INFORME FINAL DE AUDITORÍA INFORMÁTICA

Fecha del Informe: 09/11/2025
Nombre de la Entidad: Empresa de Medicina Prepaga OSDE
Objetivo: Evaluar la seguridad, organización y protección de la Red Física utilizada por el área de sistemas, determinando el riesgo de acceso físico no autorizado, la integridad del cableado y la continuidad operativa.
Lugar de la Auditoría: Área de Sistemas / Centros de Atención
Grupo de Trabajo de Auditoría: Torres Exequiel
Fecha de Inicio de Auditoría: 01/11/2025
Tiempo estimado de proceso de revisión: 80 hrs
Fecha de Finalización de la Auditoría: 13/11/2025

II. Alcance de la Auditoría
La auditoría se centró exclusivamente sobre la Red Física de la empresa, abarcando las áreas de Hardware, Usuario y Software. El trabajo se enfocó en la infraestructura crítica, especialmente en el control de acceso físico a servidores (Riesgo 95%) y la protección del cableado (Riesgo 90%), siendo estos los puntos con mayor probabilidad de afectar la continuidad operativa y la confidencialidad de la información.

III. Herramientas Utilizadas

- Etiquetadora, Libreta, Cámara Fotográfica, Lista de Verificación (Checklist), Cinta métrica, Planos de la Oficina.
- CMDB, Diagramas Lógicos de Red, Hoja de Cálculo / Software de Reporting, Consola de Gestión de Servidores/Switches, Documentación del fabricante (UPS).
- Registros de Control de Acceso (Biométrico/Libro), Herramienta de Auditoría de Cuentas (Consola AD), Consola de Gestión de Identidades (IAM/SSO).
- Correo electrónico de prueba, Registros de DLP.
- Visor de Eventos del SO, Herramienta de extracción forense, Herramienta de Cálculo de Hash, Herramienta SIEM, Servidor / Cronómetro.
- Consola de Gestión de Licencias, Inventario de Software, Consola de Monitoreo, Software de Gestión de Monitoreo.

- Escáner de Vulnerabilidades (ej. Nessus, OpenVAS), Herramienta de Gestión de Parches (WSUS/SCCM).
- Checklist de Mantenimiento, Medidor de Voltaje/Carga.

IV. Procedimientos a Aplicar

- Inspección física del etiquetado de al menos 10 puertos en switches y servidores.
- Comparación del Mapeo Físico (conexión real) contra la data registrada en la CMDB.
- Generación de una Lista de Inconsistencias detectadas entre el inventario físico y la CMDB.
- Inspección visual de que todos los servidores críticos cuenten con dos fuentes de poder conectadas a distintas líneas eléctricas.
- Validación en la Consola de Gestión de la configuración de alertas ante un fallo de PSU.
- Prueba de extracción simulada de una PSU para validar la alerta y la continuidad del servicio.
- Inspección visual de la limpieza interna de al menos 5 servidores críticos (niveles de polvo, suciedad).
- Observación directa de 3 accesos a la sala para verificar si el personal deja fuera dispositivos de almacenamiento no autorizados.
- Toma de evidencia fotográfica del estado de organización y limpieza general de la sala.
- Verificación visual de cables de red y alimentación que cruzan pasillos o áreas de alto tráfico.
- Medición de la distancia física entre el cableado de red y las líneas de alimentación eléctrica en un muestreo de 5 puntos.
- Toma de evidencia fotográfica del estado del cableado y el uso de bridas.
- Intento de acceso a una cuenta de administrador de dominio utilizando solo contraseña (verificar fallo por MFA).
- Revisión de la configuración técnica de las cuentas administrativas para confirmar la inexistencia de cuentas genéricas sin propietario único.
- Simulación de solicitud de acceso temporal (JIT) para verificar que el sistema limita el tiempo de privilegios.
- Observación directa de 5 estaciones de trabajo del área administrativa para verificar si la PII queda visible en pantallas desatendidas.
- Prueba de intento de envío de un archivo con datos sensibles (ej. historial clínico) a través de un correo electrónico personal no cifrado.
- Inspección de las bandejas de entrada de un muestreo de 3 usuarios para validar el uso de herramientas de cifrado/transferencia segura.
- Extracción de un archivo de logs de un servidor crítico (ej. de la última semana) utilizando herramientas forenses.
- Cálculo del Hash (SHA-256) del archivo de logs extraído antes de su análisis y transferencia para verificar la integridad.
- Verificación en el sistema SIEM de la capacidad de retención y la integridad de los logs más antiguos (revisión de metadatos).
- Inspección de las propiedades de licenciamiento dentro del software de monitoreo de red para determinar su fecha de caducidad.

- Confrontación de la cantidad de dispositivos monitoreados activamente vs. la capacidad máxima permitida por la licencia activa.
- Generación de un reporte sobre el estado de la cobertura del software de monitoreo.
- Inspección física de la UPS para verificar su estado, conexiones y registro de mantenimiento visible.
- Cálculo de la antigüedad de las baterías de la UPS y su vida útil teórica.
- Medición de la autonomía real de la UPS durante una prueba de descarga bajo carga simulada.
- Ejecución de un escaneo de vulnerabilidades a un muestreo de 5 servidores críticos.
- Verificación en la Consola de Gestión de Parches las fechas de aplicación de los últimos parches de seguridad críticos.
- Comparación del nivel de parcheo (basado en el escaneo) con el estándar de clasificación de riesgo CVSS.

Situación Actual	Recomendación
Existe una desorganización extrema del cableado que impide identificar a qué terminal se conecta cada puerto del switch. La CMDB está desactualizada en este aspecto.	Estandarizar e Inventariar: Realizar una certificación completa del cableado para actualizar el Mapeo Lógico/Físico de puertos. Etiquetar cada cable en ambos extremos con su destino, y migrar esta información a la CMDB para mantenerla como fuente única.
Los servidores en los centros de atención están al acceso de cualquier persona del área de sistemas. No existe ningún registro formal de entradas y salidas de la sala.	Implementar Controles de Acceso: Instalar sistemas biométricos o de tarjetas de proximidad para limitar el ingreso. Implementar el uso obligatorio de un Libro de Registro (Log) para cada entrada y salida a la Sala de Cómputos.
La limpieza interna de los servidores es deficiente y no programada. La acumulación de polvo y suciedad es visible.	Formalizar Mantenimiento Preventivo: Crear un Plan de Mantenimiento Preventivo (PMP) con limpieza interna obligatoria de los servidores críticos de forma trimestral. Asignar un responsable y documentar la ejecución.
Los cables de red que están "a la vista de todos" muestran desgaste, daños menores y obstaculizan el paso en zonas de tránsito.	Proteger y Reemplazar: Reemplazar de inmediato los cables dañados o desgastados. Reubicar los cables que obstruyan el paso, utilizando canaletas de piso o protectores de cable para eliminar riesgos de accidente y fallo.
Ausencia de Autenticación Multifactor (MFA) para el acceso remoto/administrativo. Existe el riesgo de cuentas genéricas o contraseñas que no cumplen con los requisitos de robustez.	Reforzar Seguridad de Identidad: Implementar el uso obligatorio de MFA para todos los accesos con privilegios. Eliminar cuentas genéricas y aplicar

	una Política de Contraseñas Robustas (longitud mínima, símbolos) obligatoria.
Se observa PII visible en pantallas desatendidas. El personal carece de capacitación formal sobre las políticas de manejo seguro y cifrado de datos sensibles.	Estrategia de Concientización y DLP: Establecer un programa de capacitación formal, periódica y obligatoria en PII. Reforzar el estándar de "Escritorio Limpio" y exigir el uso de herramientas DLP o cifrado para la transferencia de datos.
Las licencias del software de monitoreo (ej. Nagios, Zabbix) no están actualizadas y existe falta de control sobre su vigencia y la cantidad de dispositivos monitoreados.	Gestión Centralizada de Activos: Crear un registro centralizado de todas las licencias y sus fechas de caducidad. Actualizar a la última versión estable del software de gestión para asegurar soporte y cobertura total.

VI. Conclusión

Sobre la base de los procedimientos de auditoría aplicados y la evidencia suficiente y adecuada obtenida, esta auditoría emite una opinión con salvedades sobre el entorno de la Red Física de OSDE.
La infraestructura se encuentra en un estado de riesgo inaceptablemente alto debido a la insuficiencia de controles de seguridad en las áreas de Acceso Físico a Servidores (95%) y la protección del Cableado de Comunicaciones (90%).
Esta condición representa una amenaza crítica a los pilares fundamentales de la seguridad:
Confidencialidad: Comprometida por la exposición de la Información Confidencial de Pacientes (PII) y la ausencia de Autenticación Multifactor (MFA) en accesos privilegiados.
Integridad: Comprometida por la falta de controles de acceso físico que impiden la trazabilidad y por la gestión deficiente de parches y vulnerabilidades en servidores.
Disponibilidad: Comprometida por la vulnerabilidad del cableado físico y el riesgo inminente de fallo del Sistema de Alimentación Ininterrumpida (UPS).
El cumplimiento de los objetivos de seguridad y la mitigación efectiva de los riesgos están supeditados a la implementación inmediata de las seis políticas formales y sus procedimientos asociados, transformando las recomendaciones en controles internos permanentes y auditables. Se requiere un compromiso explícito de la Gerencia para asignar los recursos necesarios y asegurar la adopción de estos

nuevos estándares de seguridad y continuidad operativa.