**2. Nivel de Riesgo General**

**ALTO (92%)**

**Justificación:**  
El proveedor presenta una combinación crítica de vulnerabilidades técnicas (puertos expuestos, falta de MFA, discos sin cifrar), ausencia de controles organizativos clave (sin análisis de riesgos, sin responsable formal de seguridad, sin formación al personal), deficiencias en el cumplimiento normativo (sin certificaciones, desconocimiento de ENS/RGPD) y exposición histórica a incidentes (filtraciones, malware, phishing). Pese a algunas señales recientes de mejora cultural (iniciativas de concienciación y ausencia de nuevos incidentes en los últimos 6 meses), el riesgo inherente sigue siendo muy elevado.

**3. Controles Críticos No Cumplidos o Parcialmente Cumplidos**

1. **Gestión de Identidades y Accesos**
   * No se aplica autenticación multifactor (MFA).
   * Acceso remoto sin restricciones ni protección adecuada.
   * No se revisan los accesos ni se monitorizan eventos de seguridad.
2. **Gestión de Activos y Actualizaciones**
   * Ausencia total de inventario técnico.
   * No existen políticas de actualización o mantenimiento de sistemas.
3. **Protección de Datos y Cumplimiento Normativo**
   * No se ha designado responsable formal de seguridad ni se ofrecen datos de contacto.
   * Desconocimiento parcial de ENS y RGPD; sin evidencia de cumplimiento.
   * Sin certificaciones ni auditorías de terceros subcontratados.
4. **Seguridad Técnica y Física**
   * No hay cifrado de discos ni bloqueo de dispositivos externos.
   * Equipos propios sin validación de seguridad avanzada.
   * Medidas de seguridad física solo parciales.
5. **Gestión de Riesgos y Continuidad de Negocio**
   * No se ha realizado un análisis de riesgos para el contrato.
   * No existe plan de continuidad, ni pruebas ni definición de RTO/RPO.
   * Carece de seguro frente a ciberataques.

**4. Recomendaciones Específicas y Priorizadas**

1. **Designación Formal de un Responsable de Seguridad y Evaluación de Riesgos (Alta Prioridad)**
   * Nombrar un CISO o DPO con datos de contacto accesibles.
   * Realizar de inmediato un análisis de riesgos del servicio conforme a ISO 27005 y ENS.
2. **Implementación de Controles Técnicos Básicos (Alta Prioridad)**
   * Aplicar MFA, cifrado de discos, restricción del acceso remoto y bloqueo de dispositivos externos.
   * Mantener inventario actualizado y políticas de parcheo/actualización periódica.
3. **Cumplimiento Normativo y Certificaciones (Media Prioridad)**
   * Iniciar procesos de adecuación al ENS (categoría básica al menos) y a ISO/IEC 27001:2022.
   * Formalizar contratos con subcontratistas que incluyan cláusulas de seguridad y mecanismos de auditoría.
4. **Planificación de Continuidad y Gestión de Incidentes (Media Prioridad)**
   * Definir RTO/RPO y diseñar un plan de continuidad de negocio con pruebas regulares.
   * Ampliar el procedimiento de gestión de incidentes incluyendo notificación al cliente y autoridades.

**5. Conclusión**

El proveedor evaluado presenta un perfil de **riesgo elevado** con carencias críticas en múltiples áreas de seguridad y cumplimiento. Se recomienda extremar la cautela y condicionar cualquier relación contractual a mejoras verificables.