SMARTGROUP

Departamento de Soporte Técnico

Guía de Herramientas y Accesos del Departamento

VoIP · Redes · Sistemas · IT

Índice

1. Introducción y Propósito

1.1 Propósito del documento

Este documento detalla las herramientas, plataformas y accesos que utiliza el Departamento de Soporte Técnico de Smartgroup en su operativa diaria. Su objetivo es servir como referencia rápida para que cada miembro del equipo conozca dónde acceder, cómo utilizar y qué buenas prácticas seguir con cada herramienta.

1.2 Alcance

Aplica a todo el equipo de Soporte Técnico (3 personas) y cubre todas las herramientas utilizadas en la gestión de incidencias, administración de centralitas, diagnóstico de conectividad, acceso remoto, gestión documental y seguridad de credenciales.

1.3 Clasificación de herramientas

Las herramientas se organizan en las siguientes categorías:

Categoría	Herramientas
Gestión de Incidencias	JDS (CRM propio)
Repositorio y Documentación	BookStack, MEGA
Gestión de Contraseñas	Passbolt
Administración de Centralitas	PekePBX, MeetIP, Yeastar, Issabel, FreePBX
Diagnóstico de Conectividad	Repositorio de Fibras, Portal Movistar, Teki (LCR)
Acceso Remoto	AnyDesk, TeamViewer
Herramientas de Diagnóstico	Wireshark, Winbox, PuTTY, navegadores

2. Sistema de Gestión de Incidencias – JDS

2.1 Descripción general

JDS es el CRM propio de Smartgroup utilizado para el registro, seguimiento y resolución de todas las incidencias del departamento. Es la herramienta central de la operativa diaria y todo ticket debe quedar registrado aquí.

2.2 Datos de acceso

Parámetro	Detalle
URL de acceso	http://192.168.172.102/PrinMailMail.jsp
Autenticación	Usuario y contraseña personal (almacenada en Passbolt)
Perfil	ALPHA (Soporte Técnico)
Red	Acceso exclusivo desde la red interna de Smartgroup

2.3 Funcionalidades principales

- **Consulta de correo:** Acceder a la sección «Consultar correo» para convertir emails entrantes en tickets.
- **Creación de tickets:** Asignar cliente, seleccionar tema (Información, Gestión BO, Incidencias, Oficina Técnica), tipo y prioridad.
- **Seguimiento interno:** Registrar cada acción con fecha en el campo de seguimiento.
- **Escalado:** Opciones de escalado a Operador, Gestor, BO o Cliente según corresponda.
- **Cierre:** Documentar solución y confirmar con el cliente antes de cerrar.

2.4 Buenas prácticas

- Verificar siempre que el cliente esté en el perfil ALPHA antes de crear un ticket.
- Documentar cada acción en el campo «Seguimiento interno» con fecha y hora.
- No cerrar nunca un ticket sin completar el campo «Solución».
- Utilizar las plantillas de correo predeterminadas para comunicaciones con clientes y operadores.

> **CRÍTICO:** Nunca cerrar un ticket sin haber completado el campo Solución y actualizado el Seguimiento Interno.

3. Repositorio de Documentación e Información

3.1 BookStack

BookStack es la plataforma principal de gestión del conocimiento del equipo. Aquí se almacena toda la información técnica de los clientes, runbooks, configuraciones, guías de diagnóstico y documentación interna.

Parámetro	Detalle
URL de acceso	https://bookstack.api2smart.com/
Autenticación	Usuario y contraseña (almacenada en Passbolt)
Contenido	Documentación de clientes, configuraciones, runbooks, guías

Contenido típico almacenado en BookStack

- Fichas técnicas de clientes: configuración de red, centralita, IPs, VLANs, credenciales de equipos.
- Runbooks y checklists de diagnóstico para incidencias recurrentes.
- Guías de configuración de equipos y servicios.
- Documentación de proyectos e instalaciones.
- Procedimientos operativos y protocolos del equipo.

> **CONSEJO:** Antes de escalar una incidencia, consulta siempre BookStack para verificar si existe documentación específica del cliente o de la incidencia.

3.2 MEGA

MEGA se utiliza como almacenamiento complementario en la nube para archivos de mayor tamaño, backups de configuraciones, capturas PCAP, imágenes de instalaciones y otros recursos que requieren espacio adicional.

Buenas prácticas de almacenamiento

- Mantener una estructura de carpetas organizada por cliente y tipo de documento.
- Nombrar los archivos de forma descriptiva incluyendo fecha y cliente.
- No almacenar contraseñas en archivos de texto dentro de MEGA; usar siempre Passbolt.
- Sincronizar periódicamente la información crítica entre BookStack y MEGA.

4. Gestor de Contraseñas – Passbolt

4.1 Descripción general

Passbolt es el gestor de contraseñas corporativo implementado en Smartgroup. Centraliza todas las credenciales de acceso a sistemas, equipos de clientes, portales de operadores y herramientas internas, garantizando la seguridad y trazabilidad de los accesos.

4.2 Datos de acceso

Parámetro	Detalle
URL de acceso	https://passbolt.api2smart.com/app/passwords
Autenticación	Cuenta personal con extensión del navegador
Tipo	Gestor de contraseñas open-source autohospedado

4.3 Políticas de uso obligatorio

1. Todas las contraseñas de acceso a equipos, portales y herramientas deben almacenarse en Passbolt.
2. Nunca almacenar credenciales en archivos de texto, hojas de cálculo o notas adhesivas.
3. Cuando se cree un nuevo acceso o se modifique una contraseña, actualizar Passbolt inmediatamente.
4. Organizar las contraseñas por carpetas: Clientes, Operadores, Herramientas Internas, Infraestructura.
5. Compartir credenciales con otros miembros del equipo exclusivamente a través de Passbolt.

4.4 Seguridad

- Utilizar la extensión del navegador de Passbolt para autocompletar credenciales de forma segura.
- No copiar contraseñas en el portapapeles durante más tiempo del necesario.
- Reportar inmediatamente cualquier sospecha de acceso no autorizado.

> **IMPORTANTE:** Passbolt es la única vía autorizada para almacenar y compartir credenciales. Queda prohibido el uso de cualquier otro método.

5. Administración de Centralitas

5.1 Descripción general

Para la gestión de incidencias relacionadas con la centralita telefónica del cliente, el equipo debe acceder al panel de administración de la centralita correspondiente. Smartgroup trabaja con múltiples plataformas de centralita según el cliente.

5.2 Plataformas de centralita soportadas

Plataforma	Tipo	Casos de uso típicos
PekePBX	Centralita virtual cloud	Clientes con PBX alojada en la nube de Smartgroup
MeetIP	Centralita virtual	Clientes con soluciones de comunicaciones unificadas
Yeastar	Centralita física/virtual	Clientes con PBX Yeastar (Serie S/P/Cloud)
Issabel	Centralita open-source	Clientes con PBX basada en Asterisk/Issabel
FreePBX	Centralita open-source	Clientes con PBX basada en FreePBX/Asterisk

5.3 Procedimiento general de acceso

1. Identificar la centralita del cliente consultando BookStack o el ticket en JDS.
2. Obtener las credenciales de acceso desde Passbolt (buscar por nombre del cliente o centralita).
3. Acceder al panel de administración vía web utilizando la IP o dominio correspondiente.
4. Realizar el diagnóstico o la configuración requerida.
5. Documentar todos los cambios realizados en el ticket de JDS.

5.4 Buenas prácticas

- Verificar siempre la versión del firmware antes de realizar cambios.
- Realizar capturas de pantalla de la configuración antes y después de cualquier modificación.
- En caso de cambios críticos, documentar un plan de rollback antes de ejecutar.
- Para incidencias de audio (one-way, cortes, eco), capturar PCAP con Wireshark.

> **IMPORTANTE:** Antes de modificar cualquier configuración en producción, asegurarse de tener documentado el estado anterior y un plan de retroceso.

6. Diagnóstico de Conectividad y Fibra

6.1 Descripción general

Cuando un cliente reporta problemas de conectividad (caída de router, ONT, fibra o servicio degradado), el equipo debe seguir un procedimiento específico según el operador de fibra contratado.

6.2 Paso 1 – Localización de la fibra

1. Solicitar al cliente la dirección exacta de la sede afectada.
2. Acceder al repositorio interno de fibras para localizar el servicio.

Parámetro	Detalle
URL del repositorio	http://192.168.172.201:8000/
Contenido	Registro completo de todas las fibras gestionadas por Smartgroup
Red	Acceso exclusivo desde red interna

3. Identificar el operador de fibra (Movistar, LCR u otro) y el número de servicio.

6.3 Paso 2A – Fibra Movistar

Si la fibra es de Movistar, seguir este procedimiento:

1. Acceder al portal de Movistar:

URL: https://paut.telefonica.es/mi-area

Iniciar sesión con el correo y contraseña indicados en Passbolt.

2. Verificar si hay acceso al router del cliente.
3. Si no hay acceso al router, contactar con Movistar:

Parámetro	Detalle
Teléfono	1489
Dato necesario	Número de fibra del servicio afectado
Requisito	Proporcionar número de contacto (Movistar lo solicita para comprobaciones)

4. Abrir la incidencia con Movistar proporcionando el número de fibra y un teléfono de contacto.
5. Registrar el número de incidencia de Movistar en el ticket de JDS.

> **IMPORTANTE:** Movistar siempre solicita un número de contacto para realizar comprobaciones. Facilitar un número operativo del cliente o de Smartgroup.

6.4 Paso 2B – Fibra LCR

Si la fibra es de LCR, seguir este procedimiento:

1. Intentar acceder al router por la IP pública del cliente utilizando Winbox.
2. Si no hay acceso al router, seguir con el proceso de diagnóstico en Teki:

Parámetro	Detalle
URL de acceso	https://www.teki.es/proc/servicio_tecnico/busc
Autenticación	Usuario y contraseña de Smartgroup (almacenada en Passbolt)
Función	Portal de gestión técnica del operador LCR

3. En Teki, navegar a Gestión de servicios → Informe de conectividades.
4. Ejecutar una telediagnosis de la fibra afectada.
5. Si la fibra no sincroniza, abrir avería en Teki:

Ir a Área Técnica → Abrir Ticket y rellenar los datos necesarios del servicio.

6. Registrar el número de ticket de LCR en el seguimiento del ticket de JDS.

> **CRÍTICO:** Las averías con LCR deben reiterarse cada hora hasta su resolución. Si no se reitera, la avería puede perder prioridad.

6.5 Diagrama de decisión rápido

Paso	Acción	Si OK	Si FALLA
1	Localizar fibra en repositorio	Identificar operador	Solicitar datos al cliente
2	Acceder al router	Diagnosticar en equipo	Ir a Paso 3
3a	Portal Movistar	Gestionar desde portal	Llamar al 1489
3b	Winbox (LCR)	Diagnosticar por Winbox	Ir a Teki
4	Telediagnosis (Teki)	Monitorizar recuperación	Abrir avería en Teki
5	Seguimiento	Reiterar cada hora	Escalar internamente

7. Herramientas de Acceso Remoto

7.1 Descripción general

El acceso remoto es esencial para resolver incidencias en los equipos de los clientes sin necesidad de desplazamiento físico. Smartgroup utiliza dos herramientas complementarias para garantizar la cobertura en cualquier escenario.

7.2 Herramientas disponibles

Herramienta	Uso principal	Características
AnyDesk	Herramienta principal de acceso remoto	Ligera, rápida, ideal para soporte inmediato
TeamViewer	Herramienta alternativa / secundaria	Compatible con más plataformas, acceso desatendido

7.3 Procedimiento de conexión remota

1. Informar al cliente de que se va a realizar una conexión remota a su equipo.
2. Solicitar al cliente que abra la aplicación de AnyDesk (o TeamViewer si es necesario).
3. El cliente debe facilitar el ID de conexión y aceptar la solicitud de acceso.
4. Realizar las acciones técnicas necesarias para resolver la incidencia.
5. Informar al cliente de todas las acciones realizadas al finalizar.
6. Documentar la sesión remota en el ticket de JDS incluyendo: hora de conexión, acciones realizadas y resultado.

7.4 Buenas prácticas de acceso remoto

- Siempre solicitar permiso explícito del cliente antes de conectarse.
- No dejar sesiones remotas abiertas sin supervisión.
- Cerrar la sesión inmediatamente al finalizar las tareas.
- Si es necesario acceso desatendido (por ejemplo, para mantenimientos programados), configurarlo previamente con autorización del cliente.
- Nunca instalar software sin autorización previa del cliente.

> **IMPORTANTE:** Toda sesión remota debe quedar registrada en el ticket de JDS con detalle de las acciones realizadas.

8. Herramientas Complementarias de Diagnóstico

8.1 Wireshark

Herramienta de análisis de protocolos de red utilizada para capturar y analizar tráfico. Esencial para incidencias VoIP (análisis SIP/RTP) y problemas de red.

- Uso principal: capturas PCAP para incidencias de VoIP, red y diagnóstico avanzado.
- Filtros clave: sip, rtp, ip.addr==X.X.X.X, tcp.port==XXXX.
- Las capturas PCAP deben adjuntarse como evidencia en los tickets de JDS.

8.2 Winbox

Herramienta de administración para equipos MikroTik (routers y switches). Permite acceso por IP o MAC address para configuración y diagnóstico de equipos de red.

- Uso principal: acceso a routers MikroTik de clientes para diagnóstico y configuración.
- Permite acceso por capa 2 (MAC) cuando no hay conectividad IP.
- Credenciales de acceso almacenadas en Passbolt.

8.3 PuTTY / Terminal SSH

Cliente SSH utilizado para acceder a equipos Linux, centralitas basadas en Asterisk/Issabel/FreePBX y otros dispositivos que requieran acceso por línea de comandos.

- Uso principal: administración de servidores, centralitas y equipos vía SSH.
- Guardar sesiones frecuentes para agilizar el acceso.
- Registrar todos los comandos ejecutados relevantes en el ticket de JDS.

8.4 Navegadores Web

Los navegadores se utilizan para acceder a los paneles de administración de centralitas, portales de operadores (Movistar, Teki), BookStack, JDS y Passbolt. Se recomienda utilizar perfiles dedicados con las extensiones necesarias (Passbolt, etc.).

9. Resumen de Accesos y URLs

Tabla resumen con todos los accesos del departamento para referencia rápida:

Herramienta	URL / Acceso	Credenciales
JDS (CRM)	http://192.168.172.102/PrinMailMail.jsp	Passbolt
BookStack	https://bookstack.api2smart.com/	Passbolt
MEGA	Aplicación de escritorio / web	Passbolt
Passbolt	https://passbolt.api2smart.com/app/passwords	Cuenta personal
Repositorio Fibras	http://192.168.172.201:8000/	Red interna
Portal Movistar	https://paut.telefonica.es/mi-area	Passbolt
Teki (LCR)	https://www.teki.es/proc/servicio_tecnico/busc	Passbolt
Centralitas	Según cliente (consultar BookStack)	Passbolt
AnyDesk	Aplicación de escritorio	ID por sesión
TeamViewer	Aplicación de escritorio	ID por sesión

10. Políticas de Seguridad y Cumplimiento

10.1 Gestión de credenciales

- Todas las credenciales se almacenan exclusivamente en Passbolt.
- Las contraseñas deben ser robustas (mínimo 12 caracteres, combinación de mayúsculas, minúsculas, números y símbolos).
- Rotación de contraseñas críticas cada 90 días.
- Nunca reutilizar contraseñas entre diferentes servicios o clientes.

10.2 Acceso a sistemas

- Acceder siempre a través de conexiones seguras (VPN cuando sea necesario).
- No compartir sesiones activas ni dejar equipos desbloqueados sin supervisión.
- Reportar inmediatamente cualquier brecha de seguridad o acceso sospechoso.

10.3 Documentación de cambios

- Todo cambio en sistemas de producción debe quedar documentado en JDS.
- Mantener un registro de antes/después en cada modificación de configuración.
- Las evidencias (capturas, logs, PCAP) deben archivarse junto al ticket correspondiente.