Soporte de ASMS a los procesos de Disponibilidad,
Capacidad y Ciberseguridad

Esta sección reúne documentación que aplica de forma transversal a varios productos de Aranda Software, en lugar de estar limitada al manual de un único producto: mapeos de soporte a marcos y procesos (por ejemplo, ITIL), arquitectura de seguridad compartida y otros contenidos de referencia que atraviesan la plataforma.

Disponibilidad, Capacidad y Ciberseguridad

Soporte de ASMS a los procesos de Disponibilidad, Capacidad y Ciberseguridad

ASMS cumple los requisitos de Disponibilidad, Capacidad y Ciberseguridad mediante sus módulos existentes de CMDB/CMS, Gestión de Eventos, Niveles de Servicio (SLA), Reportería y Dashboards, e integración con herramientas externas de monitoreo, junto con la arquitectura de seguridad propia del servicio SaaS, todo alineado con las mejores prácticas ITIL. A continuación se detalla, requisito por requisito, cómo se cumple cada uno.

> ⚐ **Nota:** cuando el cumplimiento de una capacidad se apoya en parametrización adicional o en una herramienta de monitoreo externa integrada, se indica explícitamente. La configuración específica —fórmulas, umbrales, metodología de riesgo— se ajusta al modelo definido por cada organización cliente.

Gestión de Disponibilidad

¿Para qué sirve? Permite conocer, medir y anticipar la disponibilidad de los componentes tecnológicos y de los servicios que soportan, apoyándose en la información ya gestionada en la CMDB y en las herramientas de monitoreo integradas.

¿Cómo lo soporta ASMS?

Requisito	Módulo(s) que lo soportan	Cómo se soporta
Importar datos de disponibilidad desde fuentes de monitoreo	Integraciones / APIs	La plataforma se integra con herramientas externas de monitoreo para incorporar información de disponibilidad, eventos y estado de los componentes mediante las capacidades de interoperabilidad disponibles.
Calcular la disponibilidad de componentes individuales	CMDB, Integraciones	Los indicadores de disponibilidad se apoyan en los CI registrados en la CMDB y en la información recibida desde las fuentes de monitoreo integradas.
Calcular la disponibilidad de servicios de principio a fin	CMDB, Reportería	La CMDB relaciona los servicios con los componentes que los soportan; sobre esa relación y la información de monitoreo se construyen los indicadores de disponibilidad del servicio, con el modelo de cálculo configurado según las relaciones, horarios y criterios definidos.
Listar Funciones Vitales del Negocio (FVN) y analizar el impacto de su no disponibilidad	CMDB	Permite registrar y relacionar servicios críticos, procesos y elementos tecnológicos, incorporando atributos de criticidad e impacto que apoyan la identificación de las FVN.
Gestionar calendarios de ventanas de mantenimiento programado (PSO)	Gestión de Cambios, Calendario	Administra calendarios y ventanas de mantenimiento, relacionándolos con servicios y cambios programados, con consulta y visualización dentro de la planificación operativa.

Requisito	Módulo(s) que lo soportan	Cómo se soporta
Definir umbrales para evaluar cumplimiento de SLA de disponibilidad	SLA	Permite definir metas, condiciones y umbrales de nivel de servicio y hacer seguimiento al cumplimiento de los objetivos de disponibilidad establecidos.
Calcular la confiabilidad de componentes y servicios	CMDB, Reportería	Utiliza información histórica de disponibilidad, incidentes, eventos y componentes para construir indicadores de confiabilidad, con fórmulas configurables según el modelo de medición definido.
Apoyar la creación del Plan de Disponibilidad	Gestión de Proyectos/Actividades	Registra, estructura y hace seguimiento a la información, actividades e indicadores requeridos para elaborar y mantener el Plan de Disponibilidad.
Generar alarmas al superar un umbral definido	Gestión de Eventos	Configura reglas de notificación y escalamiento ante condiciones o umbrales definidos, generando alertas y acciones cuando se detectan desviaciones.
Asistir en el análisis de riesgo de disponibilidad	CMDB, Gestión de Incidentes	Utiliza la información de criticidad, impacto, servicios, CI, incidentes y disponibilidad para apoyar la evaluación de riesgo, con el modelo de valoración configurable según la metodología del cliente.
Analizar tendencias de disponibilidad	Reportería y Dashboards	Dispone de reportería, dashboards e indicadores que explotan la información histórica para analizar tendencias de disponibilidad de servicios y componentes.
Evaluar la capacidad del servicio ofrecido por proveedores	Gestión de Proveedores	Registra proveedores, servicios, contratos y compromisos, y hace seguimiento a su desempeño mediante indicadores, con criterios de evaluación configurables.
Integrarse con herramientas de monitoreo para detectar fallas	Gestión de Eventos, Integraciones	Recibe alertas y eventos de componentes desde herramientas externas de monitoreo y genera incidentes automáticamente mediante reglas previamente configuradas.
Interfaz con el CMS	CMDB	Se apoya en el CMS/CMDB para consultar y relacionar servicios con los CI y dependencias tecnológicas que los soportan.
Análisis CFIA (Component Failure Impact Analysis)	CMDB	Las relaciones y dependencias entre componentes y servicios registradas en la CMDB proporcionan la información necesaria para el análisis de impacto de falla, con el modelo estructurado según la metodología del cliente.
Análisis FTA (Fault Tree Analysis)	CMDB, Gestión de Problemas	La información de relaciones, dependencias, incidentes, problemas y eventos apoya el análisis de fallas y sus posibles causas, con la representación configurada según el modelo requerido.
Calcular costos asociados a la no disponibilidad	CMDB, Reportería	Registra información financiera, tiempos de indisponibilidad, criticidad e impacto de servicios y componentes; el cálculo se configura según las variables y reglas financieras definidas por el cliente.

Gestión de Capacidad

¿Para qué sirve? Permite centralizar y analizar la información de capacidad de componentes y servicios, apoyándose en la CMDB, los niveles de servicio, la gestión de eventos, la disponibilidad y la información de herramientas externas de monitoreo.

> ⚐ **Nota:** las capacidades especializadas de modelado predictivo y simulación se complementan mediante herramientas analíticas o de monitoreo integradas; ASMS centraliza y correlaciona la información, no

reemplaza motores de modelado estadístico especializado.

¿Cómo lo soporta ASMS?

Requisito	Módulo(s) que lo soportan	Cómo se soporta
Registrar datos de capacidad de los componentes	CMDB	Registra y mantiene información de capacidad de los componentes tecnológicos y CI gestionados, con los atributos y métricas requeridos para su seguimiento.
Capturar información de capacidad en función de las metas de nivel de servicio	SLA	Relaciona la información de servicios con los niveles de servicio establecidos, facilitando la evaluación de las métricas de capacidad frente a los objetivos definidos.
Reportar el desempeño de servicios de extremo a extremo a partir de monitoreo	Integraciones, Reportería	Integra información de herramientas de monitoreo y la relaciona con servicios y CI para el seguimiento del desempeño de extremo a extremo.
Definir y controlar la captura de información de monitoreo	Integraciones	Define los mecanismos de recepción y procesamiento de información externa; la frecuencia y métricas específicas dependen de las capacidades de la herramienta de monitoreo integrada.
Analizar tendencias de capacidad de servicios y componentes	Reportería y Dashboards	Dispone de reportería, dashboards e indicadores que explotan la información histórica para analizar tendencias de capacidad.
Analizar carga de trabajo y patrones de uso en periodos definidos	Reportería	Utiliza información histórica y métricas de las fuentes integradas para generar indicadores de carga de trabajo y patrones de utilización.
Integrarse con herramientas de monitoreo de capacidad	Integraciones / APIs	Dispone de APIs y mecanismos de interoperabilidad para integrarse con herramientas externas de monitoreo de capacidad, rendimiento y estado.
Asistir en la elaboración del Plan de Capacidad	Gestión de Proyectos/Actividades	Registra, estructura y hace seguimiento a la información, indicadores y actividades necesarias para elaborar y mantener el Plan de Capacidad.
Apoyar el dimensionamiento de aplicaciones	CMDB, Reportería	Consolida información de capacidad, utilización, servicios y componentes para apoyar el dimensionamiento; el cálculo técnico específico depende de las métricas y herramientas especializadas de cada plataforma.
Utilizar datos históricos y actuales para pronósticos de capacidad	Reportería	La información histórica y actual gestionada o incorporada desde fuentes externas se utiliza para análisis de tendencias y estimación de necesidades futuras.
Aplicar modelos analíticos para pronósticos	Reportería	Explota la información histórica mediante reportería e indicadores configurables.
Crear simulaciones para anticipar necesidades de capacidad	CMDB, Reportería	La información gestionada puede utilizarse como insumo para escenarios de planificación.
Capturar datos de capacidad desde diversas fuentes	Integraciones	Dispone de mecanismos de integración e importación para incorporar información de distintas fuentes, sujeto a los formatos y APIs disponibles.

Requisito	Módulo(s) que lo soportan	Cómo se soporta
Integrarse con el módulo de gestión de eventos	Gestión de Eventos	La Gestión de Capacidad se articula con la Gestión de Eventos, utilizando eventos y alertas de componentes y servicios para el seguimiento de condiciones de capacidad y rendimiento.
Interfaz de integración con el CMS	CMDB	Se integra funcionalmente con el CMS/CMDB, relacionando la información de capacidad con los CI, servicios y dependencias tecnológicas registrados.
Integrarse con el sistema de disponibilidad para correlacionar eventos con los CI	CMDB	Las prácticas de Capacidad, Disponibilidad, Eventos y Configuración están articuladas, utilizando los mismos CI y relaciones de la CMDB para contextualizar eventos y métricas asociadas a los servicios.
Integrarse con las metas de SLA para evaluar la capacidad	SLA	Relaciona servicios con los niveles de servicio definidos y utiliza los objetivos establecidos como referencia para el seguimiento de indicadores de capacidad y desempeño.
Apoyar la gestión de riesgos relacionados con capacidad	CMDB, Reportería	Registra información de criticidad, impacto, servicios, CI, tendencias y condiciones de capacidad para apoyar la identificación de riesgos, con el modelo de valoración configurado según la metodología del cliente.

Ciberseguridad de la plataforma

ASMS cumple los requisitos de ciberseguridad mediante los controles de arquitectura del servicio SaaS y su modelo de responsabilidad compartida, complementando la gestión funcional de Disponibilidad y Capacidad descrita anteriormente.

Requisito	Cómo lo soporta la plataforma
Arquitectura de conectividad para descubrimiento de CI (CI discovery)	El descubrimiento de infraestructura interna se realiza mediante un recolector on-premise, con comunicación exclusivamente saliente hacia los dominios del fabricante mediante lista de permitidos y cifrado TLS vigente; no se permite la conexión directa de servidores o dispositivos a la aplicación SaaS.
Recolectores separados por ambiente o zona	La arquitectura admite componentes de descubrimiento distribuidos conforme a la segmentación y zonas definidas por el cliente, evitando el tránsito entre zonas no autorizadas.
Control de alcance y ventanas de ejecución del recolector	El alcance y la programación de las actividades de descubrimiento se configuran mediante listas de permitidos por rangos u hosts y ventanas de ejecución, evitando el escaneo indiscriminado de red.
Registro en auditoría de las actividades de descubrimiento	La plataforma registra las actividades de descubrimiento, incluyendo el nivel de detalle sobre destino, técnica, resultado y fecha/hora requerido.
Mapa técnico de discovery y limitación de servicios/puertos	Como parte de la implementación se entregan los requerimientos técnicos de conectividad, incluyendo puertos, protocolos y mecanismos necesarios, permitiendo limitar los servicios estrictamente necesarios.
Prohibición de almacenar credenciales del cliente en la nube del proveedor	El manejo de credenciales de descubrimiento se define conforme a la arquitectura aprobada, con integración a bóveda o PAM institucional u otros controles equivalentes.

Requisito	Cómo lo soporta la plataforma
Agentes firmados, con hardening y sin capacidades tipo RMM	Los agentes se implementan con firma digital, hardening, control de versiones y despliegue controlado, operando como sensores de inventario y telemetría, sin habilitar shell remoto, transferencia de archivos ni control remoto salvo requerimiento y gobierno explícitos.
Restricción de SNMP v1/v2c	El uso de SNMP se limita a SNMPv3, conforme a los requisitos de seguridad definidos por el cliente.
Restricción de WinRM	La arquitectura de descubrimiento puede definirse evitando el uso de WinRM, sujeta a los mecanismos alternativos soportados por los componentes en alcance.
Autenticación mediante llaves en accesos Linux/Unix	Los mecanismos de acceso a sistemas Linux/Unix admiten esquemas de autenticación mediante llaves, conforme a las políticas del cliente.
Restricción del escaneo general de red (ICMP/port scanning)	Los procesos de descubrimiento se configuran conforme a los rangos y activos expresamente autorizados, evitando actividades de descubrimiento indiscriminadas.
Restricción de credenciales de administrador de dominio	La operación de descubrimiento no requiere cuentas de administrador de dominio como principio general; las credenciales y privilegios se dimensionan aplicando mínimo privilegio.
Compatibilidad con EDR (Microsoft Defender for Endpoint)	Se entregan lineamientos de coexistencia y exclusiones mínimas justificadas frente a soluciones EDR ya desplegadas por el cliente.
Continuidad y recuperación (BCP/DR)	La arquitectura SaaS contempla mecanismos de continuidad y recuperación, con valores de RTO/RPO y evidencia de pruebas conforme a los compromisos del servicio contratado.
Respaldo y recuperación de información	El servicio contempla respaldos regulares de información, software e infraestructura crítica, con procedimientos documentados y probados.
Inmutabilidad de respaldos para información crítica	Para información de mayor criticidad se implementan controles de inmutabilidad en los respaldos.
Protección contra ransomware	Incluye aislamiento lógico del tenant, segmentación entre producción, administración, respaldos y DR, respaldos inmutables cifrados con retención definida, y pruebas periódicas de recuperación con RPO/RTO documentados.
Gestión de vulnerabilidades y pruebas de seguridad	La solución puede someterse a análisis de vulnerabilidades y pruebas de penetración conforme a los procedimientos y condiciones acordados con el cliente.
Auditorías de ciberseguridad	Se proporcionan las evidencias de seguridad y cumplimiento disponibles y se atienden los procesos de auditoría conforme a las condiciones contractuales y de confidencialidad aplicables.
Eliminación y borrado seguro al finalizar el contrato	Los procedimientos de retención y eliminación de información se ejecutan conforme a un estándar de sanitización equivalente a NIST SP 800-88 o ISO aplicable, con certificación del proceso de eliminación.
Eliminación autorizada de bases de datos e información	La eliminación de información se gestiona mediante procedimientos formales y autorizaciones establecidas durante la operación y finalización del servicio.

Requisito	Cómo lo soporta la plataforma
Aislamiento y segregación de tenants en SaaS	La plataforma implementa segregación lógica que mantiene el aislamiento de la información entre los distintos clientes del servicio.

⚠ **Advertencia:** los valores concretos de RTO/RPO, los resultados de pruebas de vulnerabilidad y las certificaciones de borrado son evidencias operativas del servicio contratado, no funcionalidades del producto; deben solicitarse como anexos independientes y no incluirse como texto fijo en este manual para evitar que queden desactualizados.