recuperación y de copias redundantes	3	3	**9**
	Abuso de privilegios de acceso	Roles y privilegios no siempre actualizados, cuentas sin MFA, exceso de privilegios.	1	3	**3**
Terminal de pago	Robo o manipulación de datos de tarjeta	Software desactualizado, falta de PCI DSS	2	3	**6**
Ordenador recepción	Acceso no autorizado	Falta de bloqueo automático. No existe política de contraseñas seguras. Sin MFA	2	3	**6**

Documentación en papel	Acceso no autorizado	Almacenamiento sin proteger con llave, ausencia de control de accesos	2	3	**6**
	Destrucción de información	Falta de copias digitalizadas. Ausencia de plan de conservación documental.	1	3	**3**
Personal administrativo	Ingeniería social	Falta de formación en ciberseguridad, ausencia de simulacros o puestas en práctica de medidas de seguridad.	2	3	**6**
	Error humano / mala praxis	Envío de datos a destinatario incorrecto, uso de dispositivo personal en la red privada.	1	3	**3**
Puerta de entrada	Acceso no autorizado	Cerraduras sin control electrónico, ausencia de videovigilancia	2	3	**6**
Cliente correo corporativo	Difusión de software dañino	Falta de formación, falta de filtros anti spyware y malware	3	3	**9**
Tablets y ordenador de consulta	Robo o pérdida	Almacenamiento no seguro. servicio FindMe desactivado	1	3	**3**
	Malware / Ransomware	No actualización de SO, ausencia sofware antivirus, falta de formación al personal	2	3	**6**
	Acceso no autorizado	No existe MFA.	2	3	**6**
Aplicaciones reuniones (Teams)	Fuga de información	Uso de enlaces públicos sin contraseña, grabaciones sin control.	2	3	**6**
Impresora recepción	Fuga de información de documentos impresos y/o escaneados	Acceso sin PIN, almacenamiento local sin borrado automático.	1	2	**2**
Wifi sala de espera	Acceso indebido a la red corporativa.	No existe segmentación. clave WPA2 compartida con clientes.	2	2	**4**

Activo	Amenaza	Riesgo	Tratamiento del riesgo	Control ISO 27001	Medida aplicada
Servidor central	Desastres naturales	No existe ventilación, protección anti incendios	Mitigar	7.5 Protección contra amenazas físicas y ambientales; 7.1 Perímetros físicos de seguridad	Mitigación mediante ventilación adecuada, extintores y UPS
	Difusión de software dañino	Ausencia de periodicidad en backups, falta de actualizaciones, inexistencia de política de uso adecuado	Mitigar	8.7 Protección contra malware; 8.13 Copias de seguridad; 5.1 Políticas de seguridad de la información; 8.9 Gestión de vulnerabilidades	Mitigar mediante antivirus actualizado, parches de actualización periódicos y backups periódicos.
	Acceso no autorizado	Acceso físico o por red al servidor.	Mitigar	5.15 Control de acceso; 8.2 Derechos de acceso privilegiado; 8.3 Restricción de acceso a la información; 7.2 Entrada física	Mitigar mediante control de acceso físico y lógico, credenciales únicas y revisión periódica de permisos.
Máquina Rayos X	Fallo técnico	Sobrecarga, error interno, fallo eléctrico, mal uso.	Mitigar	8.6 Gestión de capacidad; 7.13 Mantenimiento de equipo; 5.8 Seguridad de la información en la gestión de proyectos	Mitigar mediante mantenimiento preventivo, formación del personal y sistemas de monitorización de carga eléctrica.
	Robo o pérdida de información	Almacenamiento local sin cifrado, ausencia de control de acceso, transmisión sin TLS	Mitigar	8.11 Enmascaramiento de datos; 8.12 Prevención de fuga de datos; 5.15 Control de acceso; 8.5 Autenticación segura	Mitigar con cifrado de datos, acceso restringido, transmisión segura (TLS) y políticas de gestión de información sensible.
	Daños físicos	Falta medidas anti incendio, falta vigilancia, control de acceso	Transferir	7.5 Protección contra amenazas físicas y ambientales; 7.2 Entrada física; 7.3 Asegurar oficinas, salas e instalaciones	Contratación de seguro que cubra daños físicos, comeplementando con extintores y cámaras de seguridad, así como controles físicos.
Base de datos clientes (nube)	Destrucción de información	Dependencia del proveedor, ausencia de plan de recuperación y de copias redundantes	Mitigar	5.23 Seguridad de la información para el uso de servicios en la nube; 8.13 Copias de seguridad; 8.14 Redundancia de las instalaciones de procesamiento de información; 5.24 Planificación y preparación de la gestión de incidentes	Mitigar mediante SLA claros con el proveedor, backups periódicos, almacenamiento redundante y plan de recuperación ante desastres.
	Abuso de privilegios de acceso	Roles y privilegios no siempre actualizados, cuentas sin MFA, exceso de privilegios.	Mitigar	5.16 Gestión de identidad; 5.18 Derechos de acceso; 8.5 Autenticación segura; 8.3 Restricción de acceso a la información	Mitigar mediante revisión periódica de roles, implementación de MFA, principio de menor privilegio y auditorías de acceso.
Terminal de pago	Robo o manipulación de datos de tarjeta	Software desactualizado, falta de PCI DSS	Mitigar	8.7 Protección contra malware; 8.9 Gestión de vulnerabilidades; 5.1 Políticas de seguridad de la información	Mitigar mediante actualización del software, cumplimiento de estándares PCI DSS, monitoreo de transacciones y antivirus.
Ordenador recepción	Acceso no autorizado	Falta de bloqueo automático. No existe política de contraseñas seguras. Sin MFA	Mitigar	5.15 Control de acceso; 8.5 Autenticación segura; 8.2 Derechos de acceso privilegiado	Mitigar con bloqueo automático, contraseñas robustas, autenticación multifactor y revisiones periódicas de permisos.
Documentación en papel	Acceso no autorizado	Almacenamiento sin proteger con llave, ausencia de control de accesos	Mitigar	7.2 Entrada física; 7.3 Asegurar oficinas, salas e instalaciones; 5.15 Control de acceso	Mitigar mediante armarios cerrados, control de acceso físico y registro de quién accede a la documentación.
	Destrucción de información	Falta de copias digitalizadas. Ausencia de plan de conservación documental.	Mitigar	8.13 Copias de seguridad; 5.24 Planificación y preparación de la gestión de incidentes	Mitigar mediante digitalización de documentos, almacenamiento seguro en la nube o servidor interno, y plan de conservación documental.
Personal administrativo	Ingeniería social	Falta de formación en ciberseguridad, ausencia de simulacros o puestas en práctica de medidas de seguridad.	Mitigar	6.3 Concientización, educación y capacitación en seguridad de la información; 5.1 Políticas de seguridad de la información	Mitigar mediante formación periódica en ciberseguridad, simulacros de phishing y políticas claras de manejo de información sensible.
	Error humano / mala praxis	Envío de datos a destinatario incorrecto, uso de dispositivo personal en la red corporativa	Mitigar	5.15 Control de acceso; 8.12 Prevención de fuga de datos; 6.3 Concientización, educación y capacitación	Mitigar mediante políticas de uso de dispositivos personales, cifrado de datos, protocolos de verificación antes de enviar información y formación.
Puerta de entrada	Acceso no autorizado	Cerraduras sin control electrónico, ausencia de videovigilancia	Mitigar	7.2 Entrada física; 7.3 Asegurar oficinas, salas e instalaciones; 7.4 Monitoreo de seguridad física	Mitigar mediante cerraduras electrónicas, videovigilancia y registro de accesos.
Cliente correo corporativo	Difusión de software dañino	Falta de formación, falta de filtros anti spyware y malware	Mitigar	8.7 Protección contra malware; 6.3 Concientización, educación y capacitación; 8.12 Prevención de fuga de datos	Mitigar mediante filtros de correo, antivirus actualizado, formación de usuarios y políticas de uso seguro del correo corporativo.
Tablets y ordenador de consulta	Robo o pérdida	Almacenamiento no seguro. servicio FindMe desactivado	Mitigar	7.8 Emplazamiento y protección de equipos; 8.10 Eliminación de información; 8.11 Enmascaramiento de datos	Mitigar mediante cifrado de dispositivos, activación de servicios de localización/remoto (FindMe), y políticas de protección de equipos.
	Malware / Ransomware	No actualización de SO, ausencia sofware antivirus, falta de formación al personal	Mitigar	8.7 Protección contra malware; 8.9 Gestión de vulnerabilidades; 6.3 Concientización, educación y capacitación	Mitigar mediante actualizaciones periódicas, antivirus actualizado y formación del personal en buenas prácticas.
	Acceso no autorizado	No existe MFA.	Mitigar	8.5 Autenticación segura; 5.18 Derechos de acceso	Mitigar mediante implementación de autenticación multifactor y control de privilegios.
Aplicaciones reuniones (Teams)	Fuga de información	Uso de enlaces públicos sin contraseña, grabaciones sin control.	Mitigar	8.12 Prevención de fuga de datos; 5.15 Control de acceso; 5.14 Transferencia de información	Mitigar mediante políticas de uso seguro, control de enlaces compartidos, cifrado de grabaciones y acceso restringido.
Impresora recepción	Fuga de información de documentos impresos y/o escaneados	Acceso sin PIN, almacenamiento local sin borrado automático.	Mitigar	5.15 Control de acceso; 8.10 Eliminación de información; 8.11 Enmascaramiento de datos	Mitigar mediante PIN de acceso, borrado automático de trabajos y control de acceso físico a la impresora.
Wifi sala de espera	Acceso indebido a la red corporativa.	No existe segmentación. clave WPA2 compartida con clientes.	Mitigar	8.22 Segregación de redes; 8.3 Restricción de acceso a la información	Mitigar mediante segmentación de redes (red de invitados separada), gestión de contraseñas robustas y acceso limitado.

Nota: este es un caso práctico sobre el estándar ISO 27001. Los datos son ficticios.

Activo	Medida	Responsable	Plazo previsto implementación	Estado	Revisión periódica	Comentarios
Servidor central	Ventilación adecuada, detector de incendios, implementación UPS y de extintores.	IT	15/10/2025	Pendiente	Trimestral	Cumplir compromimso de renovación extintores
	Antivirus actualizado, backups periódicos (semanal)	Técnico de sistemas	14/09/2025	Parcialmente implementado	Mensual	Confirmar funcionamiento de backups y actualizaciones del sistema y antivirus.
	Control de acceso físico y lógico al servidor central, credenciales únicas.	CISO	10/09/2025	Completamente implementado	Trimestral	Registrar permisos y accesos, registrar cambios y controles aplicados.
Máquina Rayos X	Mantenmiento preventivo, formación del personal, monitorización de carga eléctrica.	Responsable de mantenimiento.	01/10/2025	Pendiente	Semestral	Registrar incidencias, revisar procedimientos.
	Cifrado de datos, acceso restringido, transmisión segura (TLS)	Técnico de seguridad	15/10/2025	Pendiente	Trimestral	
	Uso extintores, cámaras de seguridad, controles de acceso físico y ubicación en salas seguras.	CISO y compañía de seguros	30/09/2025	Parcialmente implementado	Anual	Seguro como transferencia de riesgo; extintores y vigilancia como mitigación complementaria.
Base de datos clientes (nube)	SLA con proveedor, establecer periodicidad de los backups, redundancia, establecer protocolo de recuepración de datos	CISO y técnico de seguridad	15/12/2025	Parcialmente implementado	Mensual	Comprobar ejecución de backups, realizar simulacros de recuperación. Actualizar y completar protocolo.
	Revisión periódica de roles, implementación de MFA, principio de menor privilegio y auditorías de acceso.	CISO y técnico de sistemas	30/09/2025	Parcialmente implementado	Mensual	Implantar RBAC, generar cuenta de bajo privilegio para personas en prácticas.
Terminal de pago	Actualización del software, cumplimiento de estándares PCI DSS, monitoreo de transacciones y antivirus.	Técnico de seguridad	15/10/2025	Pendiente	Trimestral	
Ordenador recepción	Implantación bloqueo automático, contraseñas robustas, autenticación multifactor y revisiones periódicas de permisos.	Técnico de sistemas	15/09/2025	Parcialmente implementado	Semestral	Generar política de contraseñas robustas y renovación de contraseña cada seis meses. Implantar MFA con teléfono de empresa como token + usuario/contraseña

Documentación en papel	Mitigar mediante armarios cerrados, control de acceso físico y registro de quién accede a la documentación.	Técnico de seguridad	15/09/2025	Pendiente	Semestral	
	Mitigar mediante digitalización de documentos, almacenamiento seguro en la nube o servidor interno, y plan de conservación documental.	Personal recepción	15/12/2025	Parcialmente implementado	-	Abandonar de manera gradual este método de recogida de datos en la medida de lo posible.
Personal administrativo	Formación en ciberseguridad, simulacros phishing.	CISO	01/11/2025	Pendiente	Semestral	Actualizar formación según nuevas amenazas detectadas.
	Generar políticas de uso de dispositivos personales, cifrado de datos, protocolos de verificación antes de enviar información y formación.	CISO y técnico de seguridad	15/12/2025	Pendiente	Semestral	
Puerta de entrada	Implantar cerraduras electrónicas, videovigilancia y registro de accesos.	Técnico de seguridad	15/01/2026	Pendiente	Anual	
Cliente correo corporativo	Uso de filtros de correo, antivirus actualizado, formación de usuarios y políticas de uso seguro del correo corporativo.	CISO y técnico de sistemas	15/09/2025	Pendiente	Semestral	
Tablets y ordenador de consulta	Cifrado de dispositivos, activación de servicios de localización/remoto (FindMe), y políticas de protección de equipos.	Técnico de seguridad	15/01/2026	Pendiente	Semestral	
	Actualizaciones periódicas, antivirus actualizado y formación del personal en buenas prácticas.	Técnico de sistemas	15/11/2025	Parcialmente implementado	Trimestral	
	Implementación de autenticación multifactor y control de privilegios.	Técnico de seguridad	30/09/2025	Pendiente	Trimestral	
Aplicaciones reuniones (Teams)	Políticas de uso seguro, control de enlaces compartidos, cifrado de grabaciones y acceso restringidido	CISO y técnico de seguridad	15/12/2025	Pendiente	Trimestral	
Impresora recepción	Generar PIN de acceso, borrado automático de trabajos y control de acceso físico a la impresora.	Técnico de sistemas	15/09/2025	Totalmente implementado	Semestral	
Wifi sala de espera	Segmentación de redes (red de invitados separada), gestión de contraseñas robustas y acceso limitado.	Técnico de seguridad	30/10/2025	Parcialmente implementado	Trimestral	Implantar DMZ

Nota: este es un caso práctico sobre el estándar ISO 27001. Los datos son ficticios.