	INFORME MENSUAL	

INFORME MENSUAL **Núm.:**

LUGAR: SUPERINTENDENCIA DE NOTARIADO Y REGISTRO	**FECHA:** 24/11/2025

PROYECTO:	ADQUISICIÓN Y/O RENOVACIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA SNR, INCLUYENDO SOLUCIONES DE RED, CONECTIVIDAD INALÁMBRICA, SEGURIDAD PERIMETRAL, CONTROL DE ACCESO, ALMACENAMIENTO Y PLATAFORMAS TECNOLÓGICAS ASOCIADAS, ASÍ COMO EL SUMINISTRO DE LICENCIAMIENTO, SOPORTE Y GARANTIAS. **LOTE 4:** Renovación y adquisición de una suite de herramientas para la administración y seguridad de los diferentes sistemas funcionales de la Superintendencia de Notariado y Registro.
CONTRATO	2554 DE 2025

EMPRESA PROVEEDORA:	MSL DISTRIBUCIONES Y CIA SAS
EMPRESA CONTRATANTE:	SUPERINTENDENCIA DE NOTARIADO Y REGISTRO
TIPO DE LICENCIAMIENTO:	Suscripción
HORAS IMPLEMENTACIÓN:	La entidad adquirió 4000 horas para soporte, configuraciones o lo que requiera la entidad de las soluciones de Broadcom

CONTACTO TECNICO:	Oscar Corredor
TELEFONO:	3012346379
CELULAR:	3012346379
MAIL:	oscar.corredor@supernotariado.gov.co

INFORMACIÓN ADICIONAL	
Fecha Inicio del Proyecto	2025/09/17
Fecha Fin del proyecto	2025/12/15
Fecha de Contrato	2025/09/10

OBJETIVO:
Se presenta informe con la relación de las horas ejecutadas en actividades programadas y autorizadas por parte de SNR:

ITEM	Solución	Horas Priorizadas Contrato No. 2554 de 2025
1	PAM	69
2	IGA	423
3	SSO	242
4	API	183
5	SDM	417
6	SDM / CHATBOT LIA FASE 2	0
7	ITCA	112
8	IM	327
9	APM	168
10	PPM / CLARITY / SUPRA	539
11	SOPORTE	700
12	CAPACITACIONES ADM	90
13	ASSESSMENT	90
14	Integración de CHATBOT LIA FASE 1	160
15	Despliegue e implementación de API Developer Portal	80
16	Interoperabilidad SNR – Catastro.	300
17	Facelogin SIR	100
TOTAL	**TOTAL**	**4000,00**

A continuación detallamos por solución las iniciativas o requerimientos gestionados, basados en las necesidades de las áreas y generando valor a la Entidad con:

1. **PAM. CA Privileged Access Manager:**

   Garantiza la seguridad de los sistemas al controlar y auditar el acceso de usuarios privilegiados a recursos sensibles.

Alcance:

De acuerdo con el objetivo de implementar Symantec PAM siguiendo las políticas de seguridad establecidas por la OTI, se ejecutan las actividades del plan de trabajo aprobado para dar continuidad en la mejora continua de la solución y aumentar el alcance de la solución en aspectos de gestión de usuarios, endpoints, credenciales y parametrizaciones de las funcionalidades ofrecidas. Cada una de estas actividades busca fortalecer las capacidades de seguridad que PAM ofrece frente a los usuarios y servidores sincronizados, así como brindar nuevas opciones para la realización de las tareas administrativas.

Como punto inicial, se actualiza el certificado dentro de PAM con uno propio suministrado por la SNR que asegura la correcta comunicación hacia los servidores sincronizados dentro de la solución y garantiza un inicio de sesión confiable a través del servicio que ya fue publicado en internet.

Frente a las actividades de gestión dentro de PAM, se han llevado a cabo múltiples sesiones en conjunto a los administradores de los aplicativos SISG y Oracle x10 con el fin de crear los servidores correspondientes para su acceso y la sincronización de las credenciales privilegiadas, aplicándoles de esta forma todas las capas de seguridad, control y auditoria que ofrece la solución. De igual forma se ha creado cada política de acceso para permitir que los usuarios realicen su ingreso centralizado únicamente a los ambientes requeridos según su rol de funcionario.

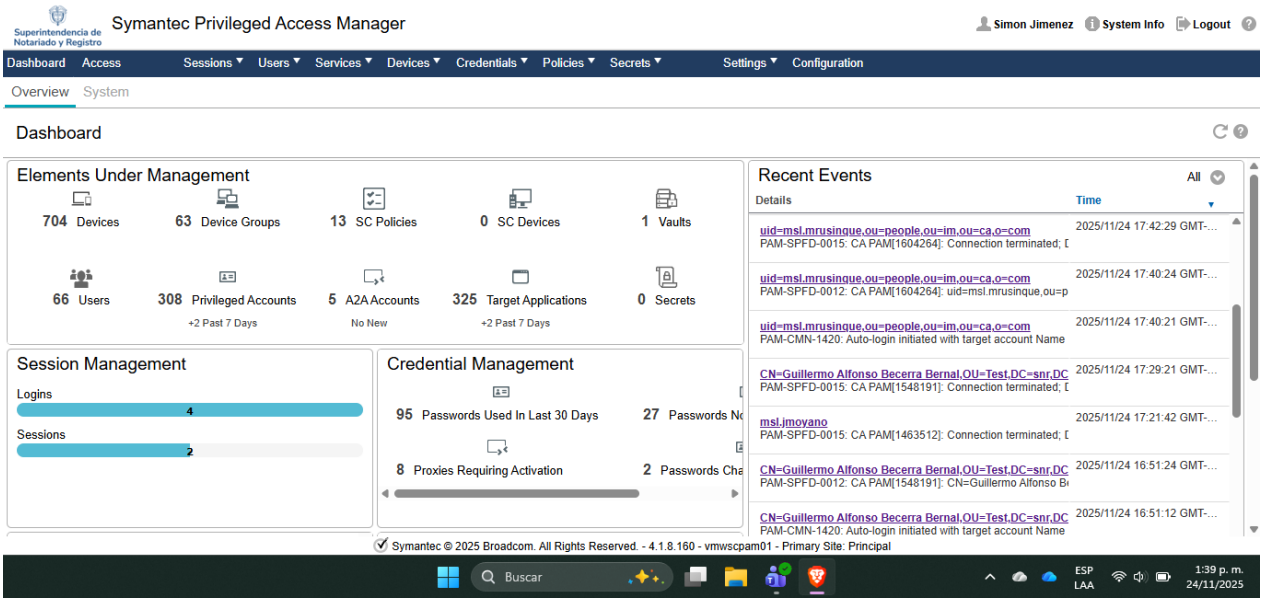
DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

Adicionalmente, se han actualizado las listas de filtrado de comandos que limitan las acciones dentro de las consolas Linux sincronizadas en la solución para evitar la ejecución de actividades consideradas riesgosas dentro del ambiente productivo de la entidad, se ha creado la bóveda de secretos interna de PAM la cual ofrece un almacenamiento seguro a toda la información crítica que deba ser resguardada ante posibles manipulaciones de terceros y se ha configurado en su totalidad la integración con la herramienta de virtualización VMware usada actualmente en la SNR para la creación de toda máquina virtual requerida para sus operaciones, con ella PAM adquiere la facultad de sincronizar automáticamente este ambiente virtual, lo que asegura la centralización de accesos para todos los usuarios administradores.

Las parametrizaciones se configuran correctamente en el ambiente productivo de Symantec PAM, asegurando su funcionamiento esperado de cara a los usuarios finales y a los administradores.

El inventario de servidores dentro de la solución ha presentado un aumento gracias a la migración de máquinas virtuales activada con la integración de VMware, las credenciales de los nuevos aplicativos sincronizados se han verificado exitosamente y se ha asegurado el acceso remoto desde el cliente de PAM, por lo que todos los usuarios pueden hacer uso sin inconvenientes de la solución con todas las características implementadas como la grabación de sesiones y la rotación de contraseñas.

A continuación se anexan evidencias de las funcionalidades de la solución:



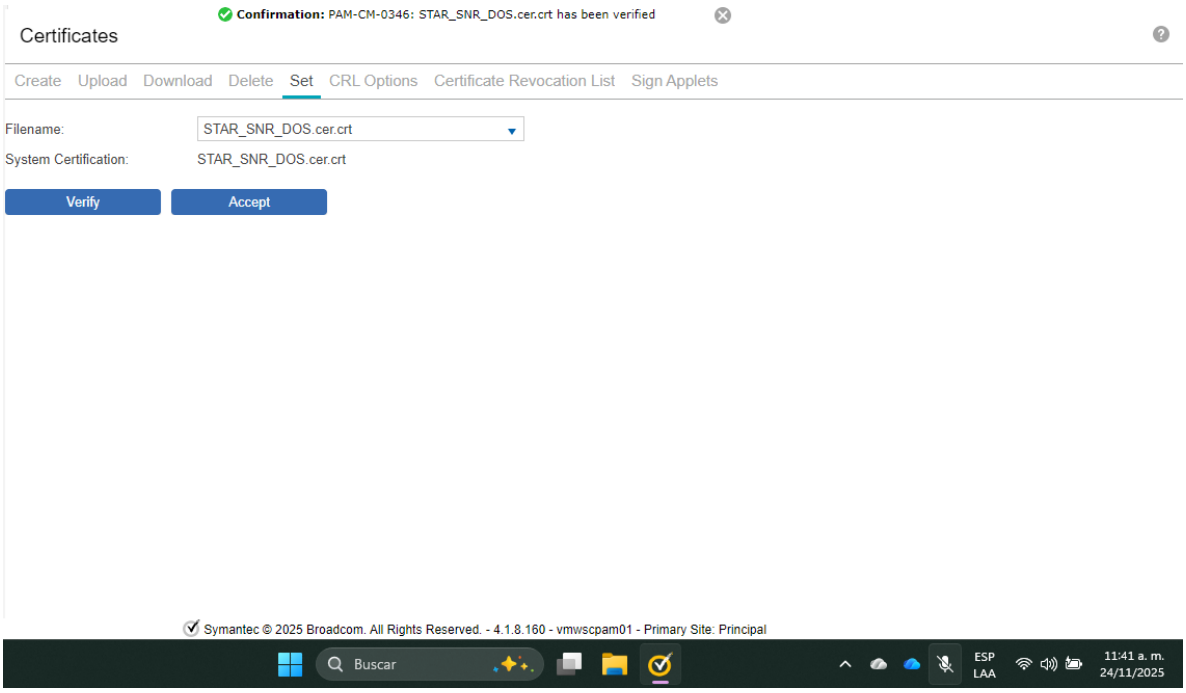
DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

Plan de trabajo:

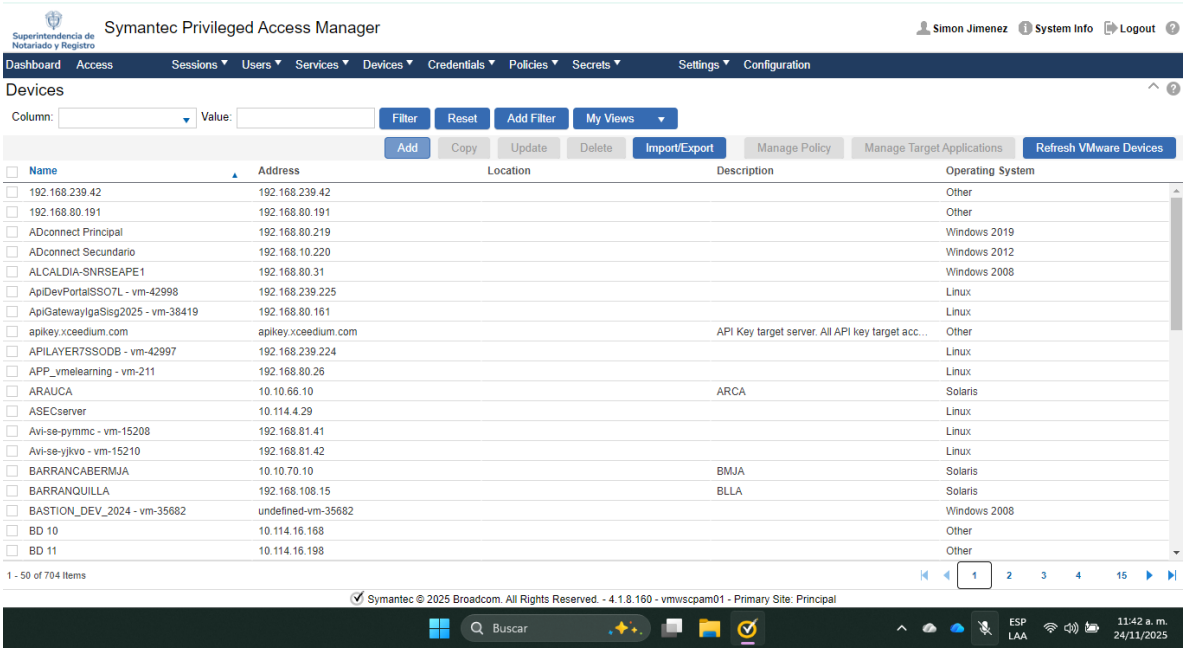
Item	Actividades	Total de horas / Tareas	69,0 / Vobo Priorización cliente
1	Prerrequisitos	Levantamiento de información con administradores de aplicativos nuevos a sincronizar dentro de PAM	1,0
2	Actualización de certificado	Configurar en modo mantenimiento los servidores	1,0
3		Detener clúster	1,0
4		Subir certificado en cada nodo de PAM	3,0
5		Aplicar Certificado y reiniciar cada nodo PAM en ambos site	6,0
6		Activar Clúster	1,0
7		Pruebas funcionales	1,0
8		Desactivar modo mantenimiento en los servidores	1,0
9	Descubrimiento automático de Servidores	Identificar los Segmentos de Red requeridos	1,0
10		Crear y ejecutar un Device Scan Profile	1,0
11		Exportar informe de los servidores descubiertos	1,0
12	Gestión de servidores	Sincronizar servidores de aplicativos misionales encontrados en el informe de descubrimiento	3,0
13		Crear servidores no presentes en el informe de descubrimiento	0,0
14		Crear Target Applications de servidores sincronizados	0,0
15	Gestión de cuentas privilegiadas	Crear Target Account con rol de administrador para cada servidor sincronizado	0,0
16		Verificar Target Account	0,0
17		Habilitar el escaneo de cuentas en cada Target Account	0,0
18	Descubrimiento Automático de Cuentas	Crear y ejecutar un Account Scan Profile	1,0
19		Exportar informe de las cuentas privilegiadas descubiertas	1,0
20	Creación de Politicas de acceso	Crear políticas de acceso	1,0
21	Rotación de contraseñas	Socialización con administradores de los aplicativos sobre la politica de rotación de contraseñas	1,0
22		Activar rotación de contraseñas en las cuentas privilegiadas designadas	0,0
23		Pruebas de acceso a través de PAM	1,0
24	Configuración de Jump Servers	Levantamiento de información para aplicaciones a incluir dentro del JumpServer	1,0
25		Habilitar herramienta de transparent Login dentro de cada Jump Server	3,0
26		Configurar accesos a portales web y/o aplicaciones dentro del Jump Server	3,0
27		Pruebas funcionales de acceso	1,0
28	Flujos de Aprobación	Crear flujos de aprobación de acuerdo a cada aplicativo sincronizado	1,0
29		Modificar estructura de correos de aprobación enviados por PAM	3,0
30	Instalación de agentes	Ejecutar instalador nativo según el Sistema Operativo	1,0
31		Activar servicio gksfd del agente	1,0
32		Configurar restricciones de accesos externos	1,0
33		Configurar en Pam la comunicación con el agente instalado	1,0
34	Actualización de Filtros	Definir listado de comandos a filtrar	1,0
35		Modificar Blacklist de comandos	1,0
36		Modificar Blacklist de bloqueo de saltos en los servidores	1,0
37	Integración Vmware	Crear Endpoint con IP de la consola VMware	0,0
38		Crear Target Account	0,0
39		Configurar la consola Vcenter dentro de PAM	1,0
40		Iniciar import de máquinas virtuales	1,0
41	Bóveda de secretos	Actualizar usuarios dentro del grupo de administración de secretos	1,0
42		Crear Vault de secretos	0,0
43	Documentación	Actualizar manuales de usuario y administrador	7,0
44		Actualizar documentación de memoria técnica y de diseño	7,0
45	WAF	migrar los servicios de la SNR al Waf suministrado por Radware para aumentar la seguridad	7,0

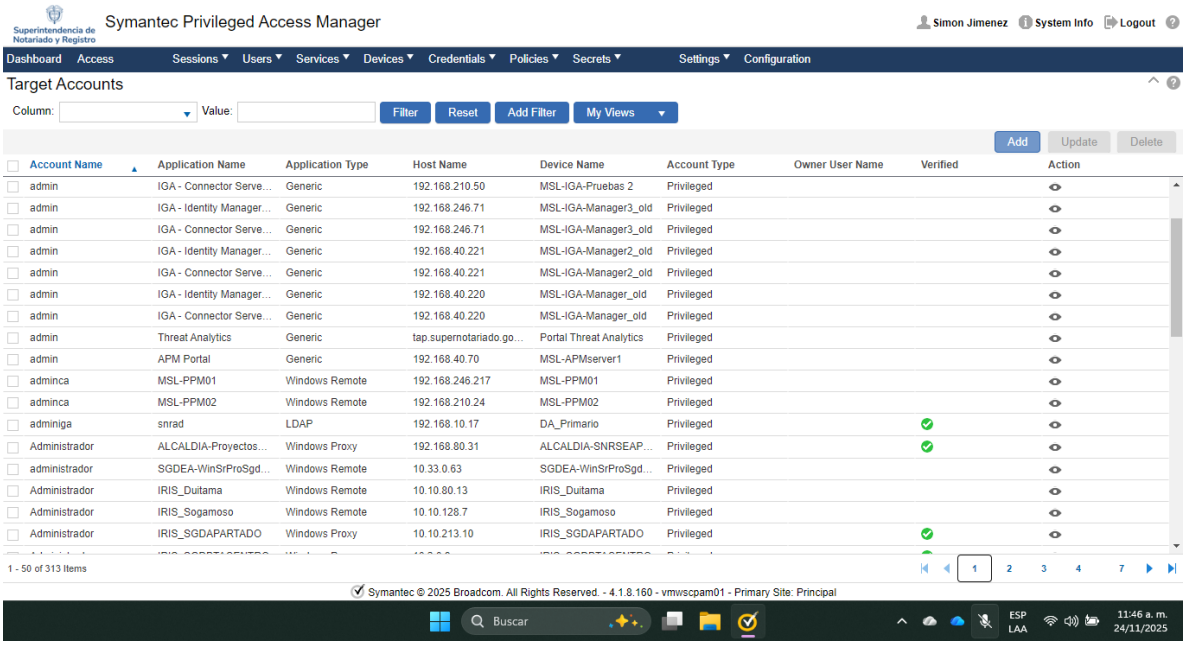
DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

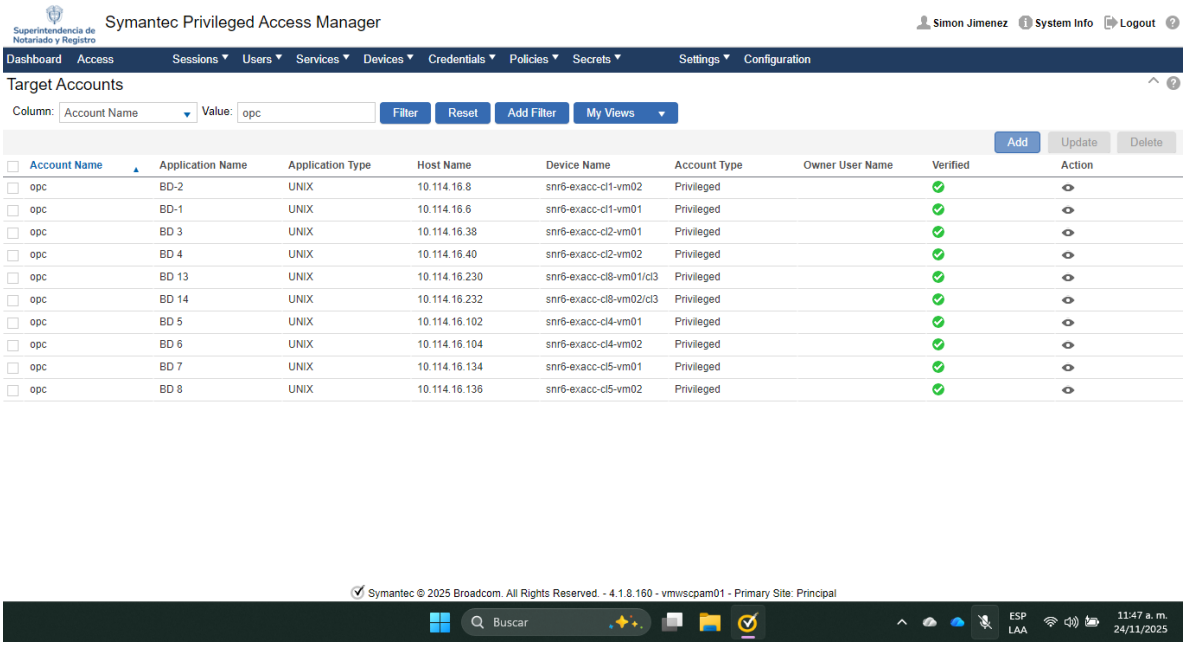
Actualización de certificado:



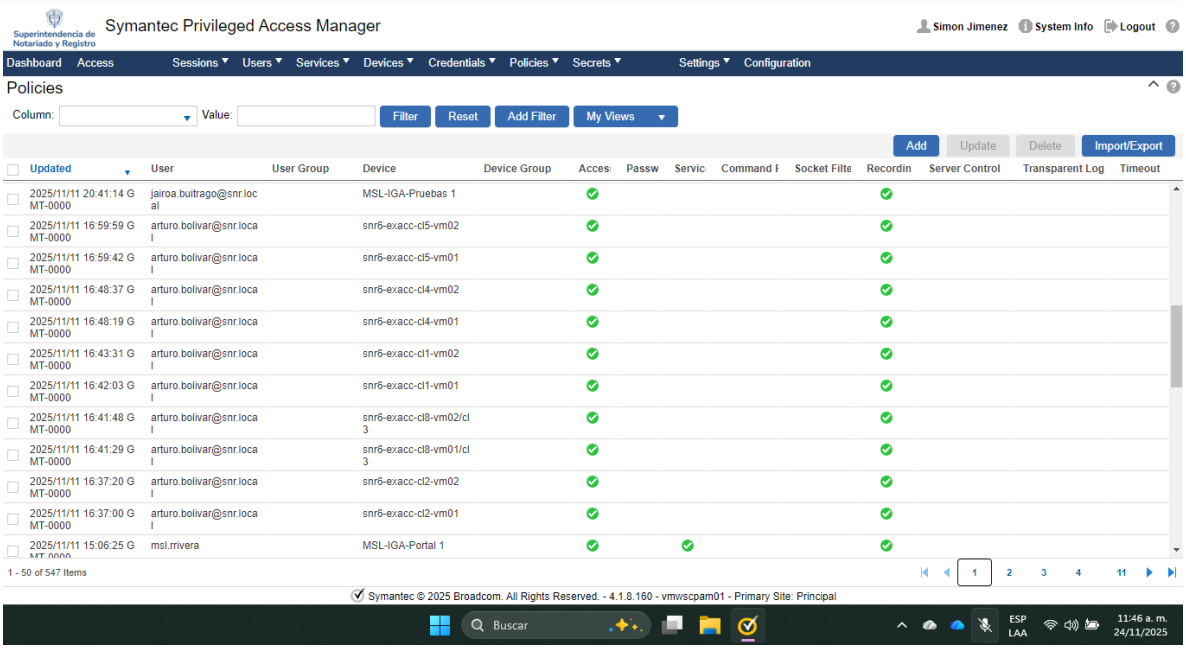
Gestión de servidores y credenciales:



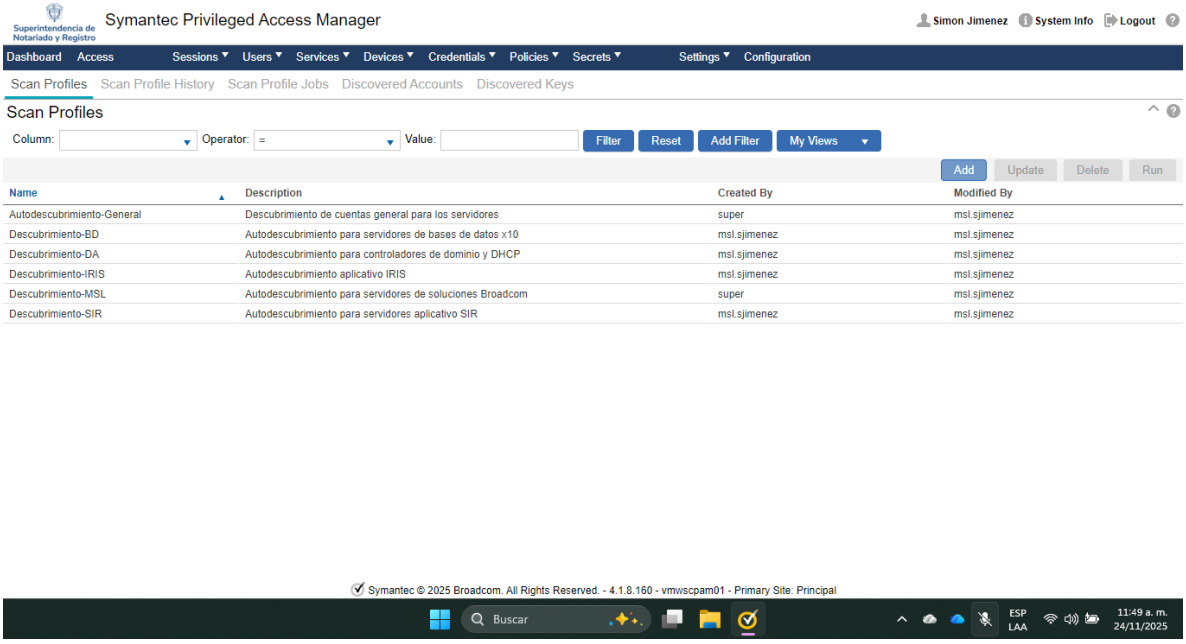

Superintendencia de Notariado y Registro
Symantec Privileged Access Manager
Simon Jimenez
System Info
Logout
Dashboard
Access
Sessions
Users
Services
Devices
Credentials
Policies
Secrets
Settings
Configuration
Target Accounts
Column:
Value:
Filter
Reset
Add Filter
My Views
Add
Update
Delete
Account Name
Application Name
Application Type
Host Name
Device Name
Account Type
Owner User Name
Verified
Action
admin IGA - Connector Serve... Generic 192.168.210.50 MSL-IGA-Pruebas 2 Privileged
admin IGA - Identity Manager... Generic 192.168.246.71 MSL-IGA-Manager3_old Privileged
admin IGA - Connector Serve... Generic 192.168.246.71 MSL-IGA-Manager3_old Privileged
admin IGA - Identity Manager... Generic 192.168.40.221 MSL-IGA-Manager2_old Privileged
admin IGA - Connector Serve... Generic 192.168.40.221 MSL-IGA-Manager2_old Privileged
admin IGA - Identity Manager... Generic 192.168.40.220 MSL-IGA-Manager_old Privileged
admin IGA - Connector Serve... Generic 192.168.40.220 MSL-IGA-Manager_old Privileged
admin Threat Analytics Generic tap.supernotariado.go... Portal Threat Analytics Privileged
admin APM Portal Generic 192.168.40.70 MSL-APMserver1 Privileged
adminca MSL-PPM01 Windows Remote 192.168.246.217 MSL-PPM01 Privileged
adminca MSL-PPM02 Windows Remote 192.168.210.24 MSL-PPM02 Privileged
adminiga snrad LDAP 192.168.10.17 DA_Primario Privileged
Administrador ALCALDIA-Proyectos... Windows Proxy 192.168.80.31 ALCALDIA-SNRSEAP... Privileged
administrador SGDEA-WinSrProSgd... Windows Remote 10.33.0.63 SGDEA-WinSrProSgd... Privileged
Administrador IRIS_Duitama Windows Remote 10.10.80.13 IRIS_Duitama Privileged
Administrador IRIS_Sogamoso Windows Remote 10.10.128.7 IRIS_Sogamoso Privileged
Administrador IRIS_SGDAPARTADO Windows Proxy 10.10.213.10 IRIS_SGDAPARTADO Privileged
1 - 50 of 313 Items
1 2 3 4 7
Symantec © 2025 Broadcom. All Rights Reserved. - 4.1.8.160 - vmwscpam01 - Primary Site: Principal
Buscar
ESP LAA
11:46 a. m. 24/11/2025


Superintendencia de Notariado y Registro
Symantec Privileged Access Manager
Simon Jimenez
System Info
Logout
Dashboard
Access
Sessions
Users
Services
Devices
Credentials
Policies
Secrets
Settings
Configuration
Target Accounts
Column: Account Name
Value: opc
Filter
Reset
Add Filter
My Views
Add
Update
Delete
Account Name
Application Name
Application Type
Host Name
Device Name
Account Type
Owner User Name
Verified
Action
opc BD-2 UNIX 10.114.16.8 snr6-exacc-cl1-vm02 Privileged
opc BD-1 UNIX 10.114.16.6 snr6-exacc-cl1-vm01 Privileged
opc BD 3 UNIX 10.114.16.38 snr6-exacc-cl2-vm01 Privileged
opc BD 4 UNIX 10.114.16.40 snr6-exacc-cl2-vm02 Privileged
opc BD 13 UNIX 10.114.16.230 snr6-exacc-cl8-vm01/cl3 Privileged
opc BD 14 UNIX 10.114.16.232 snr6-exacc-cl8-vm02/cl3 Privileged
opc BD 5 UNIX 10.114.16.102 snr6-exacc-cl4-vm01 Privileged
opc BD 6 UNIX 10.114.16.104 snr6-exacc-cl4-vm02 Privileged
opc BD 7 UNIX 10.114.16.134 snr6-exacc-cl5-vm01 Privileged
opc BD 8 UNIX 10.114.16.136 snr6-exacc-cl5-vm02 Privileged
Symantec © 2025 Broadcom. All Rights Reserved. - 4.1.8.160 - vmwscpam01 - Primary Site: Principal
Buscar
ESP LAA
11:47 a. m. 24/11/2025

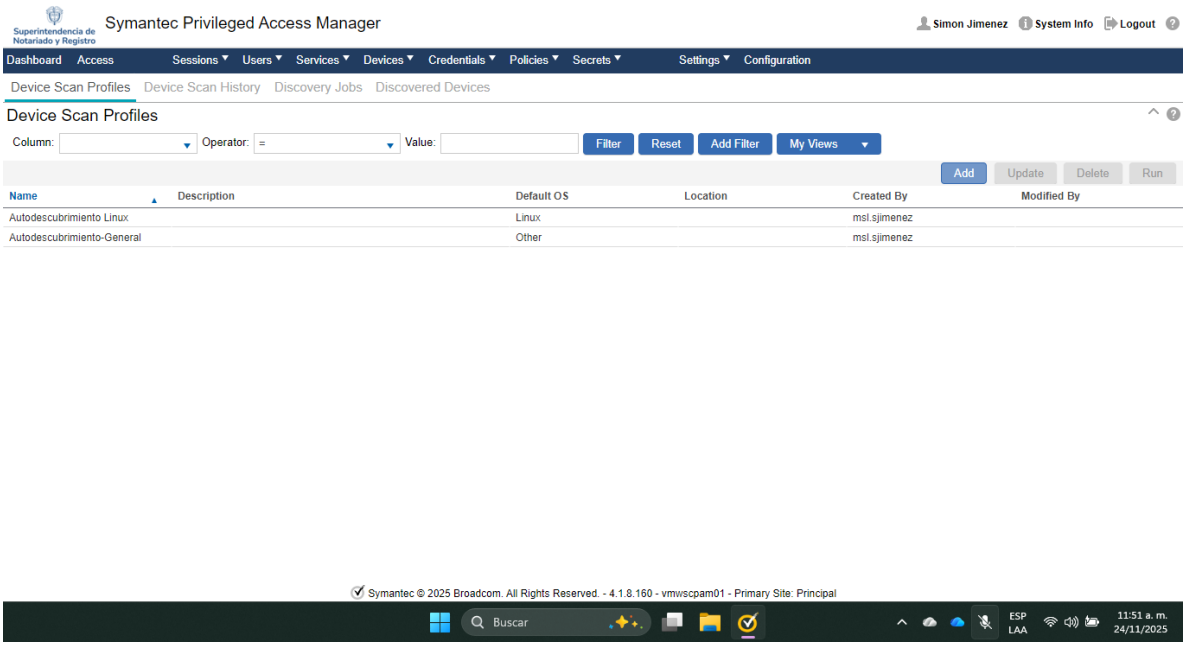
Creación de políticas de acceso:



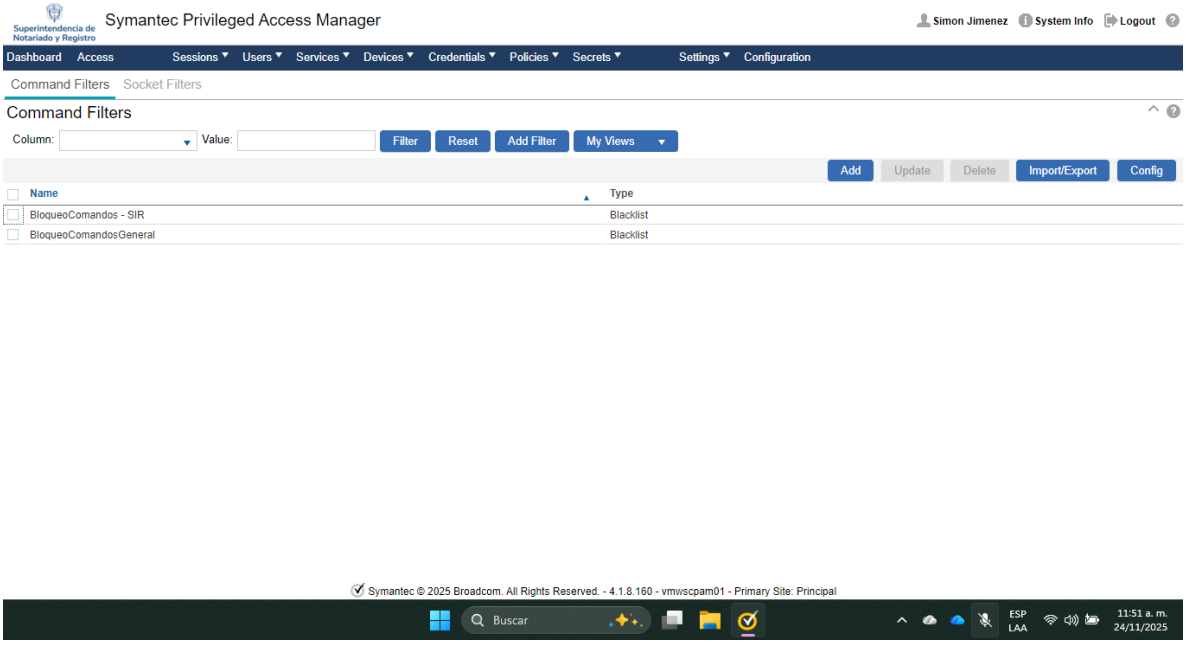
Descubrimientos Automáticos:

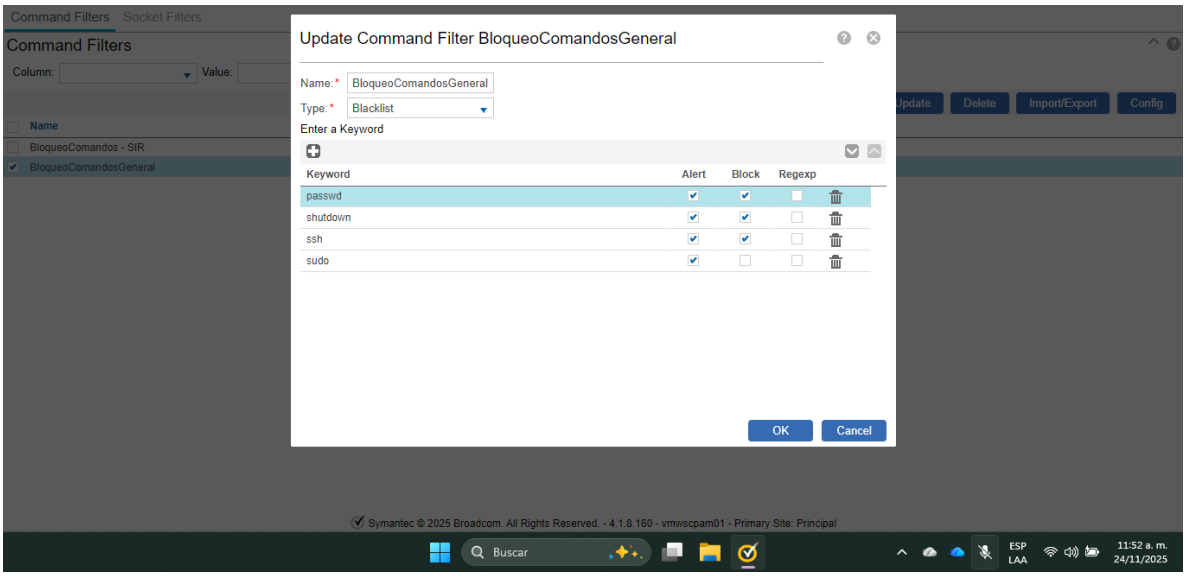


DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

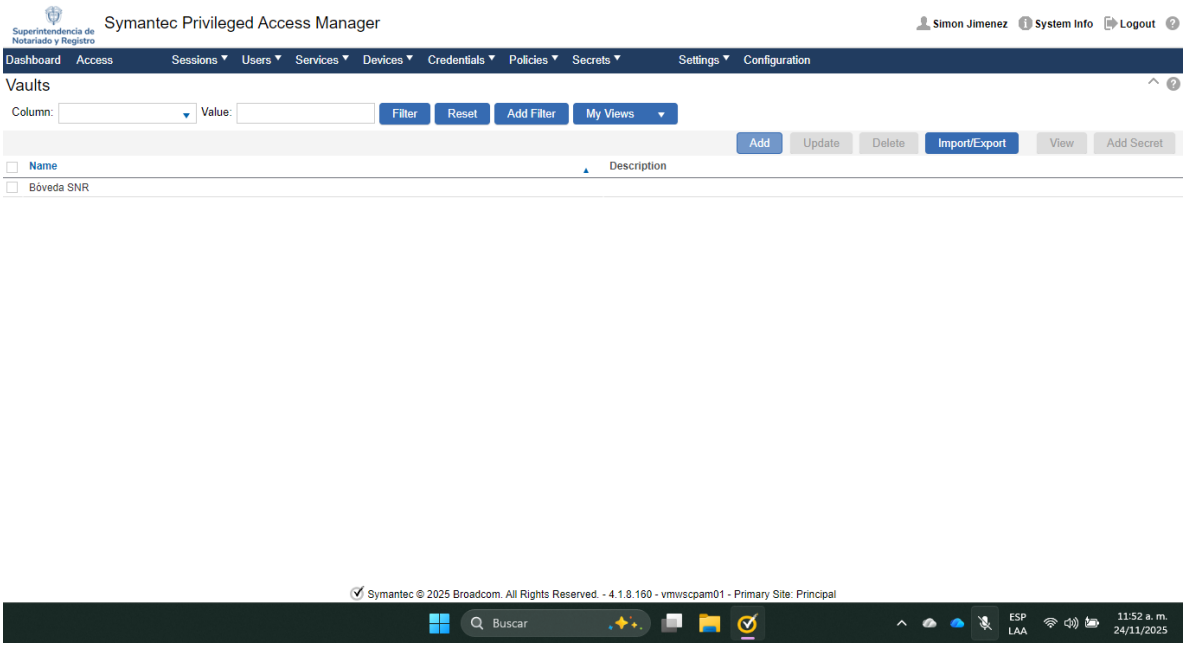


Actualización de filtros:

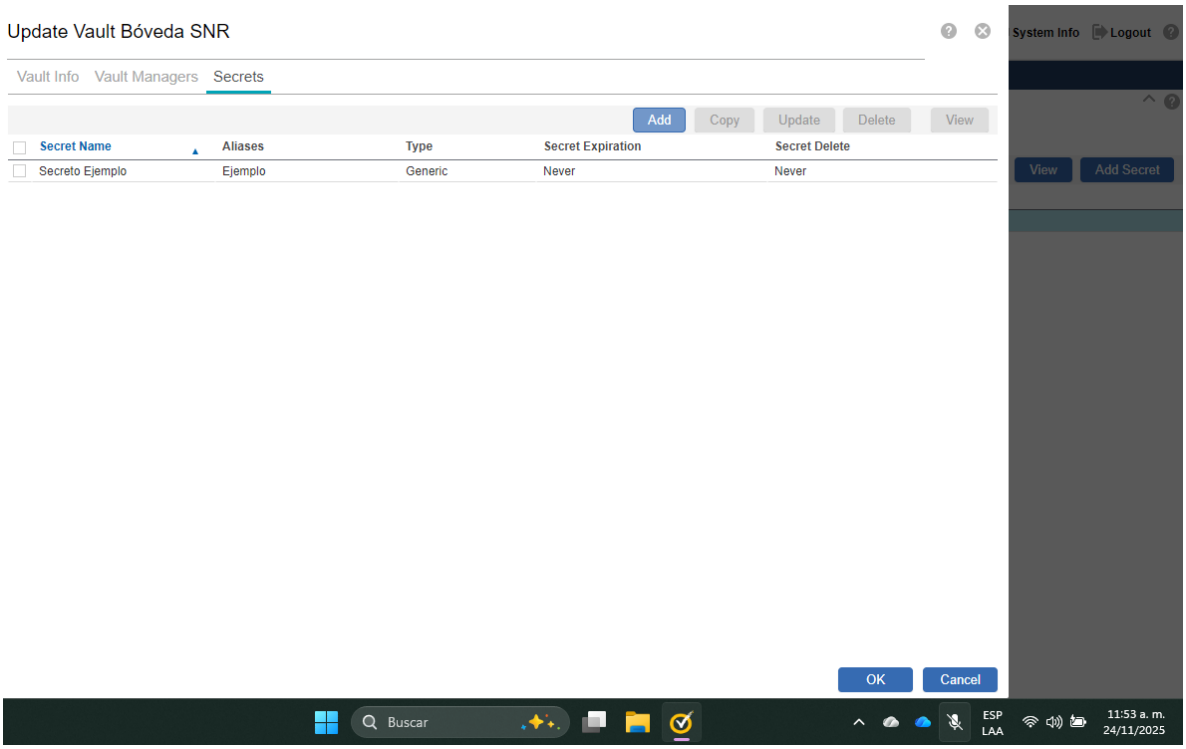




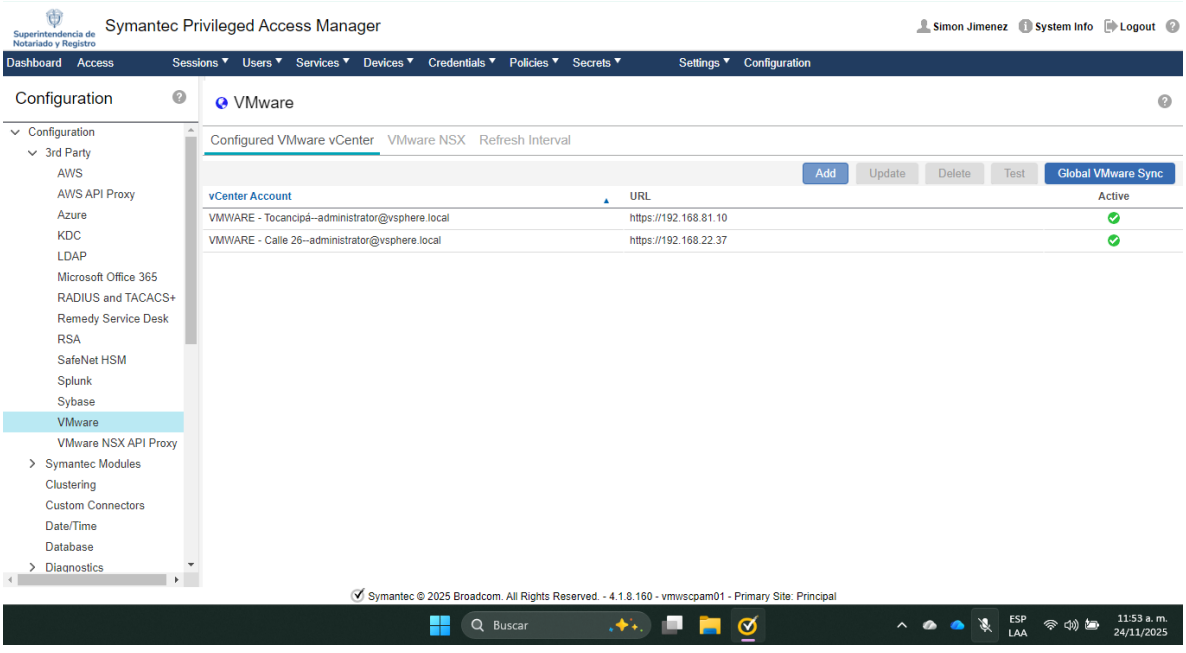
Bóveda de secretos:



DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.



Integración VMware:



2. IGA. CA Identity Governance & Administration (IGA).

Es una plataforma empresarial que permite a las organizaciones controlar, automatizar y auditar la gestión de identidades y accesos de los usuarios en todos sus sistemas y aplicaciones. Estas herramientas son fundamentales para la gestión de identidades y accesos, asegurando que solo los usuarios autorizados tengan acceso a los recursos adecuados**.**

Su objetivo principal es garantizar que la persona correcta tenga el acceso correcto, en el momento correcto y por el tiempo necesario, reduciendo riesgos de seguridad y costos operativos.

Plan de Trabajo:

Item	Actividad	Total de horas	423
		Tarea	Vobo Priorización
1	Creacion de formulario de validacion de estado de usuario Ambiente de Pruebas	Creacion documento de diseño	3,0
2		Creacion documento de plan de pruebas	3,0
3		Creacion de tarea para validacion estado e informacion de usuario	3,0
4		Creacion de formulario para validacion estado e informacion de usuario	2,0
5		Pruebas unitarias	3,0
6		Ajuste memoria técnica.	2,0
7		Sesion de transferencia de conocimiento.	2,0
8		Creacion manual de usuario	3,0
9		Creacion manual de administracion	3,0
10		Pruebas funcionales	2,0
11	Creacion de formulario de validacion de estado de usuario Ambiente de Produccion	Migracion de tarea para validacion estado e informacion de usuario	2,0
12		Migracion de formulario para validacion estado e informacion de usuario	2,0
13		Pruebas Unitarias	2,0
14		Pruebas funcionales	2,0
15	Analisis de riesgo en privilegios de usuario Ambiente de Pruebas	Levantamiento de información	3,0
16		Creacion documento de diseño	3,0
17		Creacion documento de plan de pruebas	3,0
18		Para obtener un nivel de riesgo el usuario debe adquirir el rol Administrativo o privilegiado en un aplicatiivo dentro de IGA	3,0
19		Configurar en Indentity Portal la visualización del nivel de riesgo del usuario	3,0
20		Configuración de nivel de riesgo por aplicativo	3,0
21		Pruebas unitarias	3,0
22		Ajuste memoria técnica.	2,0
23		Sesion de transferencia de conocimiento.	2,0
24		Creacion manual de usuario	3,0
25		Creacion manual de administracion	3,0
26		Pruebas funcionales	2,0
27	Analisis de riesgo en privilegios de usuario Ambiente de Produccion	Para obtener un nivel de riesgo el usuario debe adquirir el rol Administrativo o privilegiado en un aplicatiivo dentro de IGA	3,0
28		Configurar en Indentity Portal la visualización del nivel de riesgo del usuario	3,0
29		Configuración de nivel de riesgo por aplicativo	3,0
30		pruebas unitarias	2,0
31		Pruebas funcionales	2,0
32	Modulo de novedades de Usuarios IGA-DA ambiente de pruebas	Levantamiento de informacion Novedades de usuarios	3,0
33		Creacion documento de diseño	3,0
34		Creacion documento de plan de pruebas	3,0
35		Creacion de tarea de Registro de novedades de usuarios	1,0
36		Creacion de formulario de Registro de novedades de usuarios	0,0
37		Creacion de atributo para guardar fecha inicio y fecha fin de novedad de usuarios	0,0
38		Creacion Politica para inactivacion en inicio de novedad de usuarios	1,0
39		Creacion Politica para activacion en fin de novedad de usuarios	1,0
40		Pruebas unitarias	2,0
41		Ajuste memoria técnica.	2,0
42		Sesion de transferencia de conocimiento.	2,0
43		Creacion manual de usuario	2,0
44		Creacion manual de administracion	2,0
45		Pruebas funcionales	2,0

DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

46	Modulo de novedades de Usuarios IGA-DA ambiente de produccion	Migracion de tarea de Registro de novedades de usuarios	1,0
47		Migracion de formulario de Registro de novedades de usuarios	1,0
48		Migracion de atributo para guardar fecha inicio y fecha fin de novedad de usuarios	1,0
49		Migracion Politica para inactivacion en inicio de novedad de usuarios	2,0
50		Migracion Politica para activacion en fin de novedad de usuarios	3,0
51		Pruebas unitarias y funcionales	2,0
52	Modulo cambio de loginID en pruebas	Creacion documento de diseño	3,0
53		Creacion documento de plan de pruebas	3,0
54		Creacion de tarea de cambio de loginid	1,0
55		Creacion de formulario.	0,0
56		Creacion de atributo para guardar loginid disponibles	0,0
57		Creacion script para generar loginid disponibles según informicón del DA	5,0
58		Creacion de lista desplegable con loginid disponibles.	1,0
59		Generar servicio de contruccion de login id.	3,0
60		Generar script con los login id disponible en API	1,0
61		Crear java plugin para consulta en API	1,0
62		Pruebas unitarias	3,0
63		Ajuste memoria técnica.	2,0
64		Sesion de transferencia de conocimiento.	2,0
65		Creacion manual de usuario	2,0
66		Creacion manual de administracion	2,0
67		Pruebas funcionales	2,0
68	Modulo cambio de loginID en produccion	Migracion de tarea de cambio de loginid	1,0
69		Migrar formulario.	0,0
70		Migracion de atributo para guardar loginid disponibles	0,0
71		Migrar script para generar loginid disponibles	1,0
72		Migracion de lista desplegable con loginid disponibles.	1,0
73		Migrar servicio de contruccion de login id.	1,0
74		Migrar script con los login id disponible en API	1,0
75		Migrar java plugin para consulta en API	1,0
76		Pruebas unitarias y funcionales	2,0
77	Configuración de un combo (RBAC) en IGA Ambiente de Pruebas	Definicion y entrega de matriz de roles para realizacion de combos	8,0
78		Creacion documento de diseño	3,0
79		Creacion documento de plan de pruebas	3,0
80		Diseño de la configuración en IGA de un combo	8,0
81		Extender el esquema de atributos, agregando un atributo "CargoOld"	2,0
82		Ajuste al campo Actividad en IGA	3,0
83		Crear una PX Asignación de Combo	3,0
84		Crear una PX Asignar CargoOld	3,0
85		Crear una PX Retiro CargoOld	3,0
86		Crear Una PX que genere la Asignación Combo Manual-OC	3,0
87		Pruebas unitarias	3,0
88		Ajuste memoria técnica.	2,0
89		Sesion de transferencia de conocimiento.	2,0
90		Creacion manual de usuario	2,0
91		Creacion manual de administracion	2,0
92		Pruebas funcionales	2,0
81	Configuración de un combo (RBAC) en IGA Ambiente de Prorduccion	Migrar atributo "CargoOld"	2,0
82		Ajuste al campo Cargo en IGA	6,0
83		Migrar PX Asignación de Combo	5,0
84		Migrar PX Asignar CargoOld	5,0
85		Migrar PX Retiro CargoOld	5,0
86		Migrar PX que genere la Asignación Combo Manual-OC	5,0
87		Pruebas unitarias	3,0
88		Ajuste memoria técnica.	2,0
89		Sesion de transferencia de conocimiento.	2,0
90		Creacion manual de usuario	3,0
91		Creacion manual de administracion	3,0
92		Pruebas funcionales	2,0

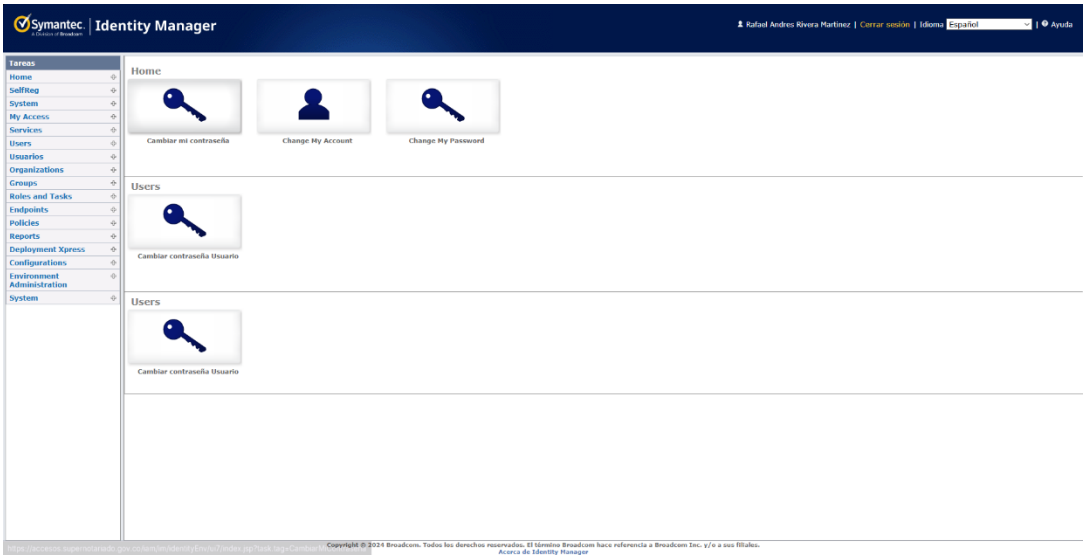
DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

255	Configurar politica de archivado de tareas	Configurar politica de periodicidad de archivado de tareas	3,0
256		Activar politica de archivado de taeas	1,0
257	Transferencia de conocimiento	Creacion plan de capacitacion	3,0
258		Capacitación Administrador	3,0
259		Capacitación Operador	3,0
260		Capacitación Usuario Final	1,0
261	Configuracion portal de aplicaciones	Configurar politicas de asignacion de roles de portal de aplicaciones	6,0
262		Asignacion masiva de roles a usuarios	4,0
263		Activacion portal de aplicaciones	1,0
264		Pruebas unitarias	1,0
265		Ajuste memoria técnica.	1,0
266		Sesion de transferencia de conocimiento.	1,0
267		Creacion manual de usuario	3,0
268		Creacion manual de administracion	3,0
269		Pruebas funcionales	1,0
270	Creacion de un modulo para el CRUD de los usuarios en IP de forma masiva o individual Ambiente de Prueaba	Crear documento de caso de uso	3,0
271		Creacion plan de prueba	3,0
272		Crear tarea de creacion de usuario en IM en ambiente de pruebas	3,0
273		Crear tarea de creacion de usuario en IP en ambiente de pruebas	3,0
274		Crear tarea de modificacio de usuario en IM en ambiente de pruebas	3,0
275		Crear tarea de modificacio de usuario en IP en ambiente de pruebas	3,0
276		Crear tarea de retiro de usuario en IM en ambiente de pruebas	3,0
277		Crear tarea de retiro de usuario en IP en ambiente de pruebas	3,0
278		Crear tarea de reintegro de usuario en IM en ambiente de pruebas	3,0
279		Crear tarea de reintegro de usuario en IP en ambiente de pruebas	3,0
280		Pruebas unitarias	3,0
281		Ajuste memoria técnica.	1,0
282		Sesion de transferencia de conocimiento.	1,0
283		Creacion manual de usuario	3,0
284		Creacion manual de administracion	3,0
285		Pruebas funcionales	1,0
286	Creacion de un modulo para el CRUD de los usuarios en IP de forma masiva o individual Ambiente de Produccion	Migrar tarea de creacion de usuario en IM en ambiente de pruebas	1,0
287		Migrar tarea de creacion de usuario en IP en ambiente de pruebas	1,0
288		Migrar tarea de modificacio de usuario en IM en ambiente de pruebas	1,0
289		Migrar tarea de modificacio de usuario en IP en ambiente de pruebas	1,0
290		Migrar tarea de retiro de usuario en IM en ambiente de pruebas	1,0
291		Migrar tarea de retiro de usuario en IP en ambiente de pruebas	1,0
292		Migrar tarea de reintegro de usuario en IM en ambiente de pruebas	1,0
293		Migrar tarea de reintegro de usuario en IP en ambiente de pruebas	1,0
294		Pruebas Unitarias en ambiente de pruebas	3,0
295		Paso a produccion	9,0
296		Pruebas fincionales en ambiente de produccion	1,0
297		Creacion manueles de usuario	3,0
298		Ajuste memoria tecnica	1,0
299	Creacion documento de "SNR - IGA - GUIA DE INTEGRACIONES IGA-SNR"	Levantamiento de informacion	1,0
300		Cosntrucción de documento basado en buenas práctica, según gestión operativa de SNR	33,0
301		Presentacion de documento y planes de trabajo	3,0
302	Integración Azure Office 365	Levantamiento de información	3,0
303		Registrar cuenta de dominio con office 0365	1,0
304		Realizar instalación del PowerShell en el conector server. Realizando los siguientes pasos de la URL adjunta	1,0
305		Realizar instalación de Microsoft Azure Active Directory Module for Windows PowerShell en el conector server. Realizando los siguientes pasos de la URL adjunta	1,0
306		Realizar instalación de Microsoft Exchange en el conector server. Realizando los siguientes pasos de la URL adjunta	1,0
307		Realizar verificación de conexión con PowerShell y office 0365. Realizando los siguientes pasos de la URL adjunta	1,0
308		Instalar certificado (En caso sea necesario la autenticación moderna vía Certificado(OPCIONAL))	1,0
309		Validar datos requeridos para la creación del enpoint en IGA	1,0
310		Creación del Endpoint Office 0365	4,0
311		Creación de atributos del Endpoint Office 0365	1,0
312		Realizar exploración y correlación del Endpoint Office 0365	3,0
313		Creación de Account Template	3,0
314		Creación de Provisioning Role	3,0
315		Pruebas unitarias	3,0
316		Ajuste memoria técnica.	1,0
317		Sesion de transferencia de conocimiento.	1,0
318		Creacion manual de usuario	3,0
319		Creacion manual de administracion	3,0
320		Pruebas funcionales	1,0

A continuación se anexan evidencias de las funcionalidades de la solución:

IGA / Identity manager:

Alcance: Identity Manager (a veces llamado IDM) es uno de los componentes centrales de la solución Broadcom IGA. Su función principal es administrar y automatizar los accesos y cuentas de usuario en los sistemas de la organización, garantizando validar logs y gestionar las tareas, políticas, módulos y demás filtros.



IGA / Configuración de un combo (RBAC):

Parametrización de un nuevo combo RBAC que consolida permisos y roles en un componente administrable y estandarizado dentro de IGA, permitiendo contar con un punto centralizado y una lógica automatizada para la asignación de roles y permisos. Y estandariza los accesos en ambientes críticos, minimiza riesgos de privilegios innecesarios, da cumplimiento a auditorías y permite un modelo de acceso más seguro y escalable.

Permite controlar mejor los accesos, reduce errores manuales, agiliza la gestión de roles y fortalece la gobernanza de identidades al ofrecer accesos coherentes y alineados con las funciones reales del personal.

IGA / Creación de formulario de validación de estado de usuario:

Diseño y validación de un formulario que permite consultar el estado de un usuario en IGA (activo, inactivo), centralizando información desde el User Store y el Provisioning Store, lo que permite mejorar los tiempos de respuesta del equipo operativo, evita reprocesos en solicitudes, y brinda una herramienta clara para validar el estado real de un usuario antes de ejecutar cambios o habilitar accesos.

DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

Optimiza la atención operativa, reduce fallas en provisión, permite diagnósticos rápidos en incidentes y reemplaza procesos manuales que antes dependían de múltiples consultas en diferentes sistemas.

IGA / Análisis de riesgo en privilegios de usuario:

Se evalúan los privilegios asignados en un entorno controlado para identificar posibles conflictos, sobrantes de acceso o violaciones a separación de funciones (SoD). Anticipa fallas de configuración, asegura que los roles definidos no generen riesgos futuros y alinea los accesos con las buenas prácticas de seguridad antes de impactar producción.

Así mismo, fortalece el cumplimiento normativo, respalda auditorías internas y externas, reduce riesgos de fraude o abuso de privilegios, y mejora la postura general de seguridad en el manejo de identidades.

IGA / Módulo de novedades de Usuarios IGA-DA:

Construcción y validación del módulo encargado de gestionar las novedades del personal, tales como vacaciones, incapacidades, licencias de maternidad o paternidad, permisos temporales y otras variaciones que afectan el estado o los privilegios de los usuarios. El módulo permite que estas novedades impacten automáticamente los atributos y accesos en IGA, asegurando que las restricciones o habilitaciones se apliquen oportunamente y garantiza que los accesos se ajusten de forma automática al estado real del funcionario, reduciendo riesgos operativos, fortaleciendo la seguridad y eliminando reprocesos derivados de actualizaciones manuales.

Esto asegura que los sistemas de la SNR ajusten permisos, bloqueos o restricciones según la situación temporal del funcionario y mejora el control interno, evita accesos indebidos durante ausencias o incapacidades, fortalece la trazabilidad frente a auditorías y aumenta la eficiencia operativa al automatizar procesos que antes dependían del área de talento humano o de acciones manuales de TI.

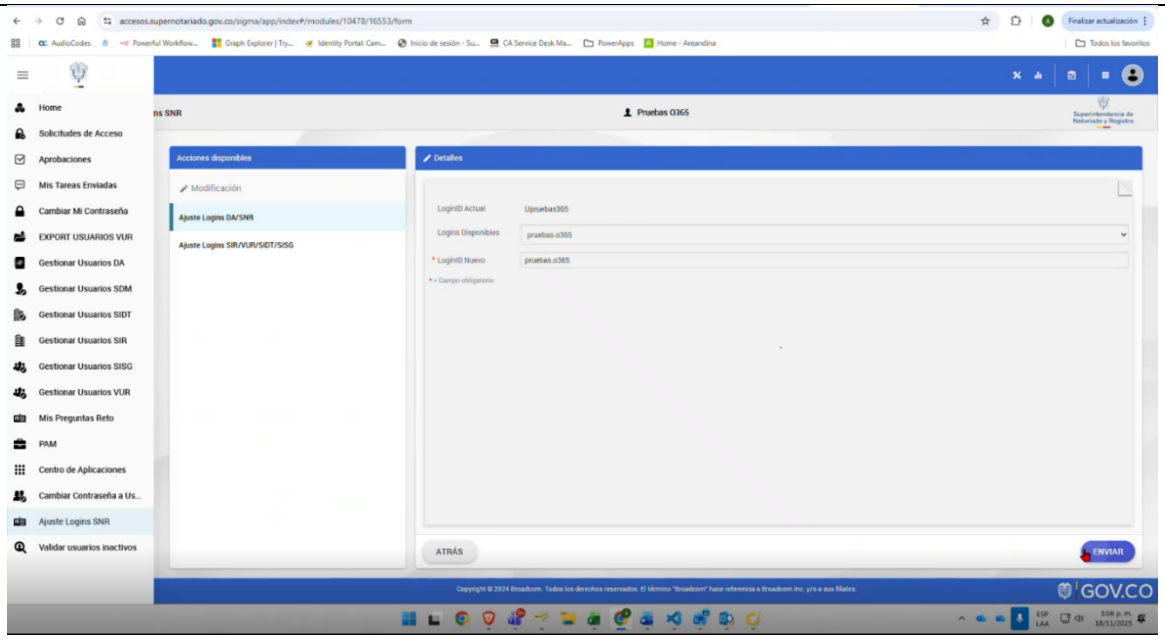
IGA / Integración Azure Office 365:

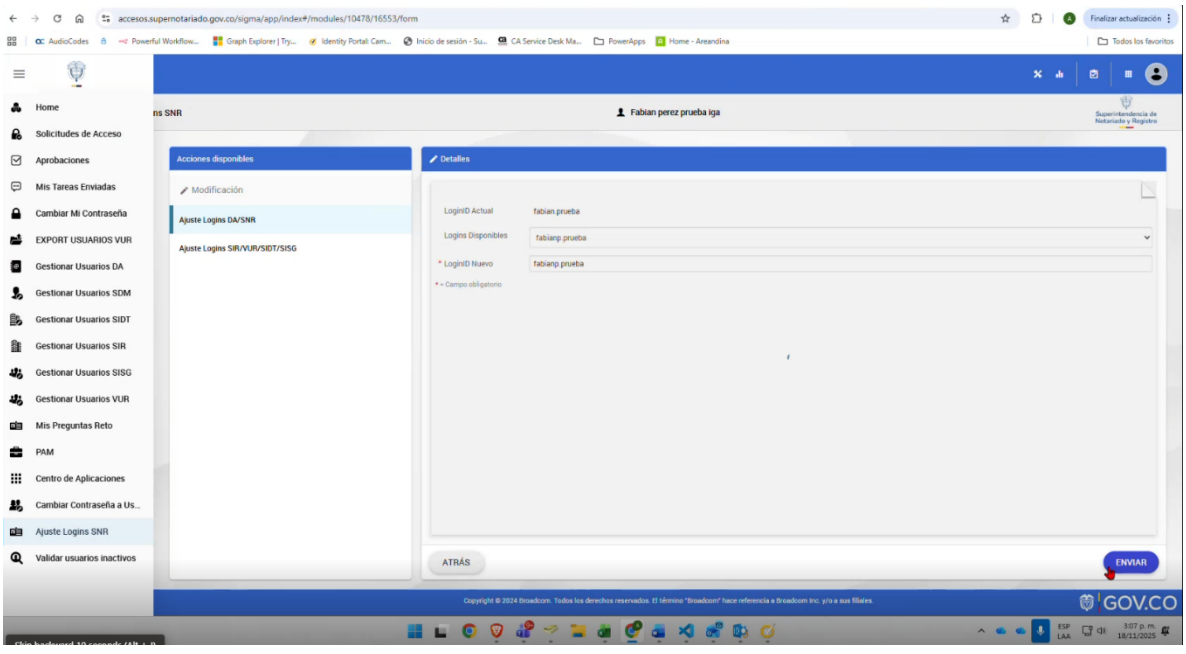
Mediante un proceso automatizado gestiona la asignación y retiro de licencias de usuarios en Office 365, permitiendo disminuir tiempo de espera y garantiza tener un control de las licencias asignadas a cada usuario desde el gestor de identidades

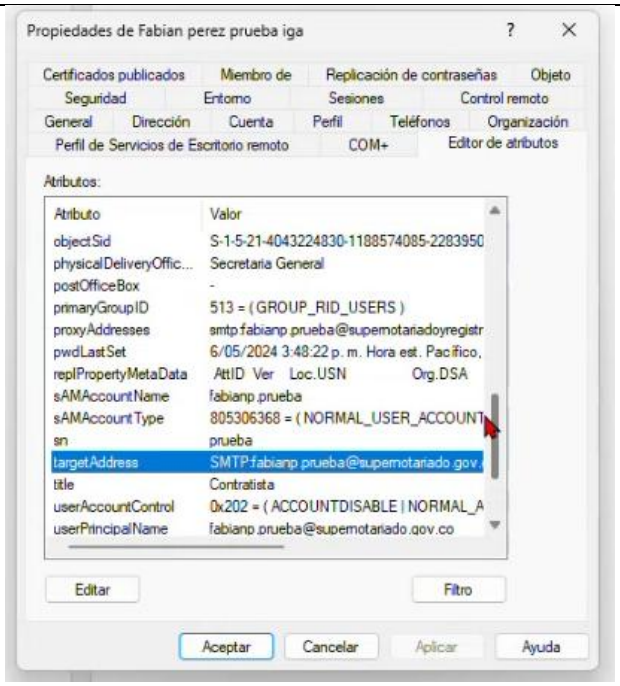
IGA / Modulo cambio de loginID:

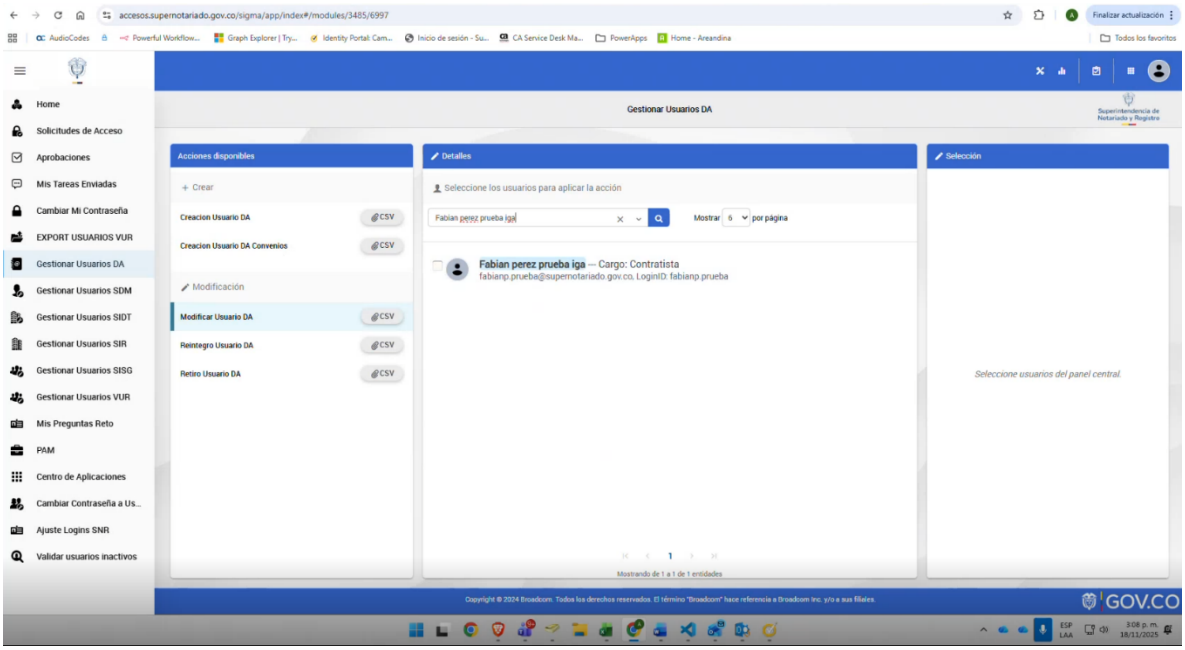
Alcance: Implementación de un mecanismo de cambio de loginID en IGA y Directorio Activo en ambiente de pruebas y producción, permitiendo automatizar el proceso de unificación de loginID y automatizar el cambio en IGA y Directorio Activo.

DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.


accesos.supernotariado.gov.co/sigma/app/index#/modules/10478/16553/form
Home
Solicitudes de Acceso
Aprobaciones
Mis Tareas Enviadas
Cambiar Mi Contraseña
EXPORT USUARIOS VUR
Gestionar Usuarios DA
Gestionar Usuarios SDM
Gestionar Usuarios SIDT
Gestionar Usuarios SIR
Gestionar Usuarios SISG
Gestionar Usuarios VUR
Mis Preguntas Reto
PAM
Centro de Aplicaciones
Cambiar Contraseña a Us...
Ajuste Logins SNR
Validar usuarios inactivos
Pruebas O365
Acciones disponibles
Modificación
Ajuste Logins DA/SNR
Ajuste Logins SIR/VUR/SIDT/SISG
Detalles
LoginID Actual
Upruebas365
Logins Disponibles
pruebas.o365
* LoginID Nuevo
pruebas.o365
ATRÁS
ENVIAR
GOV.CO


accesos.supernotariado.gov.co/sigma/app/index#/modules/10478/16553/form
Home
Solicitudes de Acceso
Aprobaciones
Mis Tareas Enviadas
Cambiar Mi Contraseña
EXPORT USUARIOS VUR
Gestionar Usuarios DA
Gestionar Usuarios SDM
Gestionar Usuarios SIDT
Gestionar Usuarios SIR
Gestionar Usuarios SISG
Gestionar Usuarios VUR
Mis Preguntas Reto
PAM
Centro de Aplicaciones
Cambiar Contraseña a Us...
Ajuste Logins SNR
Validar usuarios inactivos
Fabian perez prueba iga
Acciones disponibles
Modificación
Ajuste Logins DA/SNR
Ajuste Logins SIR/VUR/SIDT/SISG
Detalles
LoginID Actual
fabian.prueba
Logins Disponibles
fabianp.prueba
* LoginID Nuevo
fabianp.prueba
ATRÁS
ENVIAR
GOV.CO

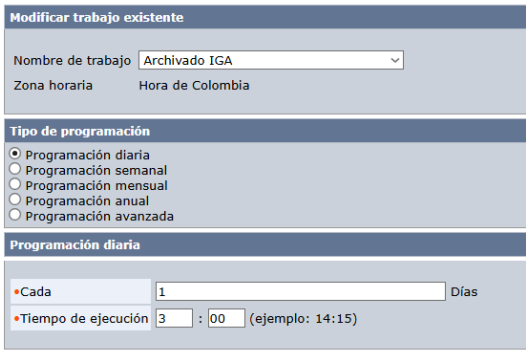


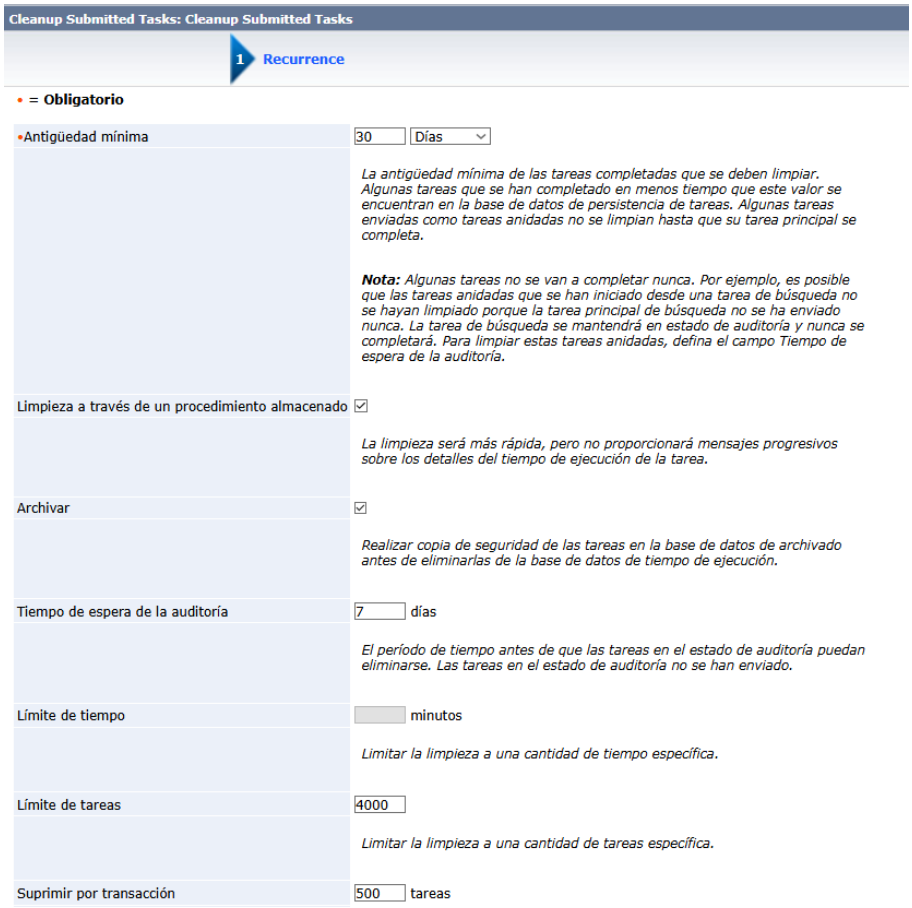


DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

IGA / Configurar política de archivado de tareas:

Alcance: Configuración de la política de archivado de tareas en ambiente de pruebas y producción, la cual permite mantener el performance optimo de la solución, mitigando la posible saturación de la base de datos, con el objetivo de que cada día se archiven las tareas del mes pasado con un límite de 4mil tareas al día de poder ser archivadas.





DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

View Submitted Tasks

Descripción	Estado	Prioridad	Iniciado por	Enviado	Última actualización	Última operación
Cleanup Submitted Tasks task	Completado	Media	MSL.RRIVERA	23/11/2025 3:00	23/11/2025 4:35	No había ningún proceso de flujo de trabajo asignado a esta tarea.
Cleanup Submitted Tasks task	Completado	Media	MSL.RRIVERA	22/11/2025 3:00	22/11/2025 23:36	No había ningún proceso de flujo de trabajo asignado a esta tarea.
Cleanup Submitted Tasks task	Completado	Media	MSL.RRIVERA	21/11/2025 3:00	22/11/2025 4:36	No había ningún proceso de flujo de trabajo asignado a esta tarea.
Cleanup Submitted Tasks task	Completado	Media	MSL.RRIVERA	20/11/2025 3:00	20/11/2025 4:51	No había ningún proceso de flujo de trabajo asignado a esta tarea.
Cleanup Submitted Tasks task	Completado	Media	MSL.RRIVERA	19/11/2025 3:00	19/11/2025 11:56	No había ningún proceso de flujo de trabajo asignado a esta tarea.
Cleanup Submitted Tasks task	Completado	Media	MSL.RRIVERA	17/11/2025 3:00	17/11/2025 16:11	No había ningún proceso de flujo de trabajo asignado a esta tarea.
Cleanup Submitted Tasks task	Completado	Media	MSL.RRIVERA	15/11/2025 3:00	15/11/2025 21:25	No había ningún proceso de flujo de trabajo asignado a esta tarea.
Cleanup Submitted Tasks task	Completado	Media	MSL.RRIVERA	14/11/2025 3:00	14/11/2025 21:54	No había ningún proceso de flujo de trabajo asignado a esta tarea.
Cleanup Submitted Tasks task	Completado	Media	MSL.RRIVERA	13/11/2025 3:00	13/11/2025 21:56	No había ningún proceso de flujo de trabajo asignado a esta tarea.
Cleanup Submitted Tasks task	Completado	Media	MSL.RRIVERA	11/11/2025 3:00	11/11/2025 23:55	No había ningún proceso de flujo de trabajo asignado a esta tarea.
Cleanup Submitted Tasks task	Completado	Media	MSL.RRIVERA	10/11/2025 3:00	10/11/2025 21:33	No había ningún proceso de flujo de trabajo asignado a esta tarea.
Cleanup Submitted Tasks task	Completado	Media	MSL.RRIVERA	9/11/2025 3:00	9/11/2025 17:26	No había ningún proceso de flujo de trabajo asignado a esta tarea.
Cleanup Submitted Tasks task	Completado	Media	MSL.RRIVERA	8/11/2025 3:00	8/11/2025 19:14	No había ningún proceso de flujo de trabajo asignado a esta tarea.

IGA / Configuración portal de aplicaciones:

Alcance: Configuración de un portal de aplicaciones en producción, el cual permite un único punto de acceso a las apps a los que el usuario tenga acceso, esto con el fin de poder automatizar procesos y gracias al uso del SSO en las aplicaciones tener un punto de autenticación unificado.

Con las políticas de asignación y retro de roles correspondiente según la aplicación, esto garantiza que solo los usuarios vean el acceso a la aplicación que realmente lo tiene.

Modify Policy Xpress Policy: Policy Xpress Search

Buscar un objeto del tipo Policy Xpress

Buscar un objeto del tipo Policy Xpress
donde Policy Name = *PORTALAPPS* Buscar Borrar

Resultados de la búsqueda

Seleccionar	Category	Policy Name	Type	Enabled	Priority
◉	DA	PX_PORTALAPPS_Asignar_ROL_DA	Tarea enviada	✓	0
○	DA	PX_PORTALAPPS_Retiro_ROL_DA	Tarea enviada	✓	0
○	SIR	PX_PORTALAPPS_AsignarYRetirar_ROL_SIR	Tarea enviada	✓	0
○	VUR	PX_PORTALAPPS_Asignar_ROL_VUR	Tarea enviada	✓	0
○	VUR	PX_PORTALAPPS_Retiro_ROL_VUR	Tarea enviada	✓	0
○	SIDT	PX_PORTALAPPS_Asignar_ROL_SIDT	Tarea enviada	✓	0
○	SIDT	PX_PORTALAPPS_Retiro_ROL_SIDT	Tarea enviada	✓	0

Edit Module: Centro de Aplicaciones

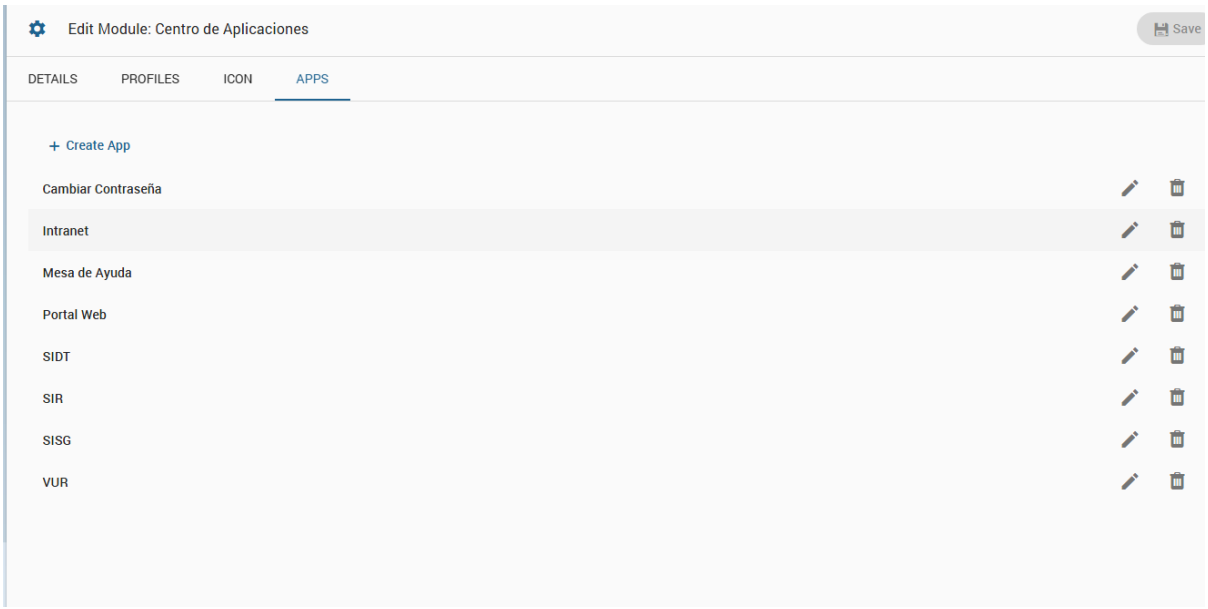
DETAILS PROFILES ICON APPS

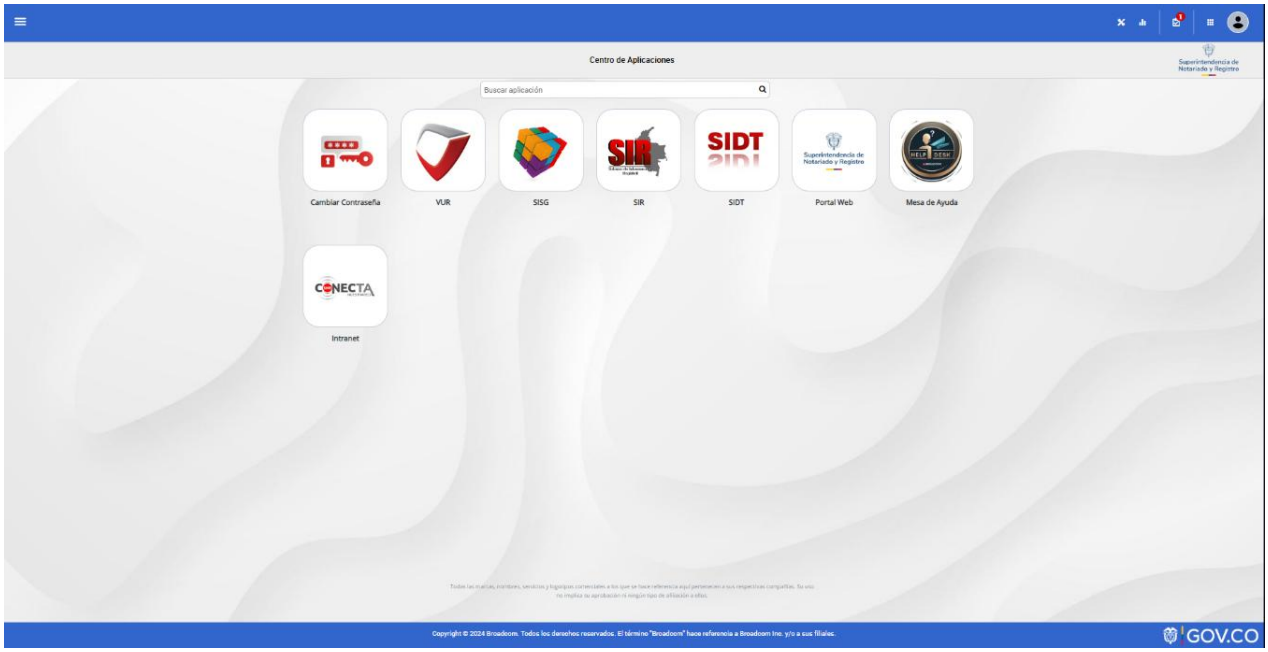
Title *
Centro de Aplicaciones

Tag *
MODULE_Centro de Aplicaciones

Type *
Apps Launchpad

DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

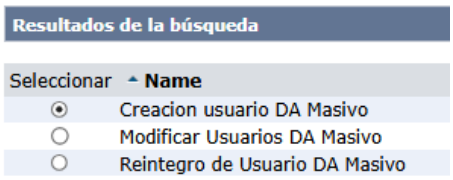


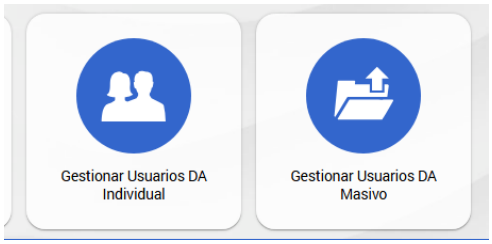


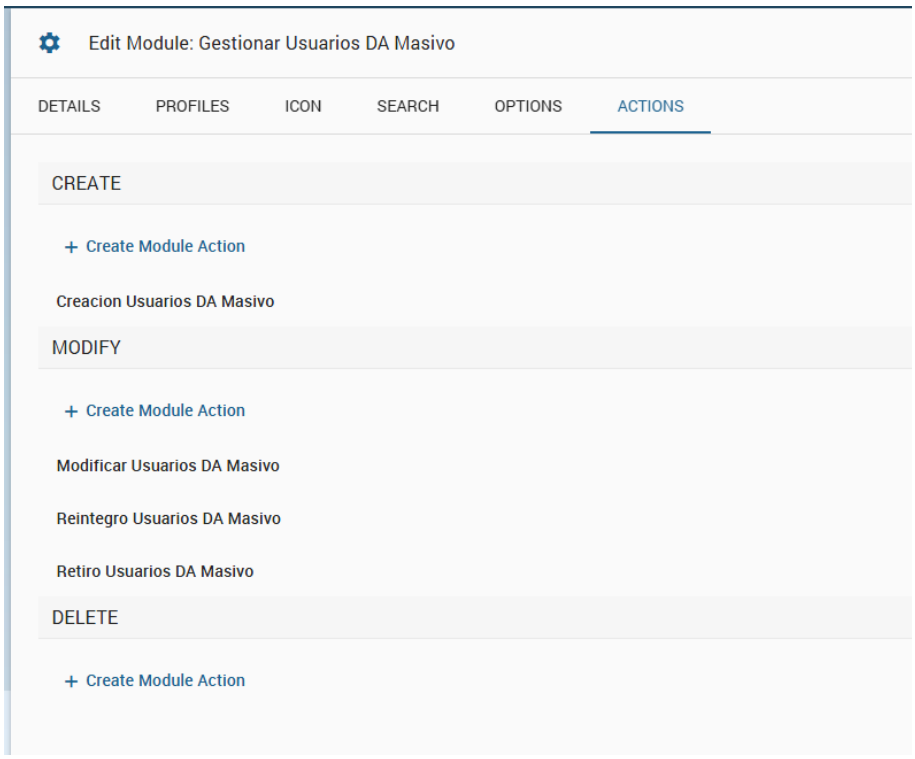
DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

IGA / Modulo para el CRUD de los usuarios en IP de forma masiva o individual:

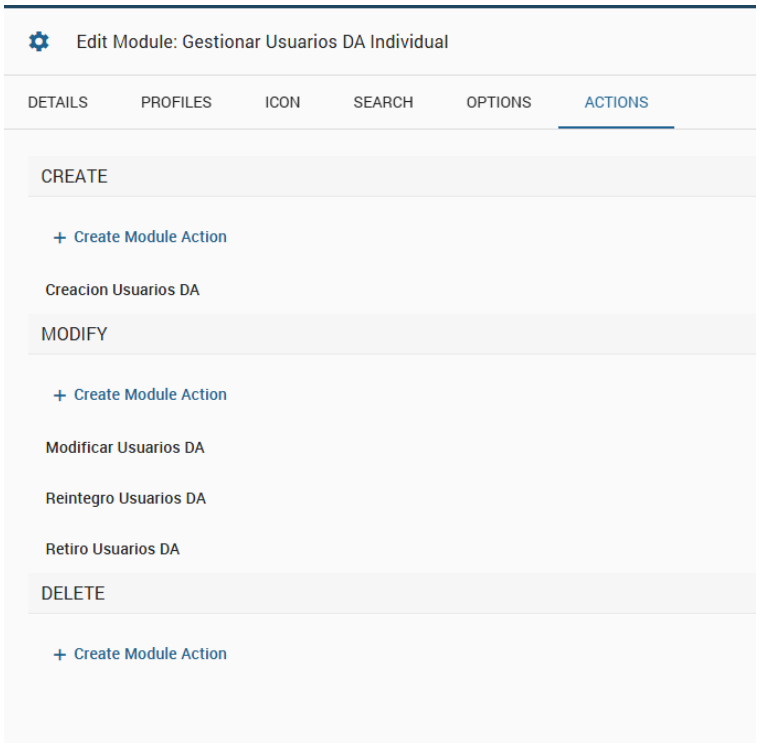
Alcance: Configuración de dos nuevos módulos en pruebas y producción los cuales permiten tanto la gestión individual y masiva de los usuarios del Directorio activo.

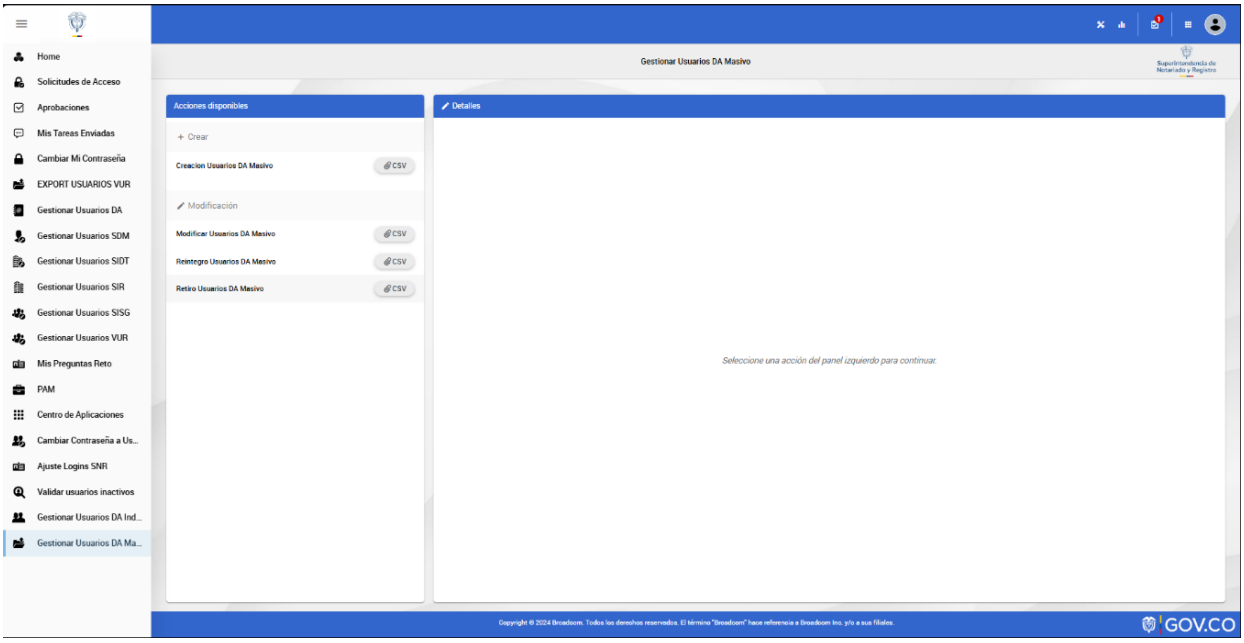




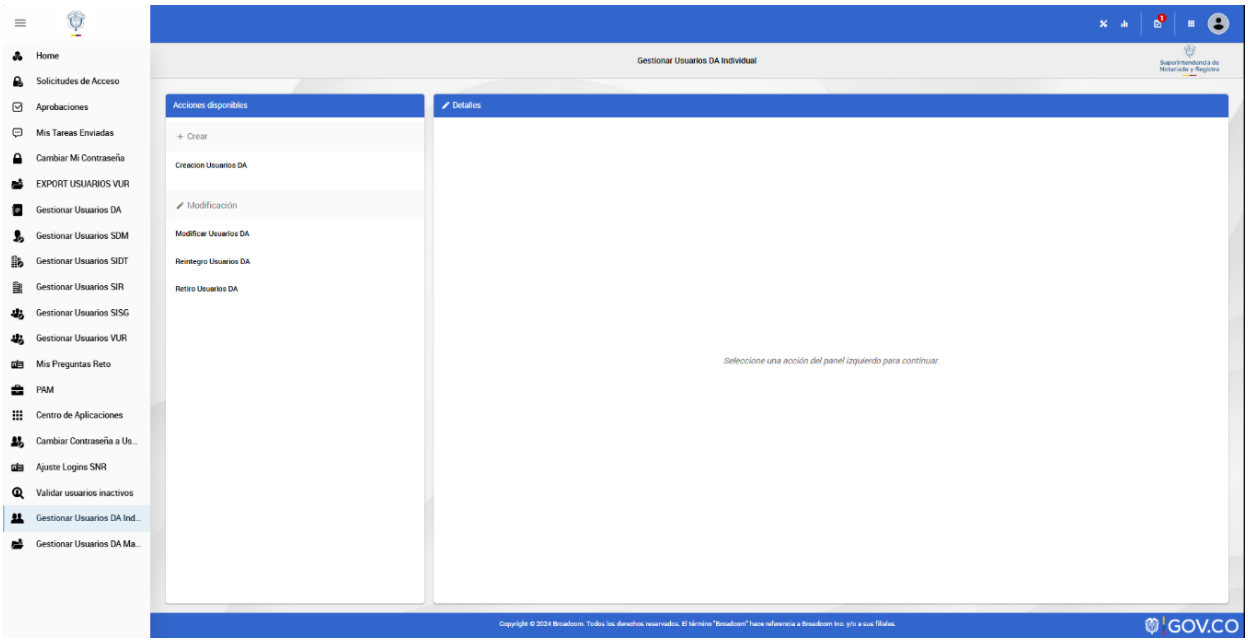


DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.





DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.



3. SSO. CA Single Sign-On (CA SSO)

CA SSO es la plataforma que unifica, protege y controla el acceso a todas las aplicaciones empresariales desde un único punto, garantizando seguridad y una experiencia fluida con Single Sign-On. Es una plataforma empresarial de gestión de acceso web que proporciona autenticación, autorización, Single Sign-On y protección de aplicaciones en ambientes on-premise, cloud e híbridos.

Su propósito es actuar como una capa de seguridad centralizada entre los usuarios y las aplicaciones, garantizando que, solo usuarios legítimos puedan acceder, tengan únicamente los permisos autorizados y el acceso se gestione de forma consistente y auditable.

CA SSO funciona como un gatekeeper (portero de seguridad) que controla el acceso a aplicaciones web, portales, APIs y servicios corporativos, sin necesidad de modificar el código de las aplicaciones.

DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

Plan de Trabajo:

Ítem	Actividad	Total de horas / Tarea	242,0 / Vobo Priorización cliente
1	Federar Servicios Office 365 y MFA	Documento de Diseño	3,0
2		Prepara SSO para integración: Esquemas de autenticación Reino de dominio Regla Política	3,0
3		Proteger la URL de autenticación affwebservices, crear proxyrules en AGW	1,0
4		Configurar ADDwebservice	1,0
5		Configurar Pasive Profile	3,0
6		Configurar Active Profile	3,0
7		Crear entidad local SSO	2,0
8		Crear entidad remota	3,0
9		Crear parnertship	3,0
10		importar certificado en SSO, Asociar al parnertship SSO	2,0
11		Creación de Aplicación Empresarial en Entra ID	2,0
12		Configuración de SAML: EntityID, AssertionConsumerService (ACS), claims persona	3,0
13		Configuración de SAML2 Authentication Scheme y Policy	3,0
14		Registro de IdP (Entra ID) en SiteMinder Federation Manager	5,0
15		importación de metadata del IdP y validación de certificado	2,0
16		Validación de metadata y atributos requeridos por SiteMinder	3,0
17		Configurar Office 365 (Dominio a federar no puede ser el default), preparación y ejecución de comandos a nivel de PowerShell, federación del Dominio	3,0
18		Pruebas Unitarias basadas en navegador web (Siute de Office), a nivel de escritorio y Mobile	3,0
19		Pruebas unitarias de Word, teams o una similar (Suite de Office) Mobile y escritorio usando Active Profile	3,0
20		Realizar Ajustes Según Pruebas Unitarias. (Si aplica)	2,0
21		Pruebas Funcionales	2,0
22		Documento De Administración	5,0
23		Documento de Memoria Técnica	3,0
47	Modernizar aplicaciones al PCA (Cambio Iplanet) VUR y SIR	VUR sesión	2,0
48		Creación del Virtual Host VUR	1,0
49		Creación de Proxy Rules	1,0
50		Validar compatibilidad de VUR con cookies HTTPOnly y Secure.	3,0
51		Pruebas sobre VUR y garantizar que no existan conflictos con headers seguros de Siteminder SSO	3,0
52		Pruebas sobre VUR (Funcionales, módulos y procesos) a través de publicación SSO.	3,0
53		Ajustes de acuerdo con pruebas realizadas	3,0
54		Realizar documento RFC	2,0
55		Gestión del cambio	2,0
56		Solicitar nuevos balanceadores para VUR por AGW	2,0
57		Ejecutar RFC (Cambiar el balanceador)	3,0
58		Validar funcionamiento	3,0
59		Sesión de entendimiento y revisión equipo SIR	2,0
60		Creación del Virtual Host SIR	2,0
61		Creación de Proxy Rules	1,0
62		Validar compatibilidad de SIR con cookies HTTPOnly y Secure.	1,0
63		Pruebas sobre SIR y garantizar que no existan conflictos con headers seguros de Siteminder SSO	3,0
64		Pruebas sobre SIR (Funcionales, módulos y procesos) a través de publicación SSO.	3,0
65		Validar funcionamiento en sesión con cliente	3,0
66		Realizar documento RFC	2,0
67		Gestión del cambio	2,0
68		Solicitar nuevos balanceadores para SIR por AGW	2,0
69		Ejecutar RFC (Cambiar el balanceador)	3,0
70		Validar funcionamiento	3,0

DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

71	Personalizar y Branding	Análisis de requerimientos de branding y lineamientos corporativos	5,0
72		Sesión con SNR(Comunicaciones) Solicitud de logos, íconos, estilos CSS.	1,0
73		Aplicación del branding en las páginas de login de SNR FCC	6,0
74		Ajuste de compatibilidad en navegadores y validación visual	5,0
75		Validación funcional del flujo de autenticación post-branding	5,0
76		Pruebas unitarias del portal de accesos (funcionalidad y diseño)	5,0
77		Actualización Documentación, Memoria Técnica y Manual Administrador	8,0
78	Auditorias (mejora)	Validación del esquema existente en PostgreSQL para auditoría	5,0
79		Revisión de las tablas y relaciones para registro de eventos de autenticación	3,0
80		Ajuste o creación del esquema lógico de auditoría si aplica	5,0
81		Extracción de datos de auditoría y validación de registros críticos (login, logout, federación)	5,0
82		Diseño y generación de informes de auditoría (consultas SQL, vistas o reportes)	6,0
83		Documentación del modelo y plan de mantenimiento de auditoría	5,0
84		Pruebas unitarias de auditoría (consistencia de datos y tiempos de registro)	5,0
85	Portal de Acceso IGA UNIFICADO	Crear Módulos	2,0
86		Crear Apps Launchpad	2,0
87		Crear Apps	5,0
88		asignar ulrs	2,0
89		pruebas unitarias	2,0
90		pruebas integrales	2,0
91		Actualizar Documentación	5,0
92	Recopilación de incidentes de seguridad y ajustes	Revisión de fuentes de logs, smaccess.log , smps.log , smpstrace.log, aff.log, FWStrace.log (Componente Policy Server y AccessGateway)	8,0
93		Definición de criterios de incidente: fallos de autenticación, accesos indebidos, errores de federación	3,0
94		Establecimiento de umbrales y parámetros de severidad (intentos fallidos, tiempos de respuesta, errores repetidos, según Revisión)	3,0
95		Extracción de logs y eventos relevantes desde servidores y componentes SSO	5,0
96		Clasificación de incidentes por tipo, severidad y origen	5,0
97		Identificación de causas raíz o justificación técnica de los incidentes	5,0
98		Registro de hallazgos en memoria técnica o bitácora de incidentes	3,0
99		Actualización de runbooks con acciones preventivas y correctivas	3,0

SSO / Federar Servicios Office 365 y MFA

Alcance: Preparación y configuración de todo el proceso necesario para que los servicios de Office 365 puedan autenticarse usando la solución de SSO (Syamntec Syteminder), incluyendo un mecanismo de seguridad adicional (MFA) propio de Microsoft. Esto implica diseñar el funcionamiento del nuevo acceso, ajustar la estructura de inicio de sesión existente, proteger las direcciones utilizadas para autenticar a los usuarios y configurar los componentes que permiten que Office 365 y la plataforma de autenticación se reconozcan entre sí. También se crea y configura la aplicación en Entra ID y se establecen los parámetros para el intercambio seguro de información.

SSO / Modernizar aplicaciones al PCA (Cambio IPlanet): VUR y SIR

Alcance: Modernización de las aplicaciones VUR y SIR, migrándolas desde el esquema actual basado en agentes IPLANET —que ya no cuentan con soporte— hacia una arquitectura más segura y estable, alineada con los estándares corporativos y la solución de autenticación Symantec SiteMinder (SSO) del SNR. La modernización se realiza mediante el componente SSO Access Gateway (AGW), configurado como proxy inverso, el cual ya está instalado e integrado con otras aplicaciones en la plataforma. Esta actualización permite garantizar compatibilidad, robustez y continuidad operativa, eliminando dependencias obsoletas y fortaleciendo la seguridad en los accesos.

DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

Para la aplicación VUR, se han ejecutado pruebas en el ambiente de pruebas, logrando la autenticación exitosa mediante la configuración y parametrización del componente SSO, incluyendo la construcción de un login de pruebas. Actualmente se continúa validando el correcto funcionamiento de los módulos internos de VUR para asegurar la integración completa.

En cuanto a SIR, se encuentra en fase de análisis para aplicar la misma estrategia de migración, garantizando que ambos sistemas operen bajo el nuevo esquema de autenticación con Access Gateway.



SSO / Personalización y Branding

Alcance: El alcance de esta actividad es adaptar la imagen gráfica de las páginas de inicio de sesión para alinearlas con la identidad visual de la organización. Esto incluye definición de colores, logos, íconos y estilos corporativos, así como la aplicación de estos elementos en las pantallas de acceso. Se contempla la validación en diferentes navegadores y dispositivos para garantizar una experiencia homogénea y funcional. Con esto se espera fortalecer la imagen institucional en los puntos críticos de interacción con el usuario, mejorar la experiencia de acceso, asegurando claridad y consistencia visual sin comprometer la seguridad y la estandarización de interfaces bajo aplicaciones integradas por la solución de autenticación de SNR de Symantec SiteMinder (SSO).

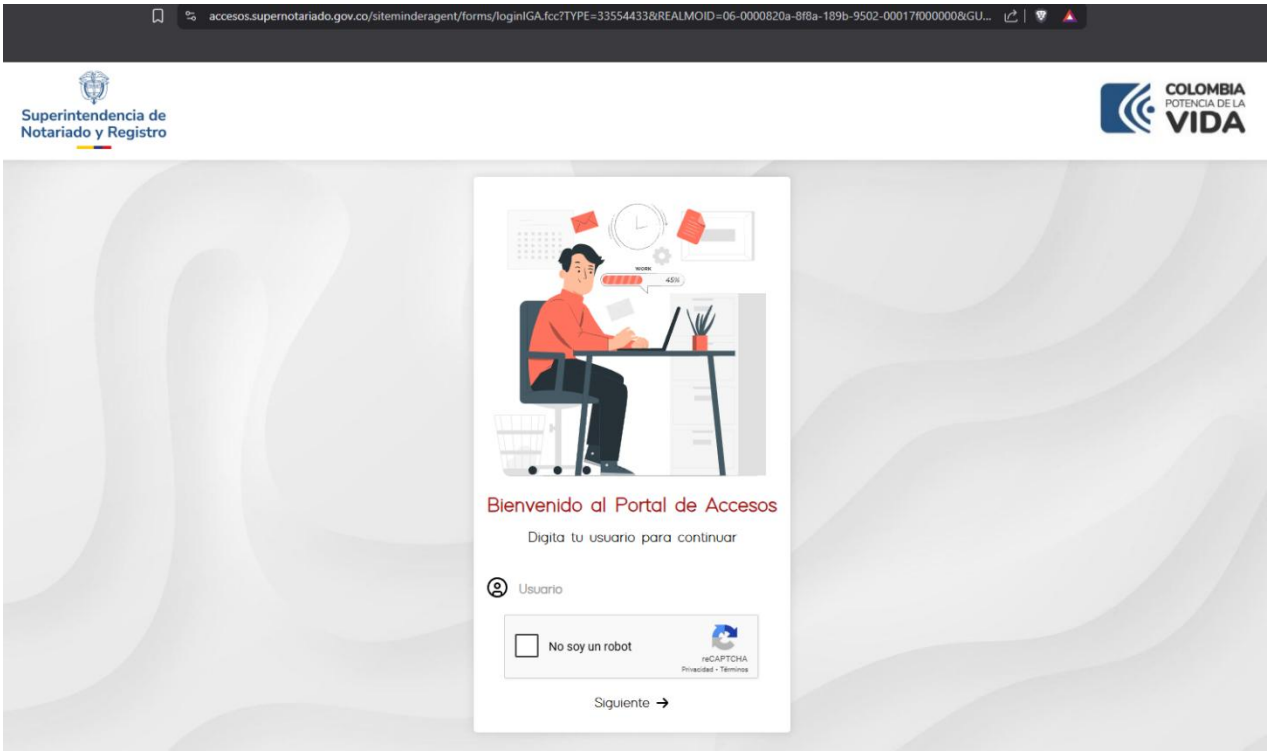
SSO / Auditorías (Mejora)

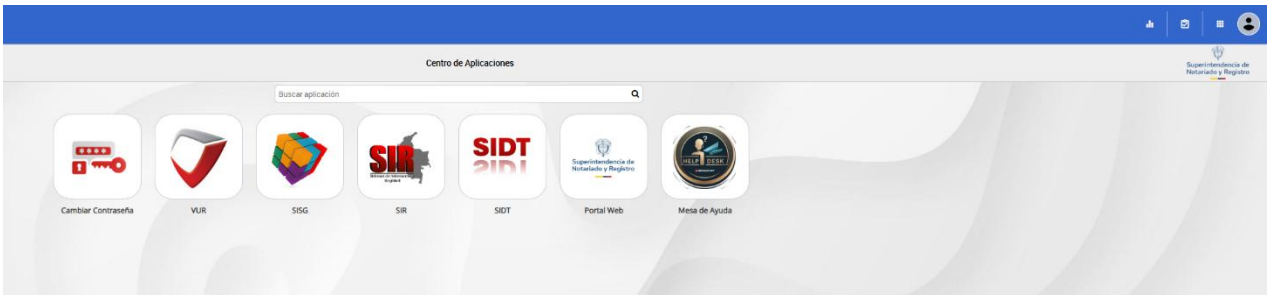
Alcance: Revisión y mejora del sistema que almacena los registros de auditoría relacionados con los accesos y autenticaciones (IP real del usuario). Permite evaluar el estado actual de la base de datos, mejoras posibles y almacenamiento de registros importantes. Mediante un reporte se puede visualizar la información relevante, el análisis de estos datos y modelo de auditoría actualizado, junto con su plan de mantenimiento. Lo que se busca incrementar la trazabilidad y confiabilidad de los registros para soportar procesos de control interno y cumplimiento normativo, mejorar la capacidad de análisis ante incidentes, reduciendo tiempos de respuesta y disponer de información estructurada para auditorías internas y externas.

DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

SSO / Portal de Acceso IGA Unificado

Alcance: Creación y adecuación del portal unificado que reúne las aplicaciones y accesos que los usuarios necesitan. Los módulos, aplicaciones y accesos correspondientes, requieren la asignación de las direcciones asociadas y de manera integrada. Desde el portal de accesos una vez el usuario se autentica a través de la solución de autenticación de SNR de Symantec SiteMinder (SSO) puede ingresar a otras aplicaciones integradas con SSO.





DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

SSO / Recopilación de incidentes de seguridad y ajustes

Alcance: Establecer un proceso sistemático para la revisión y clasificación de incidentes de seguridad en el sistema de autenticación, identificando patrones y accesos inusuales. Se definen criterios de clasificación, acciones correctivas y ajustes en los procedimientos internos para la atención y prevención de incidentes, a fin de mitigar riesgos operativos mediante la detección temprana de incidente, fortalecer la capacidad de respuesta ante fallos o errores y generar información estratégica para la toma de decisiones en materia de seguridad de Accesos.

4. API.

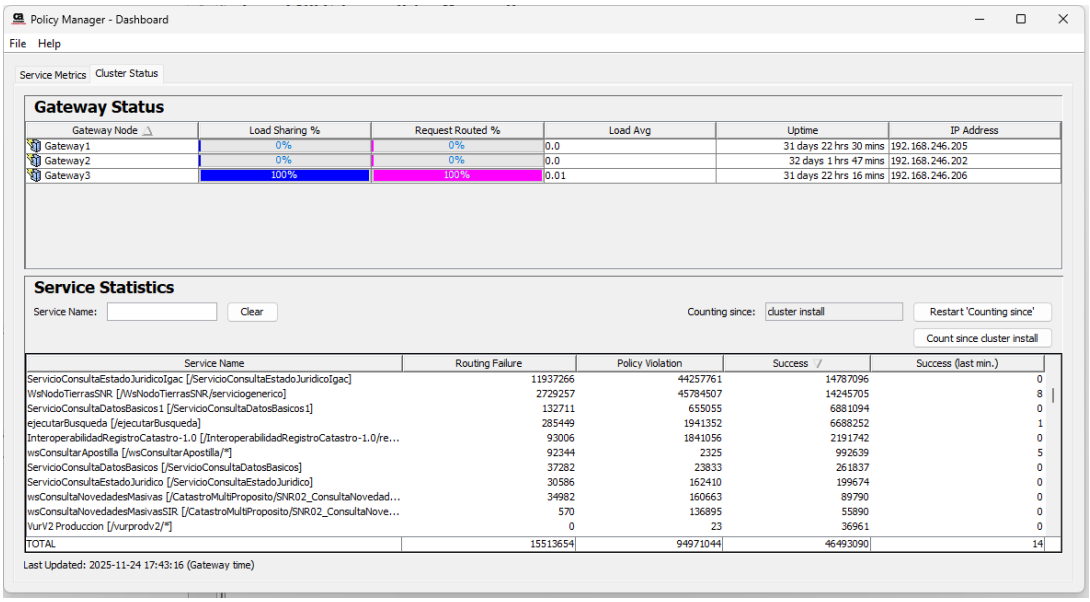
API Gateway y el API Developer Portal conforman una plataforma integral para la seguridad, gestión y habilitación del ecosistema de APIs en una organización. El API Gateway actúa como la puerta de entrada centralizada que protege y controla todo el tráfico hacia las APIs, brindando funcionalidades clave como autenticación y autorización, Single Sign-On, validación de tokens (OAuth/OIDC/JWT), protección contra ataques, limitación de consumo (rate limiting), transformación REST/SOAP, orquestación de servicios y monitoreo y auditoría. Por su parte, el API Portal funciona como el catálogo y punto de autoservicio para publicar, documentar y gestionar el consumo de APIs, permitiendo descubrimiento, registro de desarrolladores, solicitud de credenciales, versionamiento, pruebas en sandbox, gestión de suscripciones y analítica de uso.

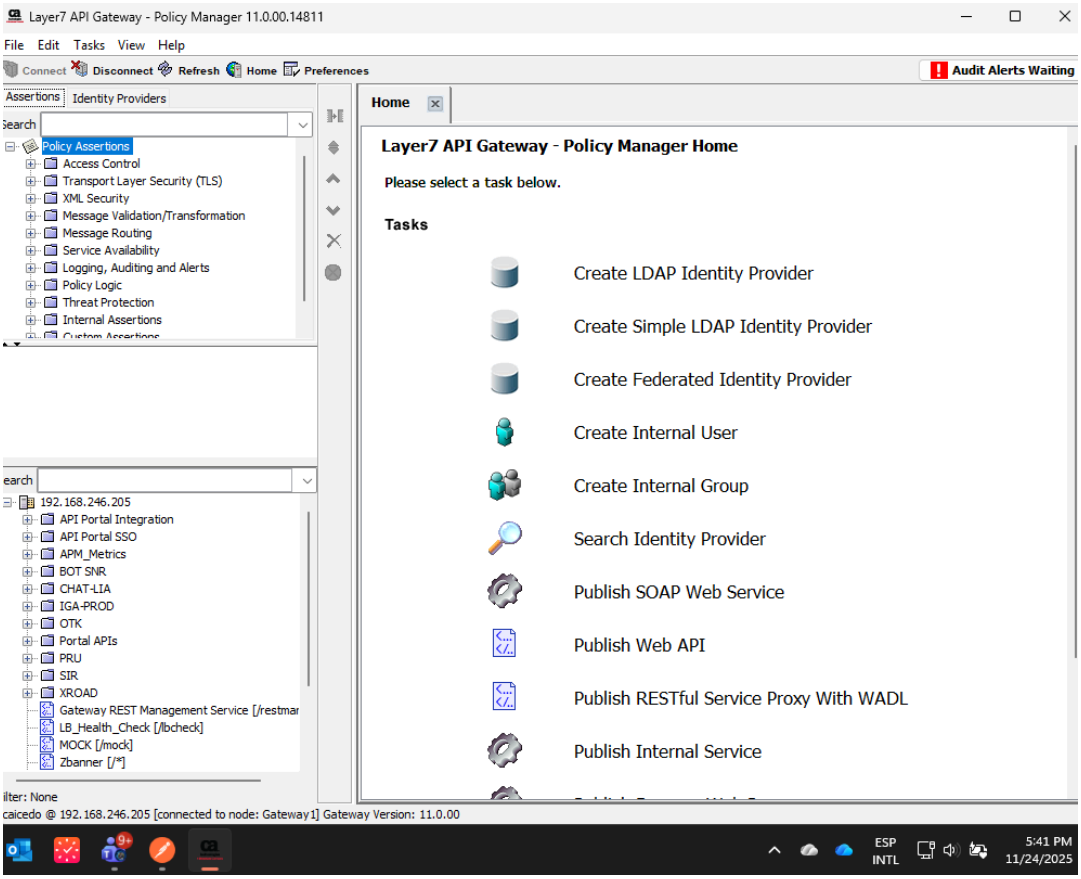
En conjunto, estas soluciones generan un alto valor para las organizaciones al aumentar la seguridad, reducir riesgos de exposición, estandarizar accesos, agilizar integraciones, reutilizar servicios, disminuir costos y tiempos de desarrollo, habilitar modelos digitales y multicanal, e incluso monetizar APIs cuando aplica. En términos estratégicos, habilitan la transformación digital, integran sistemas legacy con aplicaciones modernas y permiten que la empresa escale de forma segura y controlada su ecosistema de datos y servicios.

Plan de trabajo:

Ítem	Actividad	Total Horas / Tarea	183 / Vobo Priorización cliente
5	2. Matriz de Roles	1. Identificar roles existentes según ciclo de vida de API Gw	6
6		2. Construir documento de definición de roles y permisos por perfil	9
7		3. Configurar roles en L7 API Gw & L7 API Portal	15
8		4. Validar funcionamiento con usuarios de prueba	3
9		5. Actualización documentación (Memoria técnica y manual de administrador)	6
15	4. Integración LDAP	1. Revisión de esquema LDAP	3
16		2. Configurar conexión segura LDAPS	3
17		3. Mapear grupos y roles	9
18		4. Pruebas de autenticación	3
19		5. Actualización documentación (Memoria técnica y manual de administrador)	3
20	5. Integraciones API Gateway	1. Identificar sistemas externos	9
21		2. Documento de diseño (01 Caso de uso)	12
22		3. Definir políticas de conexión	6
23		4. Crear endpoints y flujos	18
24		5. Validar interoperabilidad de servicios	12
25		5. Actualización documentación (Memoria técnica y manual de desarrollador)	12
37	8. Portal de APIs	1.Documento diseño	12
38		2. Configuración de catálogo de APIs, de hasta 04 servicios	15
39		3. Gestión de suscriptores	9
40		4. Validación de endpoints	3
41		5. Publicación y pruebas de acceso	9
42		6. Actualización documentación (Memoria técnica y manual de administrador)	6

DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.


Policy Manager - Dashboard
File Help
Service Metrics Cluster Status
Gateway Status
Gateway Node | Load Sharing % | Request Routed % | Load Avg | Uptime | IP Address
Gateway1 | 0% | 0% | 0.0 | 31 days 22 hrs 30 mins | 192.168.246.205
Gateway2 | 0% | 0% | 0.0 | 32 days 1 hrs 47 mins | 192.168.246.202
Gateway3 | 100% | 100% | 0.01 | 31 days 22 hrs 16 mins | 192.168.246.206
Service Statistics
Service Name: Clear
Counting since: cluster install
Restart 'Counting since'
Count since cluster install
Service Name | Routing Failure | Policy Violation | Success | Success (last min.)
ServicioConsultaEstadoJuridicoIgac [/ServicioConsultaEstadoJuridicoIgac] 11937266 44257761 14787096 0
WsNodoTierrasSNR [/WsNodoTierrasSNR/serviciogenerico] 2729257 45784507 14245705 8
ServicioConsultaDatosBasicos1 [/ServicioConsultaDatosBasicos1] 132711 655055 6881094 0
ejecutarBusqueda [/ejecutarBusqueda] 285449 1941352 6688252 1
InteroperabilidadRegistroCatastro-1.0 [/InteroperabilidadRegistroCatastro-1.0/re... 93006 1841056 2191742 0
wsConsultarApostilla [/wsConsultarApostilla/*] 92344 2325 992639 5
ServicioConsultaDatosBasicos [/ServicioConsultaDatosBasicos] 37282 23833 261837 0
ServicioConsultaEstadoJuridico [/ServicioConsultaEstadoJuridico] 30586 162410 199674 0
wsConsultaNovedadesMasivas [/CatastroMultiProposito/SNR02_ConsultaNovedad... 34982 160663 89790 0
wsConsultaNovedadesMasivasSIR [/CatastroMultiProposito/SNR02_ConsultaNove... 570 136895 55890 0
VurV2 Produccion [/vurprodv2/*] 0 23 36961 0
TOTAL 15513654 94971044 46493090 14
Last Updated: 2025-11-24 17:43:16 (Gateway time)


Layer7 API Gateway - Policy Manager 11.0.00.14811
File Edit Tasks View Help
Connect Disconnect Refresh Home Preferences
Audit Alerts Waiting
Assertions Identity Providers
Policy Assertions
Access Control
Transport Layer Security (TLS)
XML Security
Message Validation/Transformation
Message Routing
Service Availability
Logging, Auditing and Alerts
Policy Logic
Threat Protection
Internal Assertions
192.168.246.205
API Portal Integration
API Portal SSO
APM_Metrics
BOT SNR
CHAT-LIA
IGA-PROD
OTK
Portal APIs
PRU
SIR
XROAD
Gateway REST Management Service [/restmar
LB_Health_Check [/lbcheck]
MOCK [/mock]
Zbanner [/*]
Home
Layer7 API Gateway - Policy Manager Home
Please select a task below.
Tasks
Create LDAP Identity Provider
Create Simple LDAP Identity Provider
Create Federated Identity Provider
Create Internal User
Create Internal Group
Search Identity Provider
Publish SOAP Web Service
Publish Web API
Publish RESTful Service Proxy With WADL
Publish Internal Service
caicedo @ 192.168.246.205 [connected to node: Gateway1] Gateway Version: 11.0.00
ESP INTL
5:41 PM 11/24/2025

API / Matriz de Roles

Alcance: Módulo en el cual se definen. Documenta y configuran la matriz de roles y permisos en el ciclo de vida de las APIs, asegurando su correcta implementación en Layer7 API Gateway, con validación y actualización de documentación técnica.

Beneficio para la entidad:

- Fortalece la seguridad y control de acceso a las APIs.
- Mejora la gobernanza y trazabilidad en la administración de APIs.
- Facilita la escalabilidad y mantenimiento, reduciendo riesgos operativos.

API / Integración LDAP

Alcance: Permite integrar el servicio de directorio corporativo (LDAP) con el Layer7 API Gateway, estableciendo conexión segura, mapeo de roles y autenticación centralizada, con documentación actualizada.

Beneficio para la entidad:

- Centraliza la gestión de identidades y credenciales.
- Incrementa la seguridad mediante autenticación robusta y cifrada. (Policy Manager)
- Alinea la plataforma con políticas corporativas y estándares internos.

API / Integraciones API Gateway

Alcance: Diseño e implementación de las integraciones entre el API Gateway y sistemas externos, definiendo políticas de conexión, endpoints y flujos, validando interoperabilidad y actualizando documentación técnica.

Beneficio para la entidad:

- Garantiza interoperabilidad segura entre sistemas internos y externos.
- Reduce tiempos de desarrollo mediante estandarización de integraciones.
- Impulsa la innovación y reutilización de servicios ya existentes en SNR.

API / Portal de APIs

API Developer Portal permite a los Administradores de API controlar cómo se publican sus APIs, permite a los consumidores descubrir qué servicios están disponibles y ayuda a los equipos de operaciones a supervisar el rendimiento de las API mediante la integración con herramientas de monitorización de API de nivel empresarial.

API Portal simplifica el descubrimiento de APIs para los desarrolladores y les proporciona acceso a datos para crear aplicaciones rápidamente. Las relaciones e interacciones con desarrolladores, socios y terceros se gestionan fácilmente.

Los desarrolladores en SNR y de entidades aliadas pueden usar API Portal para:

- Descubrir qué API están disponibles y solicitar acceso.
- Recibir autorización para usar las API y obtener llaves de API.

DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

- Comenzar a desarrollar más rápido con herramientas educativas que incluyen aplicaciones de ejemplo, API Explorer y generación de código.

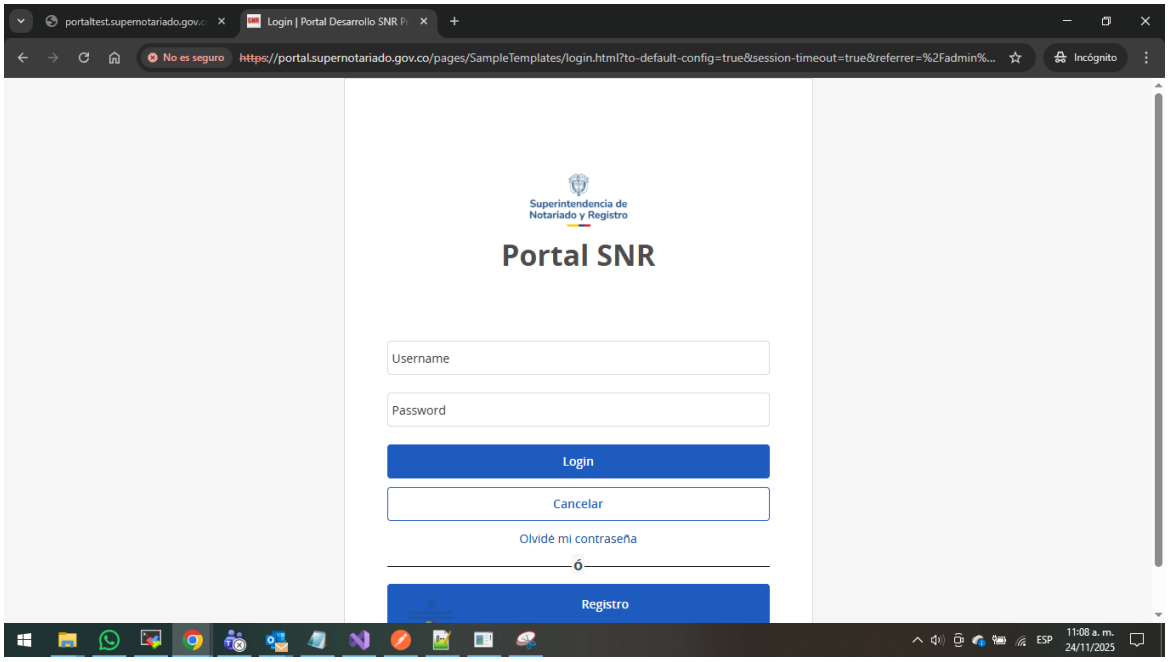
API Portal utiliza una arquitectura contenerizada que es compatible con los entornos donde residen sus aplicaciones y API facilitando la implementación, la migración y la carga de trabajo de las actualizaciones. Los componentes del portal se implementan en contenedores Docker, lo que facilita el intercambio o la sustitución de contenedores a medida que se implementan nuevas funcionalidades. Independientemente de dónde implemente, la solución utiliza la misma interfaz para administrar sus API y a sus desarrolladores. Las API integradas del portal aprovechan las herramientas de desarrollo existentes para optimizar la integración entre la gestión de API y los datos de los sistemas CI/CD.

Las API permiten la integración con herramientas integradas y almacenes de datos existentes, o bien realizan fusiones entre datos empresariales y datos de API.

Alcance:

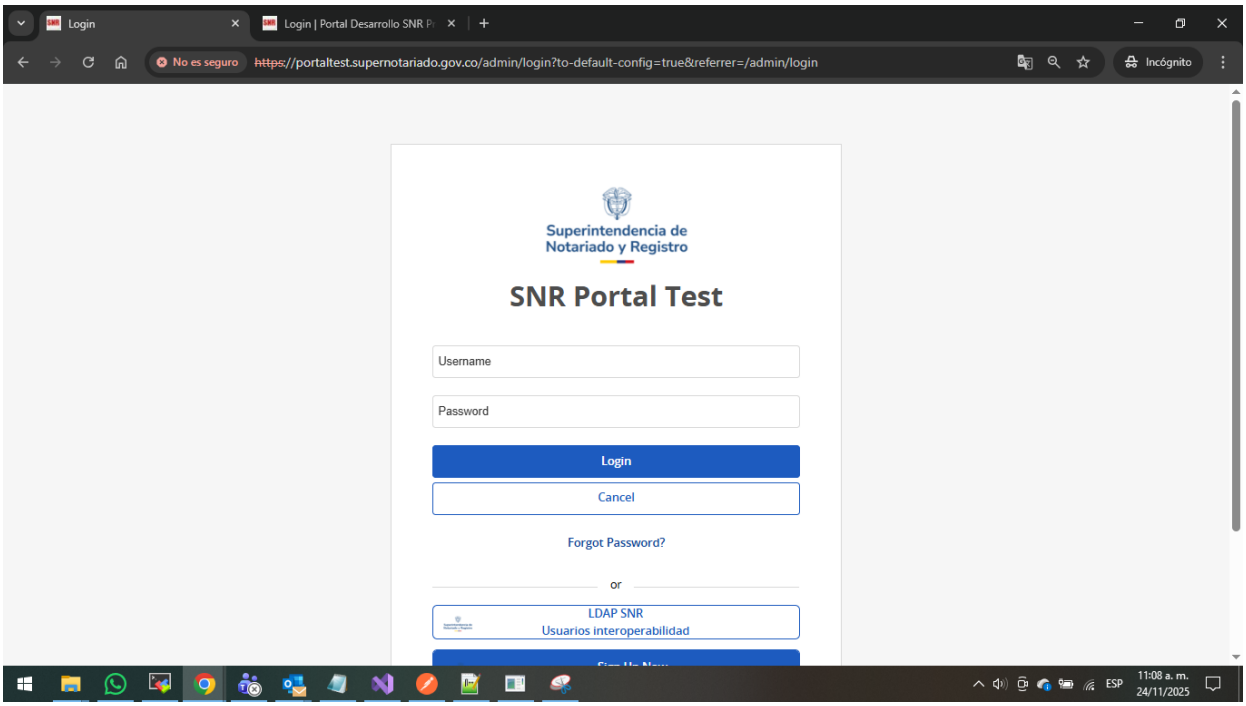
- Se Personaliza look & feel de la entidad (logotipo)
- Se establecen mensajes de mail en español vía Portal API.
- Se personaliza a español plantillas manejables de Portal API.
- Se parametrizan los manejos de eventos sobre peticiones de usuarios y servidores LDAP y SMTP.
- Se completa enrolamiento y sincronización de APIs.

Portal instancia producción

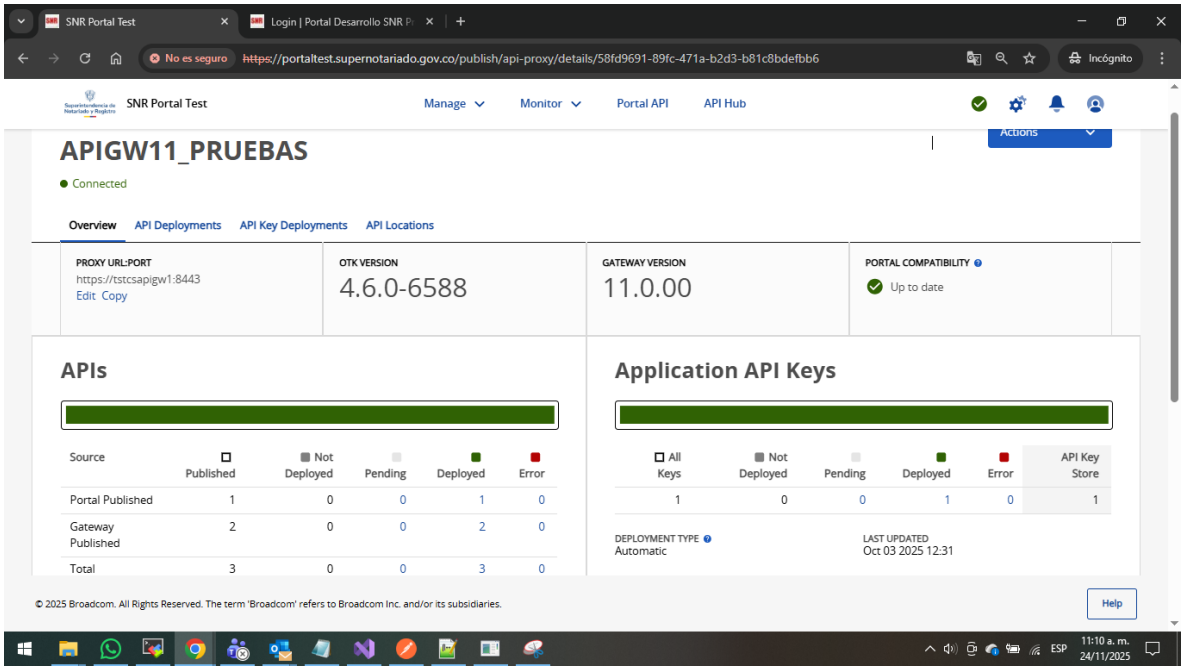


DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

Portal instancia pruebas

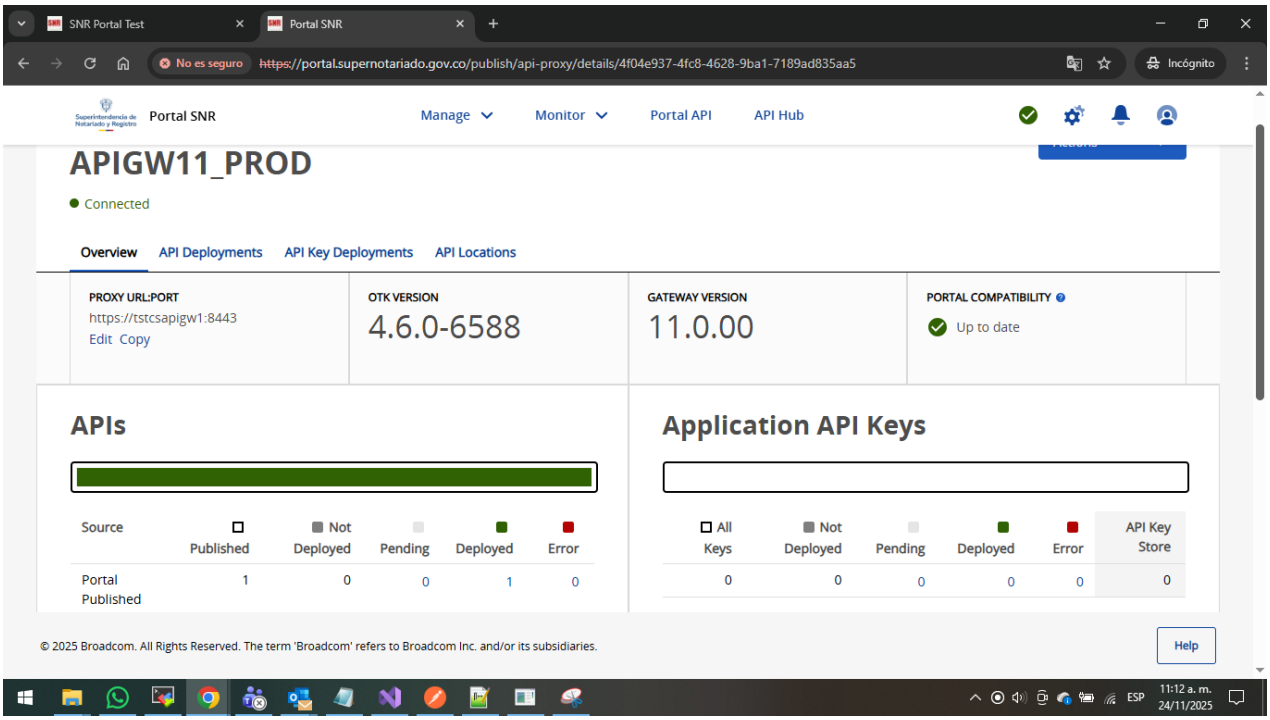


Ambiente de pruebas enrolado y conectado a API Gateway



DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

Ambiente de producción enrolado y conectado a API Gateway

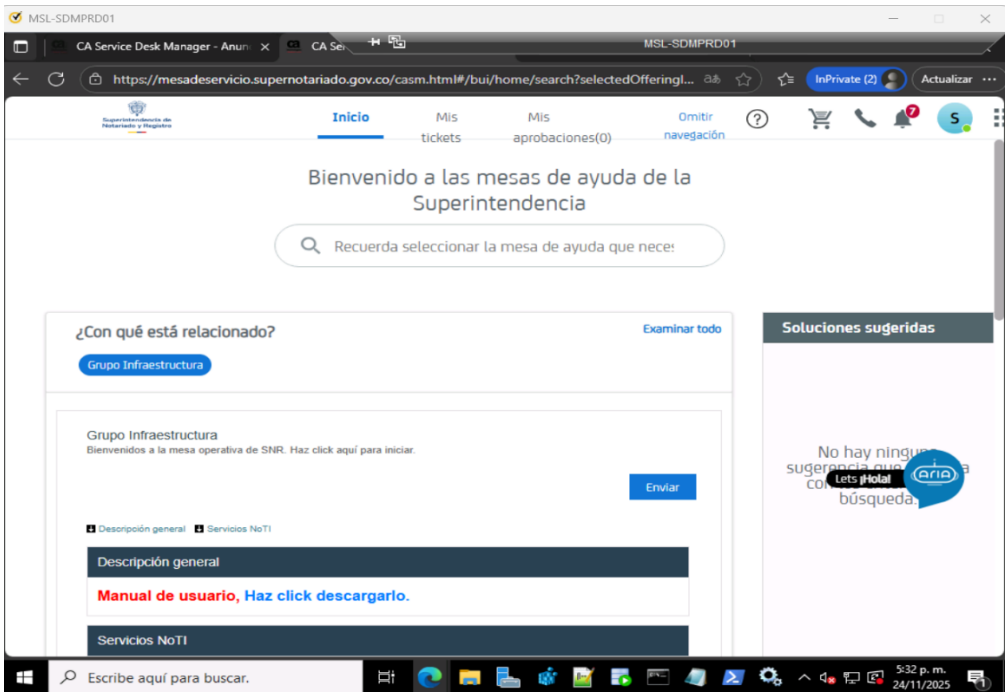


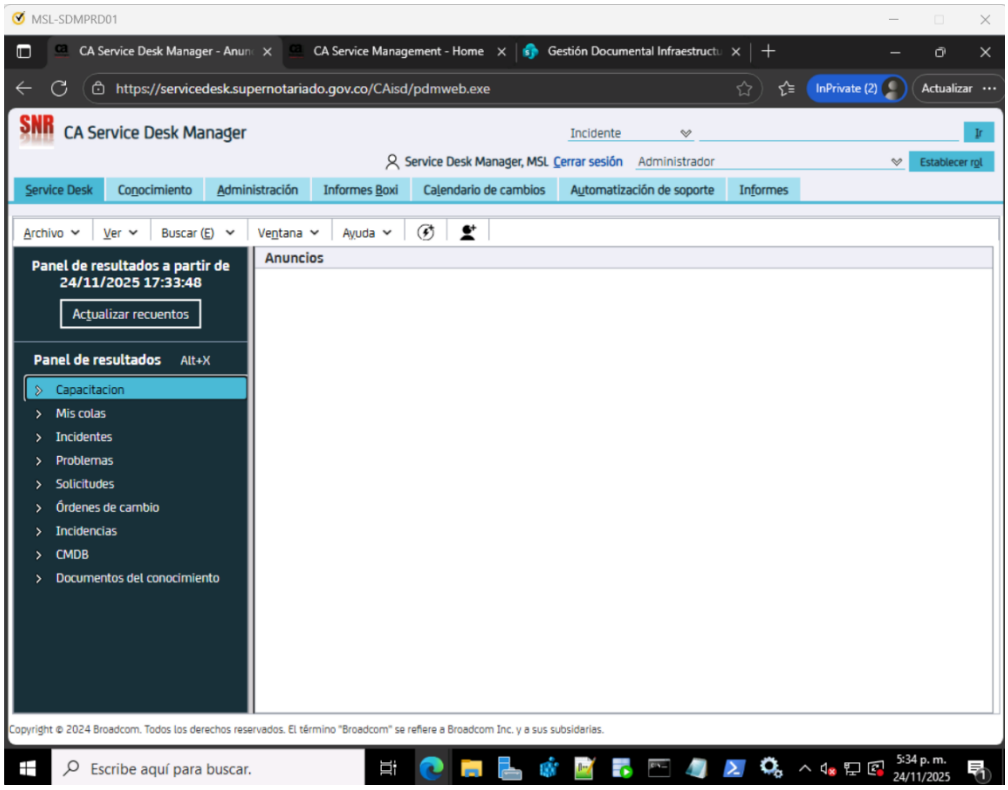
5. **SDM. CA Service Desk Manager Full License**. Es una solución empresarial de gestión de servicios TI (ITSM) diseñada para centralizar, automatizar y optimizar la atención de requerimientos e incidentes dentro de una organización. SDM permite gestionar el ciclo completo de soporte, desde la recepción de solicitudes hasta su resolución y cierre, alineándose con las mejores prácticas de ITIL. Lo que hace SDM es actuar como el núcleo operacional del soporte TI, facilitando el registro, clasificación, asignación, seguimiento y solución de incidentes, problemas, solicitudes y cambios, mejorando la eficiencia del servicio y la experiencia del usuario final.

   Además, SDM genera valor para las organizaciones al reducir tiempos de resolución, incrementar la productividad del equipo de soporte, mejorar el cumplimiento de SLA, disminuir costos operativos y ofrecer visibilidad en tiempo real del desempeño del servicio mediante reportes y analítica.

   Esta herramienta es fundamental para gestionar eficientemente el soporte técnico y la resolución de problemas en toda la organización.

DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.


MSL-SDMPRD01
CA Service Desk Manager - Anun
https://mesadeservicio.supernotariado.gov.co/casm.html#/bui/home/search?selectedOfferingI...
InPrivate (2)
Actualizar
Inicio
Mis tickets
Mis aprobaciones(0)
Omitir navegación
Bienvenido a las mesas de ayuda de la Superintendencia
Recuerda seleccionar la mesa de ayuda que nece
¿Con qué está relacionado?
Examinar todo
Grupo Infraestructura
Soluciones sugeridas
Grupo Infraestructura
Bienvenidos a la mesa operativa de SNR. Haz click aquí para iniciar.
Enviar
Descripción general
Servicios NoTI
Descripción general
Manual de usuario, Haz click descargarlo.
Servicios NoTI
Escribe aquí para buscar.
5:32 p. m.
24/11/2025


MSL-SDMPRD01
CA Service Desk Manager - Anun
CA Service Management - Home
Gestión Documental Infraestructu
https://servicedesk.supernotariado.gov.co/CAisd/pdmweb.exe
InPrivate (2)
Actualizar
SNR CA Service Desk Manager
Incidente
Ir
Service Desk Manager, MSL Cerrar sesión
Administrador
Establecer rol
Service Desk
Conocimiento
Administración
Informes Boxi
Calendario de cambios
Automatización de soporte
Informes
Archivo
Ver
Buscar (E)
Ventana
Ayuda
Panel de resultados a partir de 24/11/2025 17:33:48
Actualizar recuentos
Panel de resultados Alt+X
Capacitacion
Mis colas
Incidentes
Problemas
Solicitudes
Órdenes de cambio
Incidencias
CMDB
Documentos del conocimiento
Anuncios
Copyright © 2024 Broadcom. Todos los derechos reservados. El término "Broadcom" se refiere a Broadcom Inc. y a sus subsidiarias.
Escribe aquí para buscar.
5:34 p. m.
24/11/2025

Plan de trabajo:

ITEM	Actividad	Total de horas	417
		Tareas	Vobo Priorización cliente
1	PLAN 1. Actualizar la suite Service Management	Tomar respaldo de los servidores de pruebas	0,0
2		Tomar backup de las bases de datos	0,0
3		Actualización de SDM al RU4	4,0
4		Actualización de xflow al RU4	3,0
5		Actualización de SC al RU4	4,0
6		Actualización de Servidor de busqueda al RU4	3,0
7		Ejecución del ejecutable para la actualización de ITPAM CP04.	5,0
8		Pruebas por parte del cliente	4,0
9		Ajustes a las pruebas	4,0
10		Pruebas finales	4,0
11		Paso a Producción	0,0
12		Ventana de actualización de Service Management	0,0
13		Integración con Jasper Reports 9.0.0	11,0
14		Tomar respaldo de los servidores de pruebas	0,0
15		Tomar backup de las bases de datos	0,0
16		Actualización de SDM al RU4	4,0
17		Actualización de xflow al RU4	3,0
18		Actualización de SC al RU4	4,0
19		Actualización de Servidor de busqueda al RU4	3,0
20		Ejecución del ejecutable para la actualización de ITPAM CP04.	8,0
21		Pruebas por parte del cliente	4,0
22		Ajustes a las pruebas	4,0
23		Pruebas finales	4,0
24		Paso a Producción	0,0
25		Ventana de actualización de Service Management	0,0
26		Integración con Jasper Reports 9.0.0	11,0
65	PLAN 4. Implementacion de la CMDB	Refinamiento de la CMDB con área de trabajo que usarán este módulo	11,0
66		Creación de documento de diseño acorde al levantamiento de información	5,0
67		Transferencia de conocimiento	4,0
68		Prueba de validación de la consistencia de los campos en la CMDB	3,0
69		Pruebas de validación de las familiar y clases en la CMDB	3,0
70		Pruebas de consulta y actualización de campos en la CMDB	3,0
71		Revisión de documentos	8,0
72		Creación de campos en el esquema de SDM acorde a los campos usuados por cada CI	8,0
73		Editar las formas html para adaptar la CMDB a los campos que usará cada familia	8,0
74		Configurar archivos de cargue	5,0
75		Realizar cargue	4,0
76		Revisión del cargue	3,0
77		Paso a producción	8,0
78	PLAN 5. Implementación de la Gestión de Problemas	Descubrimiento y diseño del proceso	21,0
79		Definicion de categorias	13,0
80		Configuracion SDM	26,0
81		Transferencia de conocimiento al final de la implementación.	4,0
82		Pruebas de autoasignación, cumplimiento de SLA, notificaciones, gestión de tareas, actualización de tickets	8,0
83		Pruebas finales	3,0
84		Creación de categorías en producción	7,0
85		Creación de flujo de tareas en producción	7,0
86		Creación de notificaciones en producción	4,0
87		Creación de memoria técnica.	4,0
88		Actualización de manual de administración	7,0

DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

95	PLAN 7. Implementación Incidentes de Seguridad	Levantamiento de información	13,0
96		Construcción del documento de casos de uso	8,0
97		Creación y configuración del tipo de acceso.	4,0
98		Creación de las categorías para la clasificación de los incidentes de seguridad.	5,0
99		Creación del flujo de tareas en cada una de las categorías.	8,0
100		Creación de la macro de notificación de las tareas.	3,0
101		Modificación del formulario de CA SDM para incidentes de seguridad.	1,0
102		Pruebas Unitarias	7,0
103		Pruebas Funcionales	3,0
104		Creación y configuración del tipo de acceso en producción.	4,0
105		Creación de las categorías para la clasificación de los incidentes de seguridad en producción.	5,0
106		Creación del flujo de tareas en cada una de las categorías en producción.	8,0
107		Creación de la macro de notificación de las tareas en producción.	3,0
108		Modificación del formulario de CA SDM para incidentes de seguridad en producción.	1,0
109		Transferencia de conocimiento	3,0
110	PLAN 9. Implementación flujo de tareas en requerimientos.	Sesiones de levantamiento de información con el cliente para conocer el alcance del proyecto. Se ofertará inicialmente la solución mediante el flujo de tareas, luego se evaluará lo esperados por parte del cliente. Se realizarán sesiones para conocer el proceso y hacer el refinamiento del proyecto.	13,0
111		Creacion de categorias necesarias para llevar a cabo este proyecto. Inicialmente se consideran 15 categorías	7,0
112		Configuraciones SDM (automatizar Flujos) que harán cambios de estado de forma automática, enviarán notificaciones y llevarán el flujo de aprobación	13,0
113		Creacion de tareas por categorías, se estima 5 tareas por cada una	13,0
114		Creacion de SLA por cada tarea, se estiman 5 SLA	7,0
115		Pruebas Unitarias	7,0
116		Pruebas Funcionales	3,0
117		Implementación en producción. Creación de categorías, flujo de tareas, estados usados por las tareas y eventos de notificación.	8,0
118		Documentación del cierre de la implementación	3,0
119		Transferencia de conocimiento	3,0

SDM / Actualizar la suite Service Management versión 17.4.3.0 (RU3), hacia la versión 17.4.4.0 (RU4)

Alcance: Actualización de la plataforma CA Service Management, de la versión 17.4.3.0 (RU3), hacia la versión 17.4.4.0 (RU4). El objetivo principal es fortalecer la seguridad, estabilidad y experiencia de usuario en los módulos de Service Desk Manager, Service Catalog, xFlow y Service Point, incorporando mejoras críticas como la implementación de HTTP Strict Transport Security (HSTS), optimización del SSL Configurator, correcciones en APIs REST/SOAP y GRLoader, mejoras en la gestión de adjuntos y documentos de conocimiento. Adicionalmente, se incluyen ajustes funcionales en Service Catalog y Service Point, junto con mejoras de usabilidad en xFlow, asegurando compatibilidad con Oracle 11g–19c, y con CA Process Automation 4.4 CP4, alineándose con las directrices de seguridad y estándares corporativos definidos por la organización.

CA Service Management versión base 17.4 consiste en proveer una plataforma integrada de gestión de servicios empresariales que incluye Service Desk Manager, Service Catalog, Asset Portfolio Management, xFlow y Service Point, ofreciendo capacidades de gestión de incidentes, problemas, cambios, solicitudes y activos bajo un modelo ITIL, con soporte para bases de datos Oracle (11g–19c) integración con EEM para autenticación, compatibilidad con CA Process Automation para automatización de flujos, y mejoras en seguridad, usabilidad y reporting respecto a versiones anteriores, consolidando en una sola suite la administración de servicios, la experiencia del usuario final y la eficiencia operativa de TI.

DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

SDM / Implementación de la CMDB

Alcance: Implementación de la base de datos de gestión de la configuración (CMDB) dentro de la plataforma CA Service Management, de la versión 17.4.3.0 (RU3) a la versión 17.4.4.0 (RU4). El objetivo principal es consolidar en un repositorio centralizado la información de los elementos de configuración (CI) y sus relaciones, permitiendo una visión integral de la infraestructura tecnológica y facilitando la gestión de incidentes, problemas y cambios bajo las prácticas de ITIL. Con la actualización a RU4, se incorporan mejoras de seguridad como HTTP Strict Transport Security (HSTS) y optimización del SSL Configurator, además de correcciones en APIs REST/SOAP, GRLoader y procesos críticos de SDM, lo que asegura mayor estabilidad y confiabilidad en la integración de la CMDB. La implementación contempla la configuración inicial del esquema de la CMDB, la definición de clases y atributos de CI, la integración con Service Desk Manager y fuentes externas de inventario, así como la validación de seguridad y control de acceso, garantizando que los datos críticos de la infraestructura se gestionen bajo las políticas corporativas y estándares definidos por la organización.

Se contempla la implementación inicial de la CMDB en el ambiente de pruebas como primera fase, donde se aplica la actualización a 17.4.4.0 (RU4) y se configura el modelo de datos, se cargan los primeros elementos de configuración y se valida la integración con Service Desk Manager y los procesos de gestión de servicios. En esta etapa se ejecutan respaldos de la base MDB, se revisan los prerequisitos técnicos y se definen los casos de prueba funcionales para asegurar que la CMDB refleje correctamente la infraestructura y sus relaciones, asegurando que la implementación de la CMDB junto con las mejoras de RU4 aporte trazabilidad, control y eficiencia en la gestión de servicios de TI.

SDM / Implementación de la Gestión de Problemas

Alcance: Implementación del proceso de Gestión de Problemas dentro de la plataforma CA Service Management. El objetivo principal es establecer un marco formal para la identificación, análisis y resolución de problemas recurrentes en la infraestructura de TI, asegurando la eliminación de causas raíz y la reducción de incidentes repetitivos. Con la actualización a RU4, se incorporan mejoras de seguridad como HTTP Strict Transport Security (HSTS) y optimización del SSL Configurator, además de correcciones en APIs REST/SOAP, GRLoader y procesos críticos de SDM, lo que garantiza mayor estabilidad y confiabilidad en la gestión de problemas. La implementación contempla la configuración de workflows en Service Desk Manager para el registro y seguimiento de problemas, la integración con la CMDB para relacionar elementos de configuración afectados, y la automatización de procesos mediante CA Process Automation (ITPAM), asegurando trazabilidad, control y alineación con las prácticas de ITIL y los estándares corporativos definidos por la organización.

Se contempla la implementación inicial en el ambiente de pruebas, donde se aplica la actualización a 17.4.4.0 (RU4) y se configuran los flujos de trabajo, roles y plantillas necesarias para la gestión de problemas. En esta etapa se ejecutan respaldos de la base MDB, se revisan los prerequisitos técnicos y se definen los casos de prueba funcionales para validar la correcta identificación de problemas, su relación con incidentes y CIs en la CMDB, y la ejecución de procesos automatizados en ITPAM. Una vez validada la operación integral en pruebas —incluyendo la creación, análisis y resolución de problemas, así como la generación de reportes asociados— se procede a planificar la migración hacia el ambiente de producción, asegurando que la implementación de la Gestión de Problemas junto con las mejoras de RU4 aporte estabilidad, eficiencia y valor agregado en la gestión de servicios de TI.

SDM / Implementación Incidentes de Seguridad

Alcance: Implementación del proceso de gestión de Incidentes de Seguridad dentro de la plataforma CA Service Management. El objetivo principal es establecer un marco formal para el registro, clasificación, análisis y resolución de incidentes relacionados con la seguridad de la información, garantizando trazabilidad, control y respuesta oportuna ante eventos que puedan afectar la operación de TI. Con la actualización a RU4, se incorporan mejoras de seguridad como HTTP Strict Transport Security (HSTS) y optimización del SSL Configurator, además de correcciones en APIs REST/SOAP, GRLoader y procesos críticos de SDM, lo que asegura mayor confiabilidad en la gestión de incidentes sensibles. La implementación contempla la configuración de workflows específicos en Service Desk Manager para incidentes de seguridad, la integración con la CMDB para identificar elementos de configuración afectados, y la automatización de procesos de escalamiento mediante CA Process Automation (ITPAM), alineándose con las prácticas de ITIL y las políticas corporativas de seguridad definidas por la organización.

Se contemple la implementación inicial en el ambiente de pruebas, donde se aplica la actualización a 17.4.4.0 (RU4) y se configuran los flujos de trabajo, roles y plantillas necesarias para el registro y tratamiento de incidentes de seguridad. En esta etapa se ejecutan respaldos de la base MDB, se revisan los prerequisitos técnicos y se definen los casos de prueba funcionales para validar la correcta identificación de incidentes, su relación con CIs en la CMDB y la ejecución de procesos automatizados en ITPAM. Una vez validada la operación integral en pruebas —incluyendo la creación, clasificación, escalamiento y resolución de incidentes de seguridad, así como la generación de reportes asociados— se procede a planificar la migración hacia el ambiente de producción, asegurando que la implementación de la gestión de Incidentes de Seguridad junto con las mejoras de RU4 aporte robustez, eficiencia y valor agregado en la protección de los servicios de TI.

SDM / Implementación flujo de tareas en requerimientos.

Alcance: Implementación del flujo de tareas en requerimientos dentro de la plataforma CA Service Management. El objetivo principal es optimizar la gestión de solicitudes mediante la definición y automatización de tareas asociadas a cada requerimiento, garantizando trazabilidad, control y cumplimiento de los procesos de atención. Con la actualización a RU4, se incorporan mejoras de seguridad como HTTP Strict Transport Security (HSTS) y optimización del SSL Configurator, además de correcciones en APIs REST/SOAP, GRLoader y procesos críticos de SDM, lo que asegura mayor estabilidad y confiabilidad en la ejecución de flujos de tareas. La implementación contempla la configuración de workflows en Service Desk Manager y Service Catalog, la integración con la CMDB para relacionar elementos de configuración afectados, y la automatización de procesos mediante CA Process Automation (ITPAM), alineándose con las prácticas de ITIL y los estándares corporativos definidos por la organización.

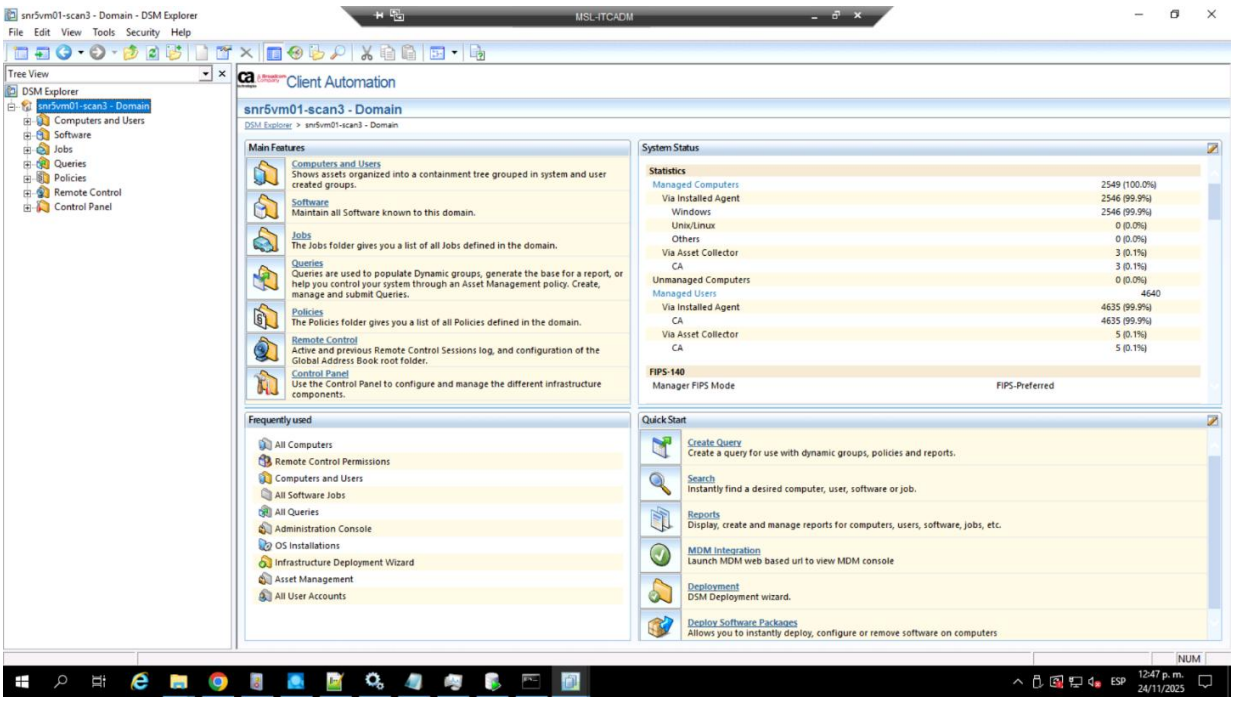
Se contempla la implementación inicial en el ambiente de pruebas, donde se aplica la actualización a 17.4.4.0 (RU4) y se configuran los flujos de trabajo, roles y plantillas necesarias para la gestión de tareas dentro de los requerimientos. En esta etapa se ejecutan respaldos de la base MDB, se revisan los prerequisitos técnicos y se definen los casos de prueba funcionales para validar la correcta creación, asignación, seguimiento y cierre de tareas asociadas a requerimientos. Una vez validada la operación integral en pruebas —incluyendo la trazabilidad de tareas, la integración con CIs en la CMDB y la ejecución de procesos automatizados en ITPAM— se procede a planificar la migración hacia el ambiente de producción, asegurando que la implementación del flujo de tareas en requerimientos junto con las mejoras de RU4 aporte eficiencia, control y valor agregado en la gestión de servicios de TI.

DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

6. **ITCA. CA Client Automation.** Es una plataforma integral de gestión, administración y automatización del ciclo de vida de dispositivos y endpoints dentro de una organización, incluyendo computadores, laptops, servidores y equipos remotos. Lo que hace ITCA es centralizar y automatizar tareas críticas como inventario, distribución de software, aplicación de parches, control remoto y cumplimiento de políticas, garantizando que todos los dispositivos estén actualizados, seguros y operativos sin intervención manual constante.

   ITCA aporta un valor significativo al permitir una operación más eficiente, reducción de costos operativos, mejoras en seguridad, menor intervención del personal técnico y una gestión unificada, incluso en entornos distribuidos o con usuarios remotos.

   Permite la gestión centralizada de los recursos informáticos, incluida la implementación de software, parches y la gestión de activos.



DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

Plan de trabajo:

ITEM	Iniciativas	Actividades	Total de horas / Tareas	112 / Vobo Priorización cliente
1	Preparación y Despliegue	Despliegue de Nuevas Licencias de ITCA	Sesiones semanales de seguimiento y apoyo. Revisión de Logs de despliegue	21,0
2		Levantamiento de Información	Sesión de levantamiento de información	1,0
9		Prerre	Revisión de Prerrequisitos - Hardware- Software - Comunicación	1,0
10			Configuración de Servidores - Hostname - Dominio	0,0
11			Instalación de Agente y Servicio de Servidor de Escalabilidad	4,0
12			Actualización a CU 7	1,0
13			Pruebas Funcionales	1,0
14			Balanceo de carga de Agentes en Servidores de Escalabilidad	1,0
15		Optimización de Motores de Procesamiento	Revisión de Engine Existentes - Solicitud de aumento de RAM Servidor Domain Manager	1,0
16				0,0
17			Creación y Configuración de Motores de Procesamiento de Información	3,0
18		Creación de Grupos Organizacionales	Creación de 100 queries para Grupos Organizacionales	1,0
19			Creación de 100 Grupos Organizacionales	1,0
20		Actualización de Documentación Existente	Actualización Manual Administrador Actualización Manual Remote Control Actualización Manual Web Console Patch Manager	5,0
21	Automatización y Configuración	Levantamiento de Información	Sesión levantamiento Información - Grupos Seguridad- Permisos - Reportes - Politicas	1,0
22		Creación de Grupos de Seguridad	Creación de Grupos de Seguridad en DA	0,0
23			Verificación de Grupos de Seguridad Existentes en DA	0,0
24			Configuración de Grupos de Seguridad y permisos en Perfiles de Seguridad de ITCA	3,0
25		Creación y automatización de Reportes	Creación - Personalización de 5 Reportes según Requerimiento SNR	8,0
26				0,0
27		Implementación de Políticas de Automatización	Creación de Políticas de Automatización	4,0
28				0,0
29			Pruebas Funcionales	1,0
30		Monitoreo de Usabilidad de Software	Creación y Configuración de Firmas Personalizadas	1,0
31				0,0
32			Creación de Collect Taks de Usabilidad de Software	3,0
33				0,0
34			Manual de Uso y Configuración	4,0
35	Catalogo y Servicios	Levantamiento de Información	Sesión levantamiento Información - Paquetes de Software - Creación de Tickets	1,0
36		Creación de Paquetes de Software	Creación de Paquetes de Software	3,0
37			Pruebas de despliegue de paquetes	1,0
38		Integración ITCA - SDM Creación deTickets	Configuración Servidor SDM	1,0
39				0,0
40			Pruebas Funcionales	1,0
41		Actualización Documentación	Manual de Creación y Despliegue de Software	1,0
42			Actualización Memoria Tecnica de Arquitectura	1,0
43	Actualización y Configuración	Levantamiento de Información	Sesión levantamiento Información - Software - Usuarios - Grupos	1,0
44		Parametrización del Modulo de Autoservicio de Software	Asignación de los Paquetes a los grupos Organizacionales	1,0
45		Actualización a Nueva Versión 14.6	Detención de Servicios	1,0
46			Backup Base de Datos	0,0
47			SnapShot servidores existentes Domain Manager y Servidores de escalabilidad	0,0
48			Copia de seguridad configuraciones, WAC, WEB Console, OSIM	3,0
49			Instalación de 14.6	5,0
50			Pruebas funcionales en el DM	3,0
51			Despliegue Actualización 14.6 hacia servidores de escalabilidad	4,0
52			Pruebas funcionales en los SS	3,0
53			Despliegue de actualización a los Agentes	3,0
54			Creación política despliegue automático	1,0
55			Pruebas finales.	3,0
56		Actualización Documentación	Actualización Memoria Técnica Instalación 14.6	2,0
57			Actualización Manual Administrador	4,0
58			Actualización Manual Remote Control	1,0
59			Actualización Manual Web Console Patch Manager	1,0
60			Actualización Memoria Tecnica de Arquitectura	1,0

ITCA / Despliegue de Agentes IT Client Automation.

Implementación gradual de 2.000 licencias adicionales, alcanzando un total de 5.500 agentes.

Alcance: Instalación del agente en estaciones y servidores objetivo, validación de conectividad, verificación de inventario y confirmación del estado operativo del agente.

- Despliegue por grupos organizacionales (sedes/unidades) en ciclos semanales o quincenales.
- Validación post-instalación, revisión de errores comunes y bloqueantes.
- Monitoreo de la tasa de éxito y análisis de fallas.

DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

ITCA / Ampliación de la Infraestructura de Escalabilidad.

Alcance: Aprovisionamiento e instalación de 3 nuevos servidores de escalabilidad para soportar los 5.500 agentes proyectados. Evitar sobrecarga de la plataforma y mantener tiempos adecuados de escaneo y respuesta.

- Solicitud y gestión del requerimiento técnico (hardware/software).
- Instalación de los servidores de escalabilidad.
- Configuración de motores y procesos propios del Scalability Server.
- Balanceo de carga y redistribución de agentes.

ITCA / Actualización de ITCA a la versión 14.6

Migración hacia la versión 14.6, prevista para implementarse aproximadamente seis meses después de su lanzamiento oficial.

Alcance: Mantener la plataforma actualizada, mejorar rendimiento y seguridad, y asegurar compatibilidad futura.

ITCA / Creación de Grupos Organizacionales

Alcance: Segmentación de agentes por unidad, sede o función para facilitar la gestión y los reportes.

- Mapeo y validación de las 190 ORIP y dependencias centrales.
- Definición de una nomenclatura estándar para los grupos.
- Creación de queries y grupos organizacionales.

ITCA / Creación de Grupos de Seguridad

Alcance: Implementación de grupos en Active Directory para asignar roles y permisos dentro de ITCA. Roles: Administración, despliegue de software, soporte remoto, reportes.

- Construcción de matriz de permisos por rol.
- Creación de grupos en AD y asociación con roles dentro de ITCA.

ITCA / Automatización y Configuración

- **Implementación de Políticas Automatizadas Descripción:** Implementar al menos 5 políticas basadas en consultas, software o eventos.
- **Optimización de Motores de Procesamiento:** Ajuste de engines para mejorar desempeño y eficiencia en la recolección de inventarios.
- **Creación de Reportes Personalizados:** Desarrollo de 5 reportes (Inventario de software, estado de despliegues, estado de agentes, uso de aplicaciones críticas, sesiones de control remoto).
- **Automatización de Reportes:** Programación automática diaria/semanal/mensual de los reportes personalizados.
- **Monitoreo de Usabilidad de Software:** Activación de métricas de uso para al menos dos aplicaciones priorizadas para generar reportes con información de uso real.

DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

ITCA / Catalogo y Servicios

- **Creación de Paquetes de Software:** Desarrollo de 5 paquetes de software para autoservicio, políticas de despliegue y gestión operativa.
- **Activación del Módulo Software Delivery Catalog:** Habilitación del catálogo de autoservicio para instalación o desinstalación de software por parte del usuario final.
- **Integración ITCA–SDM para Creación Automática de Tickets:** configuración de disparadores de tickets automáticos en SDM. Para: Fallas en instalación de paquetes, detección de software no autorizado y agentes en estado crítico o inactivo.

7. **IM. CA DX Infrastructure Management (DX NetOps):** Es una plataforma unificada de monitoreo, observabilidad y gestión proactiva de la infraestructura TI que supervisa en tiempo real servidores, redes, bases de datos, aplicaciones, nubes y dispositivos críticos; lo que hace IM es detectar fallas y degradaciones antes de que impacten al negocio, generar alertas inteligentes, correlacionar eventos, automatizar acciones de remediación, visualizar KPIs en dashboards, analizar capacidad y experiencia del servicio, e integrarse con herramientas como SDM para la creación automática de incidentes y el seguimiento end-to-end.

   Sus funcionalidades clave incluyen monitoreo en tiempo real, alertamiento y priorización, correlación y diagnóstico, automatización, gestión de capacidad, observabilidad de servicios, soporte multicloud y multiplataforma, y operación integrada con Service Desk. Para el cliente, IM genera un alto valor al reducir tiempos de caída y MTTR, anticipar fallas, optimizar costos operativos y capacidad, mejorar la eficiencia del equipo TI, aumentar la disponibilidad de servicios, y garantizar continuidad del negocio con decisiones basadas en datos.

   Esencial para monitorear y gestionar la infraestructura de TI de manera proactiva, identificando y resolviendo problemas antes de que afecten a los usuarios finales.

DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

Plan de trabajo:

ITEM	Total de horas / Actividad	327 / Vobo Priorización cliente
1	**Actualizacion DX Spectrum**	0
2	Descarga de medios de instalacion Spectrum	2
3	Copia de Seguridad Servidor SpectroServer - Snapshot Vmware	2
4	Copia de Seguridad Servidor OneClick Snapshot Vmware	2
5	Copia de Seguridad Catalogo y modelos	3
6	Copia de Seguridad Base de Datos de Reportes	3
7	Copia de Seguridad Base de Datos DDM	3
8	Upgrade Rol SpectroServer 23.3.13 a 24.x	5
9	Upgrade Rol OneClick y Spectrum Reporting 23.3.13 a 24.x	3
10	Tareas Post-Upgrade SpectroServer	3
11	Tareas Post-Upgrade OneClick	3
12	Subir Servicios de la aplicación	1
13	Pruebas de Accesos Aplicación	1
14	**Actualizacion DX Performance Management**	0
15	Descarga de los medios de instalacion para el Upgrade	2
16	Instalacion y/o Actualizacion de paquetes Linux: dialog, mcelog, zip, unzip, chrony, libcap, fontconfig, libaio, libaio-devel, numactl-libs, wget, ncurses-libs,	3
17	snapshots del servidor Data Repository	2
18	snapshots del servidor Data Aggregator	2
19	snapshots del servidor Data Collector	2
20	snapshots del servidor NetOps Console	2
21	Copia de Medios en Servidor Data Repository	1
22	Copia de Medios en Servidor Data Aggregator	1
23	Copia de Medios en Servidor Collector	1
24	Copia de Medios en Servidor NetOps Console	1
25	Copia de Seguridad Base de Datos Vertica	3
26	Copia de Seguridad Configuraciones Data Aggregator	2
27	Copia de Seguridad Configuraciones NetOps Console	3
28	Actualizacion Aplicación NetOps Console	3
29	Actualizacion Aplicación Data Repository	3
30	Actualizacion Aplicación Framework Data Aggregator	2
31	Actualizacion Aplicación Collector	2
32	Forzado de Sincronizacion de Datos	2
33	Labores Post-Upgrade	3
34	Validacion de la actualizacion NetOps Portal	1
35	Validacion de la actualizacion Data Repository	1
36	Validacion de la actualizacion Data Aggregator	1
37	Validacion de la actualizacion Data Collector	1
38	**Actualizacion DX NFA Analizador de Trafico**	0
39	Descarga de medios de instalacion Harvester y Consola	2
40	Copias de seguridad Snapshot VMware NFA	2
41	Copia de seguridad Base de datos Harvester	3
42	Copia de seguridad Base de datos Console	3
43	Configuracion de prerrequisitos para la instalacion	2
44	Actualizacion Harvester	3
45	Actualizacion NFA Console	3
46	sincronozacion integracion con NetOps Console	2
47	Pruebas de funcionamento	1

DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

48	**MONITOREO DE DISPOSITIVOS DE COMUNICACIONES DE LOS CANALES DE INTERNET**	0
49	Listado de los dispositivos de comunicaciones data center principal	0
50	Listado de los dispositivos de comunicaciones data center externo	0
51	Descubrimiento en CA Spectrum Dispositivos de comunicaciones Data center principal	2
52	Descubrimiento en CA Spectrum Dispositivos de comunicaciones Data center externo	2
53	Descubrimiento en DX NetOps Dispositivos de comunicaciones Data center principal	2
54	Descubrimiento en DX NetOps Dispositivos de comunicaciones Data center externo	2
55	Agrupacion en Global Collection	1
56	Asignacion de Llave de seguridad y control de acceso	1
57	Creacion de Politica de notificacion	1
58	Creacion de Grupo NetOps	1
59	Creacion de menu	1
60	Creacion de Dashboard	2
61	Creacion de Perfil	1
62	**Monitoreo Y Ajustes Servidores Exalogic**	0
63	Listado de Servidores de Exalogic	0
64	Redescubrmiento y validacion en dispositivos Spectrum	2
65	actualizacion Agrupacion en Global Collection	2
66	ajustes de la linea base de monitoreo (CPU-MEM)	2
67	Creacion de monitoreo procesos criticos	2
68	Creacion de Politica de notificacion	1
69	Redescubrimiento y validacion enDX NetOps	2
70	Creacion de Grupo NetOps	2
71	Creacion de menu	2
72	Creacion de Dashboard	3
73	Creacion de Perfil	2
74	**Monitoreo Y Ajustes Tableros de Control y Sevicios actualizados**	0
75	Levantamiento de Informacion de Servicios	6
76	Actualizacion Tablero de Control Dispositivos	15
77	Actualizacion Tablero Servicio SIR	6
78	Actualizacion Tablero Servicio VUR	8
79	Ajustes en modelos de servicios SISG	6
80	Ajustes en modelos de servicios Portal Web	6
81	Ajustes en modelos de servicios SIDT	6
82	Ajustes en modelos de servicios VUR	9
83	Ajustes en modelos de servicios SIR	9
84	Ajustes en modelos de servicios Portales aplicaciones	5
85	**Integracion DX Spectrum casos en Service Desk**	**0**
86	Integracion ServiceDesk con Spectrum	6
87	Definicion de Plataforma que abre Incidentes	6
88	Creacion de plantillas de Incidentes	6
89	Creacion de Policias de Incidente	6
90	Creacion de Tipos de Problemas	6
91	Creacion de Filtros de alarmas	6
92	Creacion de Script de alarmas	8
93	Configuracion de Integracion CMDB-Spectrum	3
94	Creacion de Script exportacion de CI en Spectrum	3
95	Creacion de politica de Exportacion a CMDB	3
96	**Monitoreo Orientado al Servicio**	**0**
97	Levantamiento de Informacion de Servicios Servicios	6
98	Creacion de modelo de Servicio OSB	0
99	Creacion de modelo de Servicio Content	0
100	Creacion de modelo de Servicio Nodo Central	0
101	Creacion de modelo de Servicio Nodo Sara	0
102	Creacion de monitores para Procesos Capa Media 4 Apps	0
103	Creacion de monitores para Servidores DBs 4 Apps	0
104	Creacion de monitores para puertos 4 Apps	0
105	Creacion de monitores para Portales Web Aplicaciones 4 Apps	0

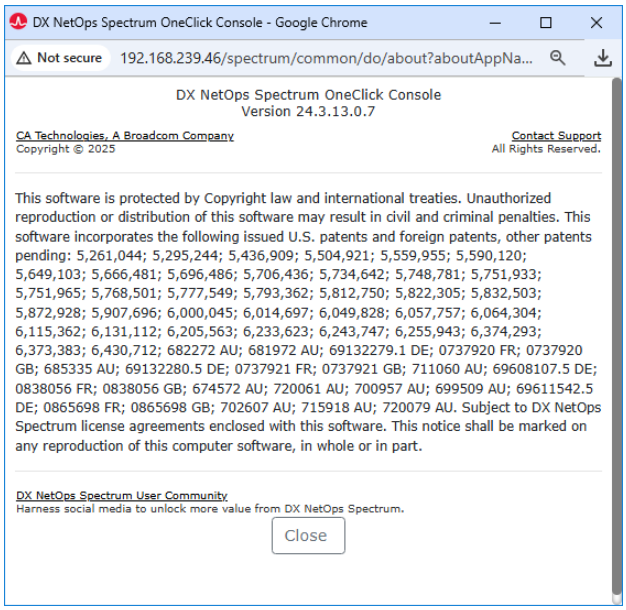
DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

106	**Monitoreo URLs Aplicaciones Servicios de Negocio**	0
107	Entrega de Listado de URLs de las aplicaciones	0
108	Configuracion de Prerrequisitos de conectividad para las URLs	3
109	Configuracion de Perfiles de Descubrimiento	3
110	Creacion de Grupo de URLs	1
111	Creacion de Reglas de Notificacion	2
112	Creacion de Grupo en NetOps	2
113	Creacion de Tablero de Control de URLs NetOps	3
114	Configuracion de perfiles de Acceso	2
115	**Monitoreo Servidores Oracle**	0
116	Listado de Servidores de Oracle	0
117	Redescubrmiento y validacion en dispositivos Spectrum	2
118	actualizacion Agrupacion en Global Collection	2
119	ajustes de la linea base de monitoreo (CPU-MEM)	2
120	Creacion de monitoreo procesos criticos	2
121	Creacion de Politica de notificacion	1
122	Redescubrimiento y validacion enDX NetOps	2
123	Creacion de Grupo NetOps	2
124	Creacion de menu	2
125	Creacion de Dashboard	3
126	Creacion de Perfil	2
127	**Monitoreo Dispositivos Solucion de Backup**	0
128	Listado de los dispositivos de Backup	0
129	Compilacion de Archivos de MIBs	3
130	Descubrimiento en CA Spectrum Dispositivos	2
131	Descubrimiento en DX NetOps Dispositivos	2
132	Agrupacion en Global Collection	1
133	Asignacion de Llave de seguridad y control de acceso	1
134	Creacion de Politica de notificacion	1
135	Creacion de Grupo NetOps	1
136	Creacion de menu	1
137	Creacion de Dashboard	2
138	Creacion de Perfil	1
152	**Documentacion**	0
153	Documento actualizacion Spectrum	3
154	Documento actualizacion DX NetOps Performance	3
155	Documento actualizacion NFA	3

IM / Actualización Soluciones de Software Observabilidad

Alcance: La actualización continua de las versiones del Software garantiza acceder a soporte continuo por parte del fabricante, ya que las versiones antiguas de productos van perdiendo el soporte y para su atención de incidentes fabrica solicita estar en las últimas versiones de producto, además las últimas versiones de producto corrigen y/o amplían funcionalidades según sus características. La solución de Observabilidad de DX Spectrum va de la versión 23.3.13 a la versión 24.3.13.

DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.



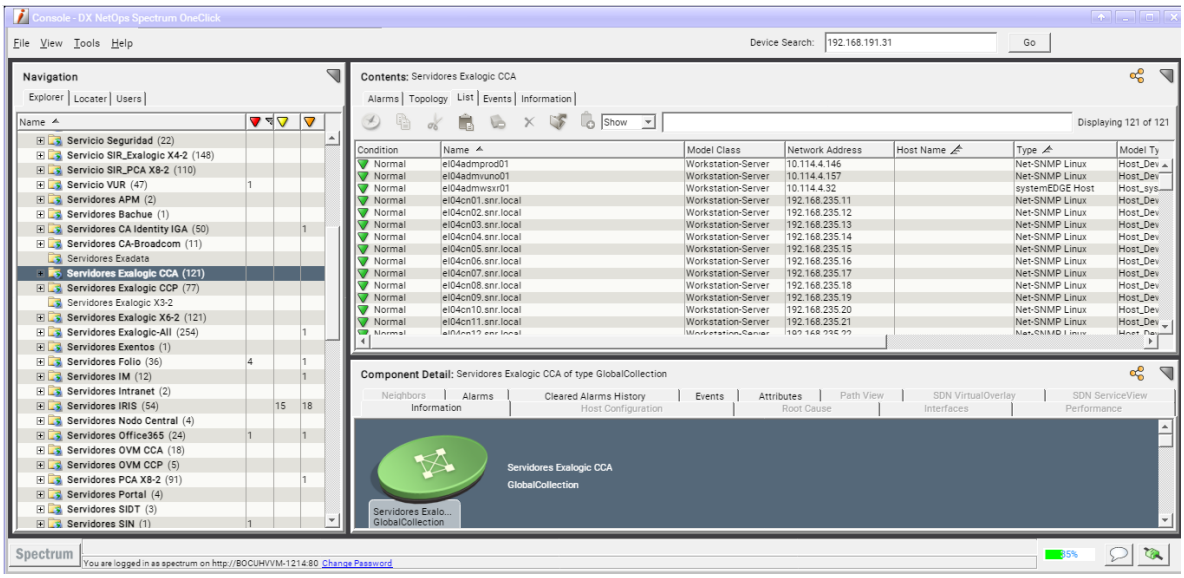
IM / Monitoreo de Dispositivos de Comunicaciones de los Canales de Internet

Alcance: Los canales de Datos y Canales de Internet es un servicio ofrecido por un tercero, dicho servicio es un componente crítico y cualquier falla o intermitencia del servicio compromete la prestación de los servicios misionales de la entidad, por lo anterior es primordial garantizar el monitoreo continuo de dichos canales.

IM / Monitoreo y Ajustes Servidores Exalogic

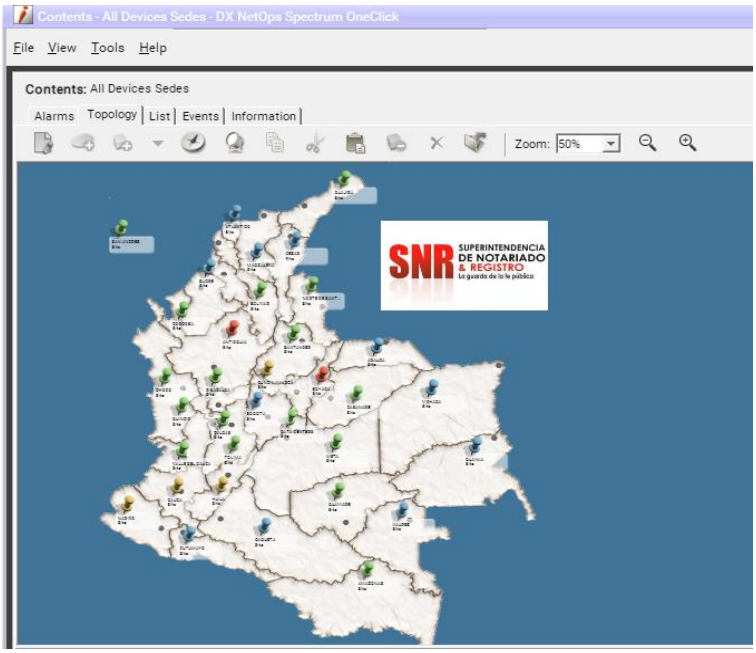
Alcance: La plataforma conjunta de los servicios de almacenamiento, aplicaciones y servicios de infraestructura conexos de los Exalogic es una parte fundamental que soporta las aplicaciones críticas de la entidad; por lo anterior se hace indispensable garantizar un monitoreo continuo sobre dicha plataforma. Configuraciones necesarias para realizar el descubrimiento y monitoreo de los elementos de la plataforma de Exalogic

DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

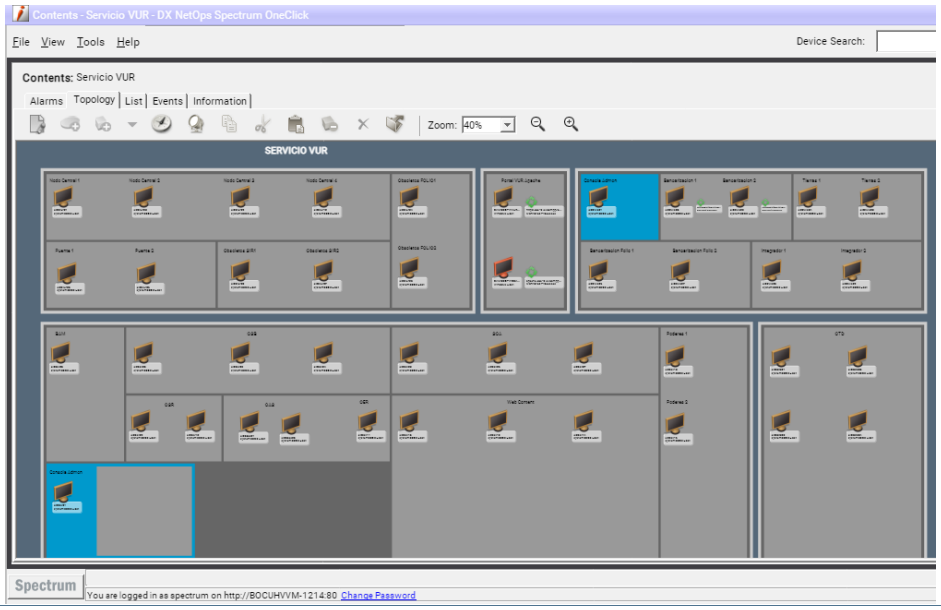


IM / Monitoreo y Ajustes Tableros de Control y Servicios actualizados

Alcance: Mejora y ajuste de la capa de presentación de los diferentes tableros de control que representan las diferentes plataformas monitoreadas, ya que debido a los diferentes cambios por renovación tecnológica y/o actualizaciones en las diferentes aplicaciones a menudo se deben de ajustar los tableros de control en donde se ofrece la capa de Observabilidad de la aplicación.



DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.



All Groups

Overview vServers Exalogic PCA X8-2

Last Hour | Today 12:58 PM to 1:58 PM

Table Average - Memory

Site: vServers Exalogic PCA X8-2

Timeframe: Last Hour Metric Calculate Level: by Device Resolution: As Polled Data

Critical Status Major Status Minor Status Normal Status

Quick Filter

Group/Device Name	Utilization - Average	Total - Average	Used - Average	Free - Average	Utilization - Minimum	Utilization - Maximum
vServers Exalogic PCA X8-2	40.45%	31.9 GB	14.7 GB	17.1 GB	2.89%	99.67%
ovcamn06r1	99.61%	376.1 GB	374.6 GB	1.5 GB	99.52%	99.67%
el03sv12	98.1%	47.3 GB	46.4 GB	919.7 MB	98.03%	98.26%
el03otd03	92.93%	11.7 GB	10.9 GB	847.2 MB	92.51%	93.29%
el03otd04	83.83%	11.7 GB	9.8 GB	1.9 GB	83.45%	84.19%

5 per page | Page 1 of 20 | Displaying 1 - 5 of 98

All Groups

Servicio SIR_PCA X8-2

Last Hour | Today 12:59 PM to 1:59 PM

Table Average - CPU

Site: Servicio SIR_PCA X8-2

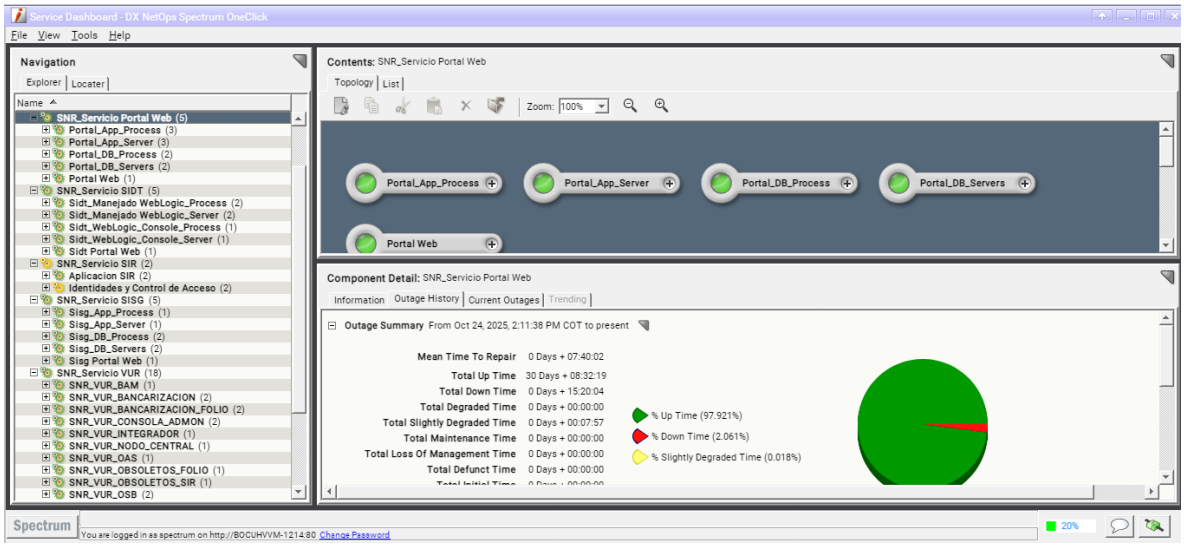
Timeframe: Last Hour Metric Calculate Level: by Device Resolution: As Polled Data

Critical Status Major Status Minor Status Normal Status

Quick Filter

Group/Device Name	Utilization - Average	Utilization - Minimum	Utilization - Maximum
Servicio SIR_PCA X8-2	4%	0.07%	52.93%
el03sir01.snr.local	18.06%	0.99%	52.93%
el04sir07	8.48%	1.35%	18.4%
el03sir02.snr.local	4.95%	0.81%	15.22%
el03sir04.snr.local	4.38%	0.46%	15.34%
el03sir06.snr.local	3.95%	1.51%	10.85%
el03sir05.snr.local	2.8%	1.04%	9.21%
el03sir08.snr.local	2.45%	0.95%	6.38%
el03sir03.snr.local	2.37%	0.81%	5.99%
el04sir09.snr.local	0.39%	0.08%	1.89%

10 per page | Page 1 of 2 | Displaying 1 - 10 of 13



IM / integración DX Spectrum casos en Service Desk

Alcance: La solución de Observabilidad al tener un monitoreo en línea permite identificar las fallas sobre la plataforma de Infraestructura y aplicaciones de una forma inmediata, permitiendo registrar dichos eventos críticos en la mesa de servicios, con lo anterior se logra obtener un registro automático que permite no solo registrar el caso de soporte en SDM si no que lo asigna al responsable de atender el incidente para lograr una atención inmediata para la resolución de los incidentes

IM/ Monitoreo Orientado al Servicio

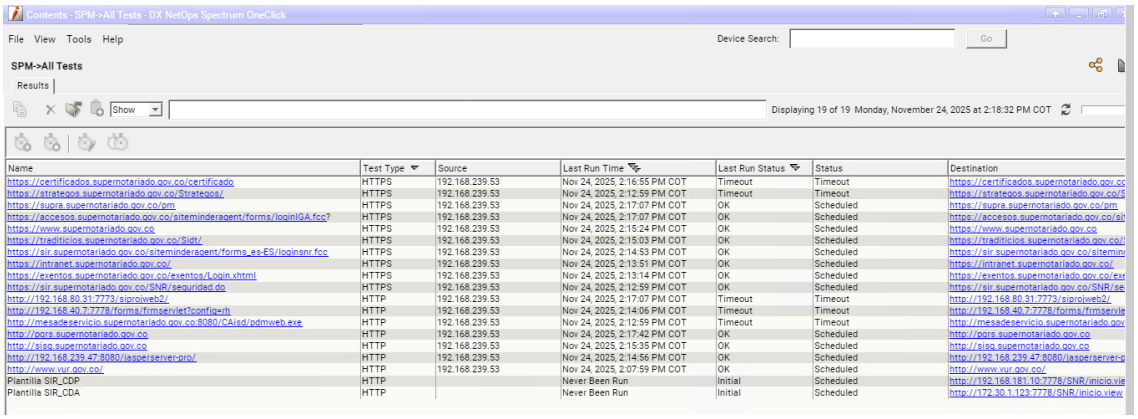
Alcance: La solución de Observabilidad permite tener una identificación de todos aquellos Items de configuración de los servicios, de tal forma que con una medición de disponibilidad conjunta permite medir todo el servicio como un único componente y generar indicadores precisos para conocer cuando el servicio de alguna aplicación critica se encuentra fuera de servicio.

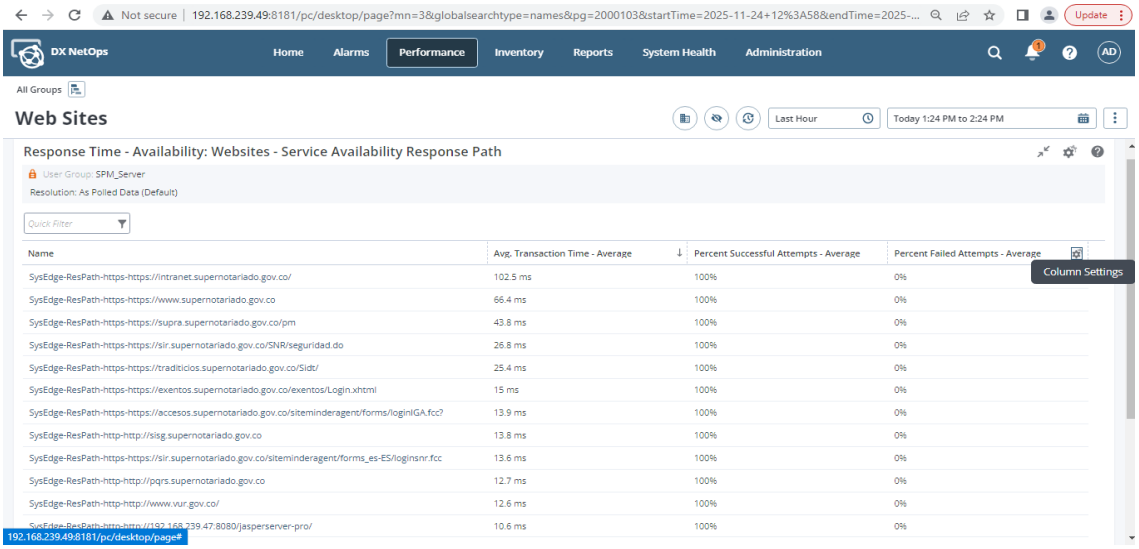
IM / Monitoreo URLs Aplicaciones Servicios de Negocio

Alcance: Los servicios Web de las aplicaciones se constituyen en capa de presentación para el acceso de todos los servicios tecnológicos que ofrece la entidad, dichas URLs al no estar monitoreas dejan sin Observabilidad a nivel de disponibilidad a los administradores de las plataformas y a los gestores de servicios tecnológicos, es por lo anterior primordial garantizar un monitoreo continuo sobre dichos portales Web de las aplicaciones. Se tiene un cubrimiento de URLs criticas consideradas por la entidad.

Portales Web Monitoreados.

DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.





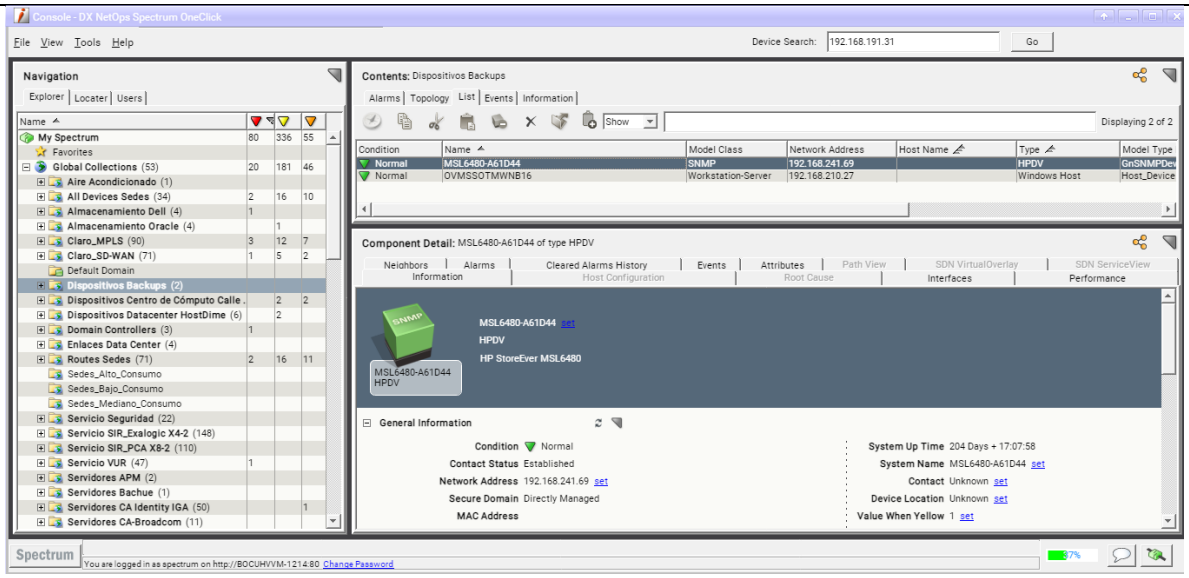
IM / Monitoreo Servidores Oracle

Alcance: Los servidores de las bases de datos permiten que las aplicaciones críticas de negocio almacenen los datos propios de cada aplicación, dichos servidores son componentes críticos que requieren un monitoreo continuo que garantice tomar acciones rápidas e inmediatas cuando se presenten fallas en dicha plataforma.

IM / Monitoreo Dispositivos Solución de Backup

Alcance: La plataforma de Backups garantiza obtener copias de seguridad, la cuales deben de estar disponibles para ser restauradas en caso que presentarse incidentes que comprometan la disponibilidad, seguridad e integridad de la información, por lo anterior es primordial garantizar un monitoreo continuo sobre la infraestructura de Backup que informe cuando dicha plataforma presente fallas que impidan su funcionamiento.

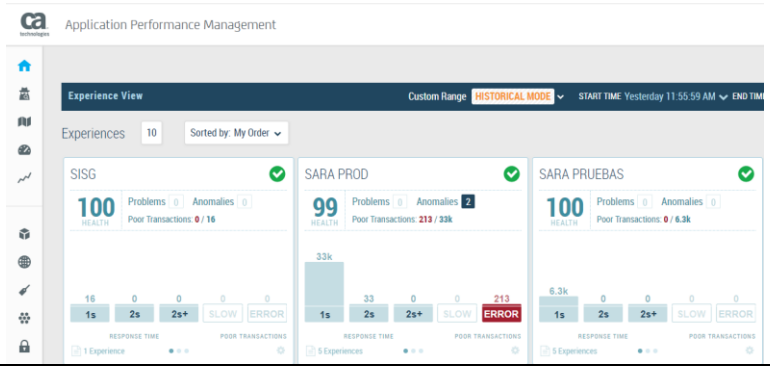
DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.



8. **APM. CA Application Performance Management:** Es una plataforma de monitoreo y gestión del rendimiento de aplicaciones que permite visualizar en tiempo real la disponibilidad, tiempos de respuesta, errores y transacciones de servicios críticos; lo que hace APM es detectar y alertar de manera proactiva sobre lentitud, fallas y cuellos de botella, mapear dependencias, analizar causa raíz, monitorear la experiencia del usuario final, automatizar acciones de remediación, trazar transacciones extremo a extremo, generar dashboards y KPIs, integrarse con SDM para crear incidentes automáticamente y soportar entornos on-premise, cloud, microservicios y contenedores.

   Sus funcionalidades clave incluyen monitoreo en tiempo real, alertamiento inteligente, diagnóstico y trazabilidad, mapeo de arquitectura, analítica y paneles ejecutivos, automatización, experiencia del usuario e integración con Service Desk. Para la organización, APM genera alto valor al reducir tiempos de resolución y caídas, mejorar la estabilidad y disponibilidad, prevenir fallas antes de impactar al negocio, optimizar costos operativos, elevar la experiencia digital del cliente y facilitar la colaboración entre equipos Dev, Ops y TI con decisiones basadas en datos. Permite monitorear y optimizar el rendimiento de las aplicaciones empresariales, asegurando una experiencia de usuario fluida

Actualmente están reportando las aplicaciones de API GATEWAY, SISG, SARA PRODUCCION Y SARA.



DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

Plan de trabajo:

ITEM	Total de horas	168
	Actividad	Vobo Priorización cliente
1	**Ajustes Recuperar Monitoreo SIR**	0
2	Validacion de Permisos de conexión entre App y la solución DX APM Servidores Migrados	2
3	Instalación de 11 agentes en servidor de aplicaciones Migrados	8
4	Configuración de agente en servidor de aplicaciones	3
5	Reinicio de servidor de aplicaciones	0
6	Reconfiguracion de métricas	3
7	Reconfiguracion de alertas	3
8	Reconfiguracion de tableros	3
9	Reconfiguracion de acciones	3
10	Reconfiguracion de reglas de correos	2
11	**Ajustes Recuperar Monitoreo OSB-EX4**	0
12	Validacion de Permisos de conexión entre App y la solución DX APM Servidores Migrados	2
13	Instalación de 3 agentes en servidor de aplicaciones Migrados	5
14	Configuración de agente en servidor de aplicaciones	3
15	Reinicio de servidor de aplicaciones	0
16	Reconfiguracion de métricas	3
17	Reconfiguracion de alertas	3
18	Reconfiguracion de tableros	3
19	Reconfiguracion de acciones	3
20	Reconfiguracion de reglas de correos	2
21	**Ajustes Recuperar Monitoreo CONTENT-EX4**	0
22	Validacion de Permisos de conexión entre App y la solución DX APM Servidores Migrados	2
23	Instalación de 3 agentes en servidor de aplicaciones Migrados	5
24	Configuración de agente en servidor de aplicaciones	3
25	Reinicio de servidor de aplicaciones	0
26	Reconfiguracion de métricas	3
27	Reconfiguracion de alertas	3
28	Reconfiguracion de tableros	3
29	Reconfiguracion de acciones	3
30	Reconfiguracion de reglas de correos	2
31	**Ajustes Recuperar Monitoreo NODO CENTRAL-EX4**	0
32	Validacion de Permisos de conexión entre App y la solución DX APM Servidores Migrados	2
33	Instalación de 2 agentes en servidor de aplicaciones Migrados	3
34	Configuración de agente en servidor de aplicaciones	3
35	Reinicio de servidor de aplicaciones	0
36	Reconfiguracion de métricas	3
37	Reconfiguracion de alertas	3
38	Reconfiguracion de tableros	3
39	Reconfiguracion de acciones	3
40	Reconfiguracion de reglas de correos	2

DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

41	**Ajustes Recuperar Monitoreo SIDT**	0
42	Validacion de Permisos de conexión entre App y la solución DX APM Servidores Migrados	2
43	Instalación de 2 agentes en servidor de aplicaciones Migrados	3
44	Configuración de agente en servidor de aplicaciones	3
45	Reinicio de servidor de aplicaciones	0
46	Reconfiguracion de métricas	3
47	Reconfiguracion de alertas	3
48	Reconfiguracion de tableros	3
49	Reconfiguracion de acciones	3
50	Reconfiguracion de reglas de correos	2
51	**Ajustes Recuperar Monitoreo VUR-EX4**	0
52	Validacion de Permisos de conexión entre App y la solución DX APM Servidores Migrados	2
53	Instalación de 2 agentes en servidor de aplicaciones Migrados	3
54	Configuración de agente en servidor de aplicaciones	3
55	Reinicio de servidor de aplicaciones	0
56	Reconfiguracion de métricas	3
57	Reconfiguracion de alertas	3
58	Reconfiguracion de tableros	3
59	Reconfiguracion de acciones	3
60	Reconfiguracion de reglas de correos	2
61	**Ajustes Recuperar Monitoreo API GATEWAY**	0
62	Validacion de Permisos de conexión entre App y la solución DX APM Servidores Migrados	2
63	Instalación de 2 agentes en servidor de aplicaciones Migrados	3
64	Configuración de agente en servidor de aplicaciones	3
65	Reinicio de servidor de aplicaciones	0
66	Reconfiguracion de métricas	3
67	Reconfiguracion de alertas	3
68	Reconfiguracion de tableros	3
69	Reconfiguracion de acciones	3
70	Reconfiguracion de reglas de correos	2
76	**Documentacion**	0
77	Actualizacion Manual de usuario	5

Alcance: Implementación y recuperación del monitoreo de la aplicación API Gateway dentro de la solución de observabilidad DX APM, con el objetivo de restablecer la visibilidad de transacciones, métricas críticas y alertas tras la migración de servidores.

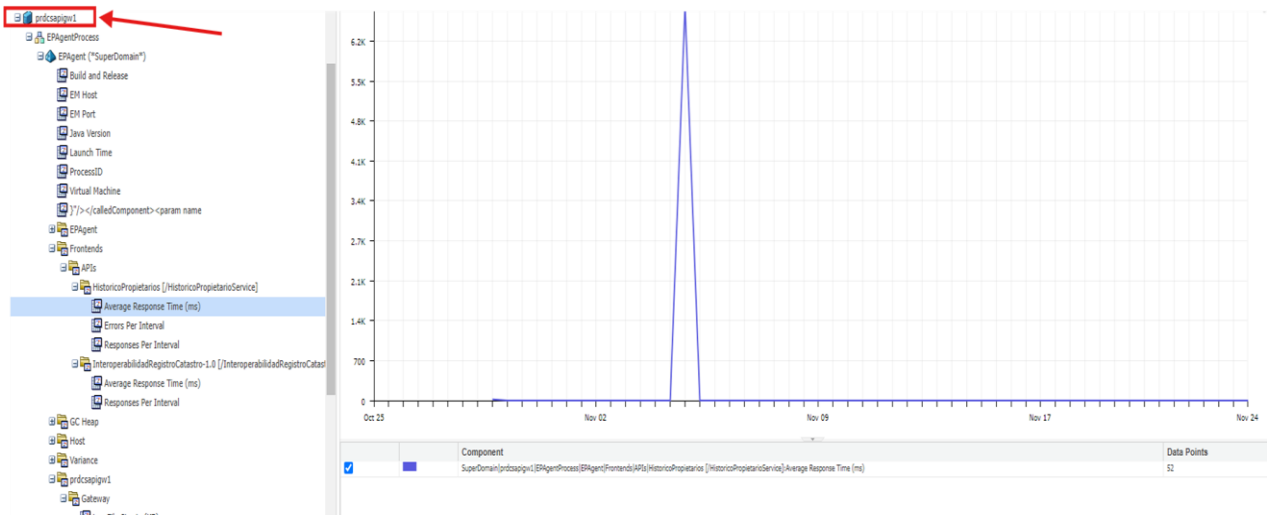
La solución mediante la instalación y configuración del Agente de CA API Gateway, captura y transfiere detalles minuciosos de las transacciones de API hacia DX APM, donde se correlacionan y se muestran junto con los datos de métricas de rendimiento. Esto permite obtener una visibilidad en tiempo real, detallada y personalizable del comportamiento de las APIs, incluyendo el seguimiento de transacciones y la medición del tiempo invertido en el servidor de aplicaciones y en los sistemas de back-end.

Para lograr esta integración, se ejecutan actividades clave como la validación de permisos de conexión entre los servidores de API Gateway y DX APM, la instalación de agentes en los servidores de API, la configuración y reinicio controlado de dichos servidores, así como la reconfiguración integral de métricas, alertas, tableros y acciones. Con ello se garantiza que el monitoreo refleje fielmente el nuevo entorno y mantenga la coherencia con las políticas de operación definidas por la organización. Adicionalmente, se valida el comportamiento de la puerta de enlace en escenarios donde las transacciones se dividen en múltiples rutas hacia sistemas de back-end, confirmando que DX APM refleje correctamente la correlación y el desempeño de cada flujo.

DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

La solución ha demostrado estabilidad y cumplimiento de los requerimientos técnicos y funcionales:

- Server **prdcsapigw1** reportando en la consola de APM



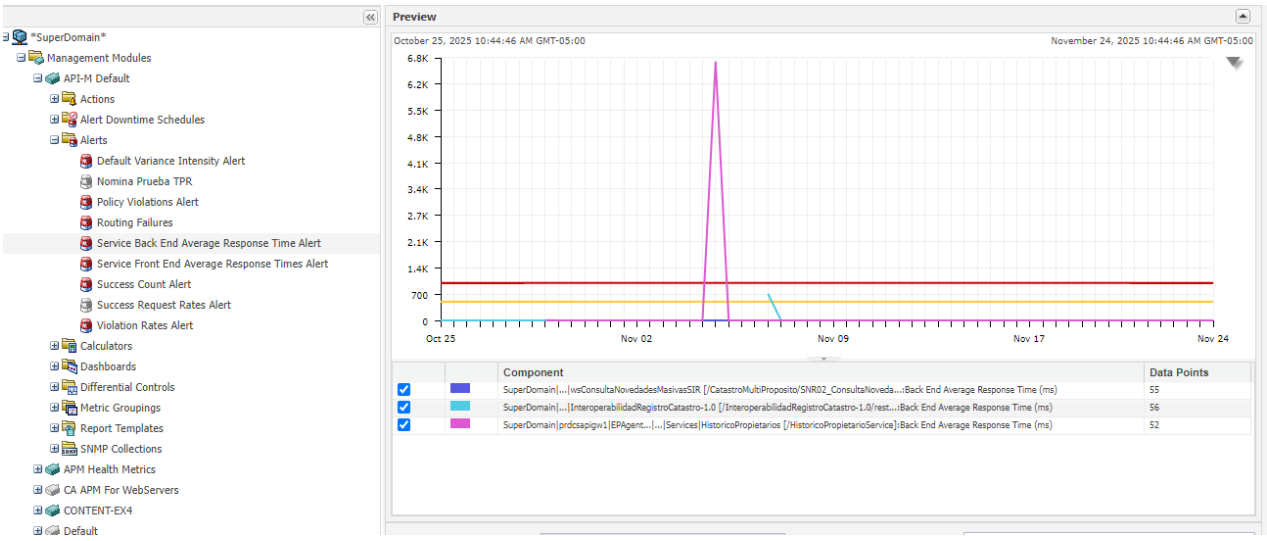


DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

- Tablero API Gateway en APM



- Alertas del módulo de API generadas en APM por el tiempo de respuesta de Backends en API Gateway.



DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

PPM. CA Clarity Core License: Clarity (PPM – Project & Portfolio Management) Es una plataforma integral que centraliza la gestión del portafolio, programas, proyectos, recursos y presupuestos, y lo que hace es permitir planificar, priorizar, ejecutar y controlar iniciativas estratégicas con visibilidad total del avance, costos, riesgos y capacidad; dentro de sus funcionalidades clave incluye la priorización y selección de proyectos, planificación y seguimiento de cronogramas, gestión y asignación de recursos, control financiero CAPEX/OPEX, dashboards y analítica, gestión de ideas y demandas, control de riesgos y cambios, flujos de trabajo y aprobaciones, soporte ágil e híbrido, e integración con sistemas corporativos. Para la organización, Clarity genera alto valor al maximizar el retorno de inversión, reducir costos y desperdicios, optimizar el uso de recursos, mejorar la toma de decisiones basada en datos, aumentar transparencia y gobernanza, acelerar la ejecución y asegurar la alineación entre negocio y TI hacia los objetivos estratégicos.

Herramienta clave para la gestión de carteras de proyectos, recursos y finanzas.

Plan de trabajo:

ITEM	Requerimientos	Actividad	Total de horas	539
			Tareas	Vobo Priorización cliente 25/11/2025
1	Prerrequisitos	Homologacion ambiente de pruebas Base de datos Clarity	Solicitud correo , homologacion de datos Produccion a Pruebas.	0,0
2			Sesión con el dba post envio de correo, para aclaración de dudas o atender el requerimiento.	1,0
3			Migrar Fyle system Produccion a pruebas	0,0
4			Migrar filestore y indexstore documentos de produccion a pruebas	0,0
5			Configurar archivo properties.xml apuntando a servidor base de datos pruebas, configuracion e IP general	1,0
6		Homologacion reporte CDP	Import reporte Solicitud CDP PDF en pruebas	3,0
7		Diseno casos de uso	Diseño y estructura del documento caso de uso Plan estrategico institucional	8,0
8			Diseño y estructura del documento caso de uso Acuerdos de Desempeño	8,0
9			Diseño y estructura del documento caso de uso Proyectos - Cadena de valor	12,0
10			Diseño y estructura del documento caso de uso Listas de chequeo	12,0
11		Documentación - Caso de Uso	Presentación caso de uso Automatizacion SIIF	5,0
12			Presentación caso de uso control Financiero generación de CDP - SIIF.	5,0
13			Ajustes Documentos	10,0
14			Presentacion Ajustes documentos casos de uso	5,0
15	Requerimiento 1 - Integracion SIIF - Desagregado y nivel decreto	Configuracion Inicial - ambiente de pruebas	Ajustes campos tipo numerico / moneda de Modulo Ejecucion Presupuestal Nivel Decreto	4,0
16			Crear campos adicionales a formato SIIF Ejecucion Presupuestal Nivel Decreto	3,0
17			Creación Modulo final inyección de datos SIIF Ejecución presupuestal Nivel Desagregado	1,0
18			Crear campos adicionales a formato SIIF Ejecución presupuestal Nivel Desagregado	3,0
19			Ajustes Campos modulo final MACRO ejecución presupuestal de gastos para inyección de datos SIIF automatizado	4,0
20			Crear Excel lógico de mapeo de atributos API SIIF DECRETO	3,0
21			Crear Excel lógico de mapeo de atributos API SIIF DESAGREGADO	3,0
22			Crear Excel lógico de mapeo de atributos API SIIF EJECUCION DE GASTOS	3,0
23			Sesión de explicación formatos mapeo atributos API para desarrollo	3,0
24			Ajustar roles y permisos sobre los nuevos componentes	4,0
25		Desarrollo lógico - ambiente de pruebas	ajustes evolutivos interfaz (mejoras/optimizaciones)	3,0
26			mapeo tabla-objeto decreto	3,0
27			mapeo tabla-objeto desagregado	3,0
28			mapeo relacion-ejecucion consolidada	3,0
29			lógica lectura/escritura decreto	5,0
30			lógica lectura/escritura desagregado	5,0
31			lógica lectura/escritura ejecución consolidada	16,0
32			integración de lógica decreto a proceso principal	3,0
33			integración de lógica desagregado a proceso principal	3,0
34		Pruebas y cierre - ambiente de pruebas	despliegue y pruebas certificación	8,0
35			Pruebas de Validación de Datos en clarity Comparar resultados del sistema automatizado vs. macro manual en Excel.	3,0
36			Pruebas de Aceptación de Usuario final	3,0
37			Aceptación del desarrollo requerimiento 1 para pase a producción	0,0
38		Configuración Inicial - ambiente de producción	Ajustes campos tipo numérico / moneda de Modulo Ejecución Presupuestal Nivel Decreto	3,0
39			Crear campos adicionales a formato SIIF Ejecución Presupuestal Nivel Decreto	1,0
40			Creación Modulo final inyección de datos SIIF Ejecución presupuestal Nivel Desagregado	1,0
41			Crear campos adicionales a formato SIIF Ejecución presupuestal Nivel Desagregado	1,0
42			Ajustes Campos modulo final MACRO ejecución presupuestal de gastos para inyección de datos SIIF automatizado	3,0
43			Ajustar roles y permisos sobre los nuevos componentes	4,0
44		Desarrollo lógico - ambiente de	Despliegue y puesta en producción	3,0
		Consumo de 21 documentos PCI +	Desarrollo para consumo de archivos planos	45,0
45		Cierre requerimiento en producción	Carga final documentos en producción por parte del usuario final	0,0
46			Aceptación del desarrollo requerimiento 1 en producción	0,0

DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

47	Requerimiento 2 - Control y seguimiento presupuestal para generación de CDP	DP - Registro de PAA y No PAA - an	Crear modulo relacionamiento directo PCI - Dependencia - RUBRO acorde a archivo levantamiento de información "Relación PCI.xlsx"	1,0
48			Crear campos relacionamiento	5,0
49			Crear lógica entre campos para mapeo automático una vez se cree o se agregue el objeto al CDP	8,0
50			Cargar datos al modulo - desarrollo plantilla api para cargue	5,0
51			Cargar datos al modulo - Ejecucion .bat de cargue	1,0
52			Crear campo PCI en modulo actual CDP asociación PAA o no PAA	1,0
53			Crear lógica de mapeo automático - crear procesos y logica de inicio	1,0
54			Crear lógica de mapeo automático - crear gel script con consulta sql server para condicion y activar proceso	5,0
55			Habilitar lógica, asociación no PAA ingreso de diferentes rubros - Eliminar procesos finalizados	1,0
56			Habilitar lógica, asociación no PAA ingreso de diferentes rubros - Editar consulta sql server y archivo xml Script Gel actual para no habilitar regla cuando tipo de CDP sea no PAA.	5,0
57			Verificar y validar procesos	1,0
58			Activar proceso	1,0
59			Ajustar lógica actual para asociación PAA solo rubros y grupos únicos - Eliminar procesos finalizados	1,0
60			Ajustar lógica actual para asociación PAA solo rubros y grupos únicos - Editar consulta sql server y archivo xml Script Gel actual para habilitar regla cuando tipo de CDP sea PAA.	8,0
61			Ajustar lógica actual para asociación PAA solo rubros y grupos únicos - Verificar y validar proceso	1,0
62			Ajustar lógica actual para asociación PAA solo rubros y grupos únicos - Activar proceso	1,0
63			Crear lógica condicional presupuestal que permita visualizar en la creación del cdp los movimientos financieros para solicitud. (Cruce información apropiación SIIF)	9,0
64			Crear lógica condicional presupuestal que permita visualizar en la creación del cdp los movimientos financieros para adición. (Cruce información CDP aprobado y registrado en SUPRA)	5,0
65			Crear lógica condicional presupuestal que permita visualizar en la creación del cdp los movimientos financieros para reducción. (Cruce información CDP aprobado y registrado en SUPRA)	5,0
66		roceso aprobación CDP - ambiente	Ajuste en proceso aprobación CDP - permitir la devolución del CDP desde la dependencia cuando haya pasado	8,0
67			Proceso control presupuestal , automatización de montos , validación de disponibilidad e información de disponibilidad - paso recurrente o proceso en CDP.	8,0
68			Paso Flujo control financiero ultima instancia de aprobación CDP- será el paso de control que valida si se descuenta o no el presupuesto con el CDP aprobado.	5,0
69			Gel Script - Desarrollo que permite aplicar la lógica matemática a los valores de apropiación para conocer estado actual presupuestal, según corte archivo cargado SIIF	8,0
70			Gel Script - Desarrollo que permite aplicar la lógica matemática a los valores de apropiación para conocer estado actual presupuestal, según corte archivo cargado SIIF	8,0
71			Ajustar roles y permisos sobre los nuevos componentes	4,0
72		Pruebas	Pruebas unitarias - creación de CDP objeto PAA y no PAA relación de PCI	4,0
73			Pruebas unitarias - verificación de saldos presupuestales acorde a lo reportado en SIIF	4,0
74			Pruebas Unitarias - Verificación de modificación de saldos presupuestales modulo ejecución SIIF para control de nuevos CDP.	4,0
75			Pruebas funcionales - Se probara todo el proceso de inicio a fin, incluyendo la configuración actual y el nuevo control presupuestal	4,0
76			Ciclo 1 - Pruebas funcionales con cliente, detallando cada uno de los controles presupuestales y finalización del proceso CDP para los 3 escenarios Solicitud, adición, reducción	5,0
77			Aceptación del desarrollo requerimiento 2 para pase a producción	0,0
78		DP - Registro de PAA y No PAA - an	Crear modulo relacionamiento directo PCI - Dependencia - RUBRO acorde a archivo levantamiento de información "Relación PCI.xlsx"	1,0
79			Crear campos relacionamiento	3,0
80			Crear lógica entre campos para mapeo automático una vez se cree o se agregue el objeto al CDP	4,0
81			Cargar datos al modulo	4,0
82			Crear campo PCI en modulo actual CDP asociación PAA o no PAA	1,0
83			Crear lógica de mapeo automático datos una vez creada la asociación	4,0
84			Habilitar lógica, asociación no PAA ingreso de diferentes rubros	4,0
85			Ajustar lógica actual para asociación PAA solo rubros y grupos únicos	4,0
86			Crear lógica condicional presupuestal que permita visualizar en la creación del cdp los movimientos financieros para solicitud. (Cruce información apropiación SIIF)	4,0
87			Crear lógica condicional presupuestal que permita visualizar en la creación del cdp los movimientos financieros para adición. (Cruce información CDP aprobado y registrado en SUPRA)	4,0
88			Crear lógica condicional presupuestal que permita visualizar en la creación del cdp los movimientos financieros para reducción. (Cruce información CDP aprobado y registrado en SUPRA)	4,0
89		roceso aprobación CDP - ambiente	Ajuste en proceso aprobación CDP - permitir la devolución del CDP desde la dependencia cuando haya pasado	4,0
90			Proceso control presupuestal , automatización de montos , validación de disponibilidad e información de disponibilidad - paso recurrente o proceso en CDP.	1,0
91			Paso Flujo control financiero ultima instancia de aprobación CDP- será el paso de control que valida si se descuenta o no el presupuesto con el CDP aprobado.	1,0
92			Gel Script - Desarrollo que permite aplicar la lógica matemática a los valores de apropiación para conocer estado actual presupuestal, según corte archivo cargado SIIF	1,0
93			Gel Script - Desarrollo que permite aplicar la lógica matemática a los valores de apropiación para conocer estado actual presupuestal, según corte archivo cargado SIIF	1,0
94			Ajustar roles y permisos sobre los nuevos componentes	3,0
95			Aceptación del desarrollo requerimiento 2 para pase a producción	3,0

DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

284	Gestion Documental	Reportes - en pruebas	Query Extracción de datos (3 reportes)	18,0
285			Cosntrucción 5 Reportes	56,0
287		Reportes - en producción	Exportar reportes jaspersoft pruebas	3,0
288			importar reportes jasperfost producción	3,0
289		Capacitacion	Material de capacitación	8,0
290			Capacitacion cargue y actualización de archivos SIIF	3,0
291			Capacitacion control financiero CDP - SIIF	5,0
291			Capacitacion procesos planeación	0,0
291		Documentación	Manual de usuario final y administrador	20,0
291			Memoria Tecnica	25,0

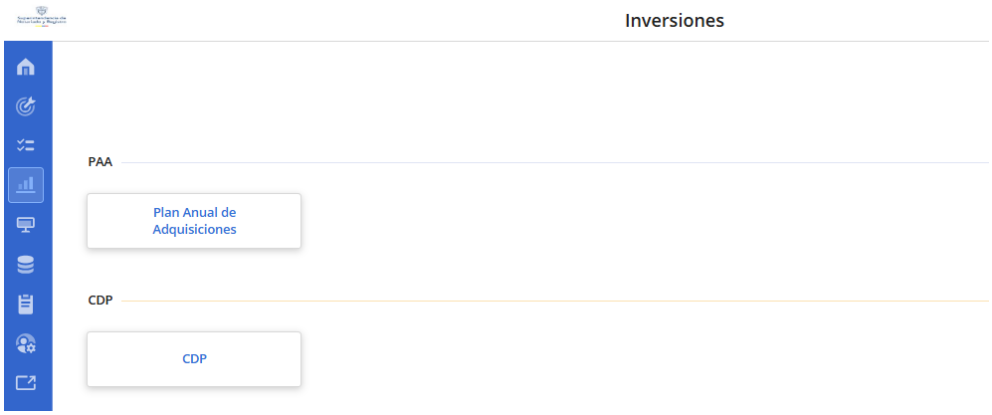
Alcance: La solución Clarity PPM (SUPRA) se encuentra implementada y en funcionamiento, garantizando la operación y ofreciendo visibilidad y gestión a las líneas del Plan Anual de Adquisiciones (PAA) en los diferentes procesos de creación, seguimiento, aprobación, modificación y eliminación.

Para esta nueva fase de implementación, se aborda la automatización del cargue financiero proveniente de SIIF. A partir de los archivos generados por SIIF y mediante un proceso de carga de archivos en Clarity, la información es procesada e inyectada en los módulos de presupuesto. Esto permite controlar y hacer seguimiento a las solicitudes de Certificados de Disponibilidad Presupuestal (CDP), proporcionando un mayor nivel de control y asegurando la disponibilidad del techo presupuestal en todo momento, lo que se traduce en una gestión financiera más precisa y eficiente.

1. MODULOS DE GESTION

En la interfaz de la página principal se muestra la vista de los siguientes módulos de:

1. Automatización SIIF
2. PCI
3. CDP



PPM/ Automatización SIIF

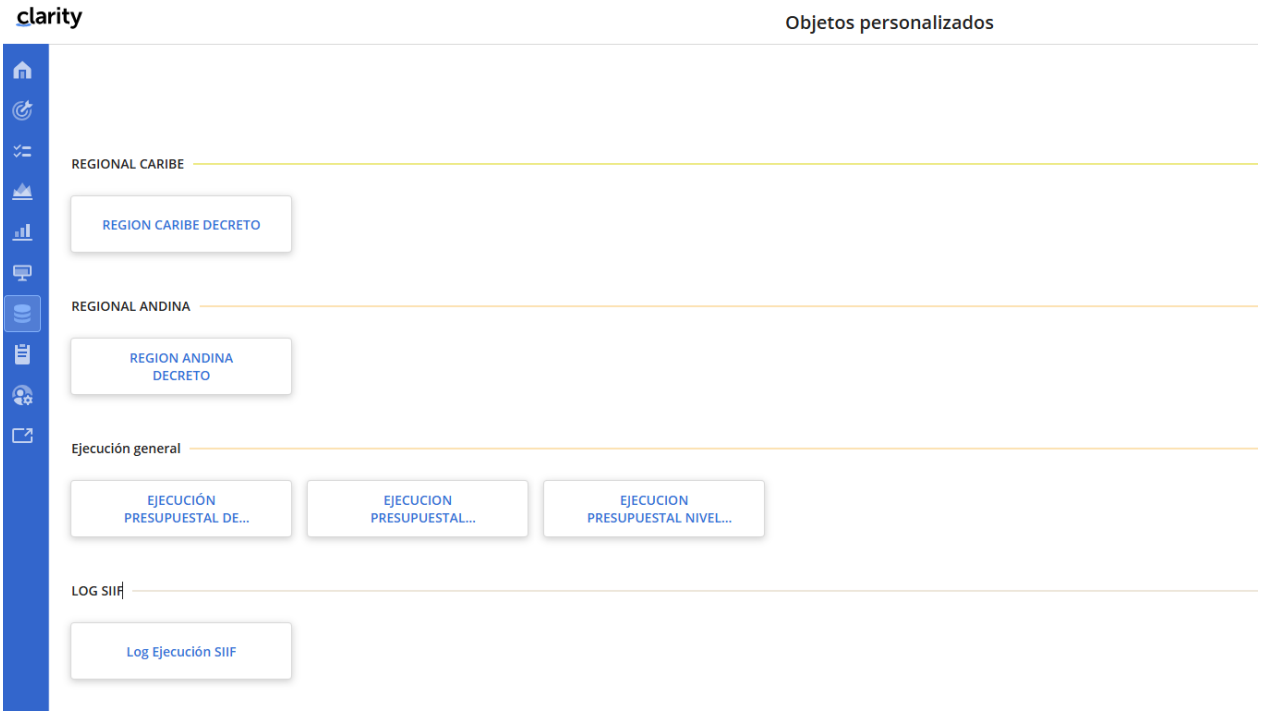
Alcance: El proceso implementado automatiza la lectura y consolidación de los archivos cargados por el área de presupuesto, eliminando la dependencia de macros manuales y hojas de cálculo dispersas. La información de ejecución presupuestal se carga directamente en los módulos de Clarity PPM, permitiendo su visualización y la integración con los módulos de seguimiento existentes.

DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

Asimismo, se actualiza los módulos que soportan la gestión presupuestal y se almacena diariamente la información histórica correspondiente a la última ejecución presupuestal generada en el día. Una vez finalizadas las cargas automáticas, se dispone de reportes diseñados para facilitar el análisis, junto con alertas que notifican cualquier error en el procesamiento de los archivos.

El proceso garantiza la consistencia de la información entre los niveles de Decreto, Desagregado y Ejecución, tanto a nivel general como por centros de costos (PCI). De esta manera, se habilita un monitoreo continuo de la ejecución presupuestal mediante reportes y tableros dentro de Clarity PPM, fortaleciendo el control y seguimiento institucional.

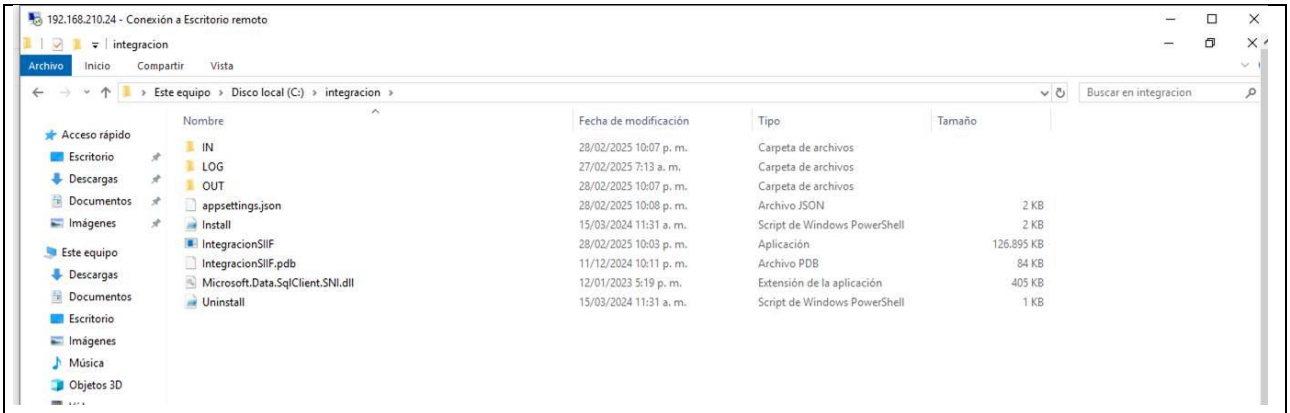
En los siguientes módulos se mapea la información proveniente de SIIF.



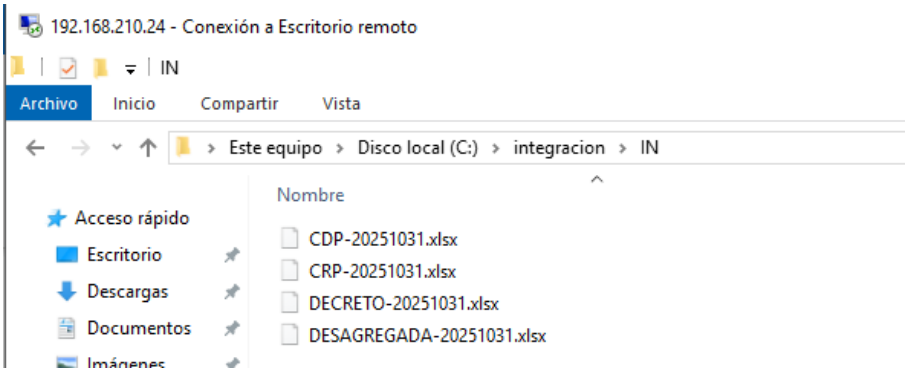
La automatización se hace con un desarrollo , que se aloja directamente en los servidores de la entidad, el cual consta actualmente de:

COMPONENTES DE INTEGRACION:

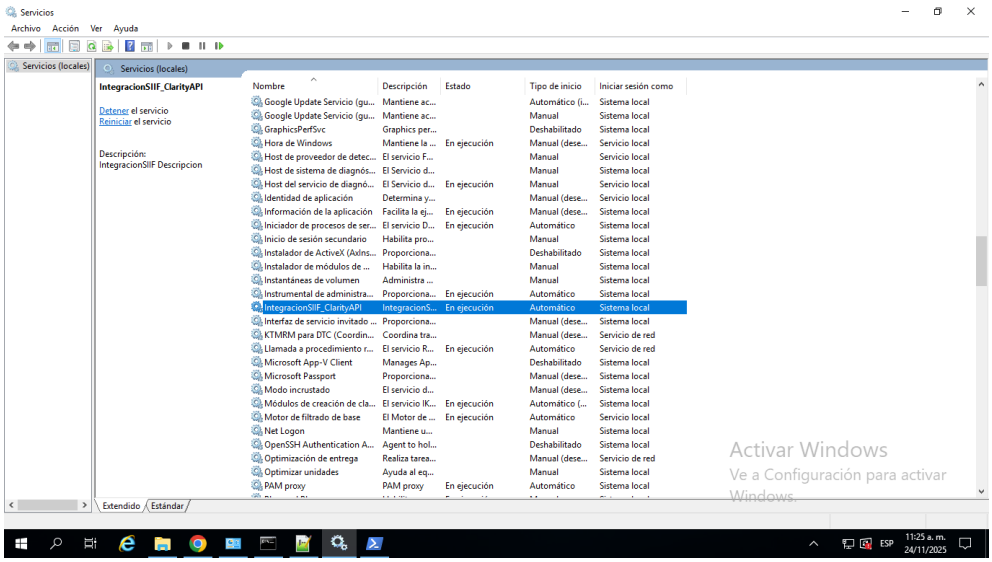
DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.



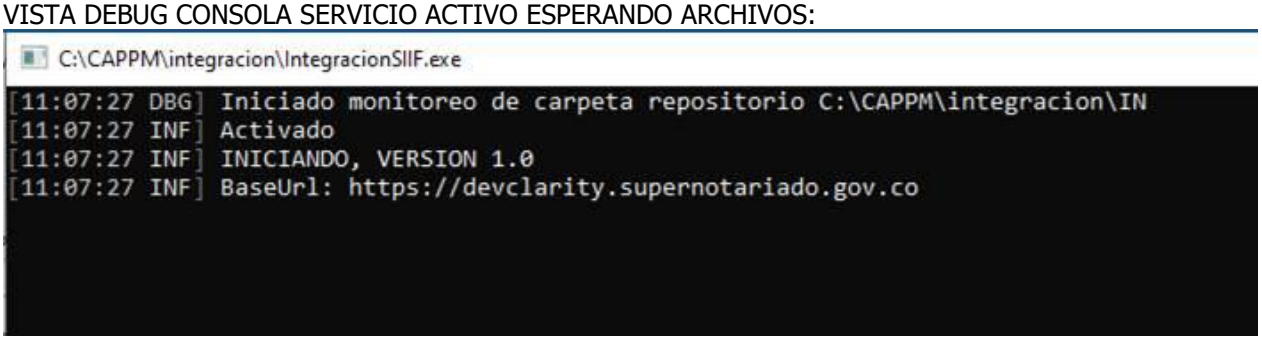
CARPETA IN:



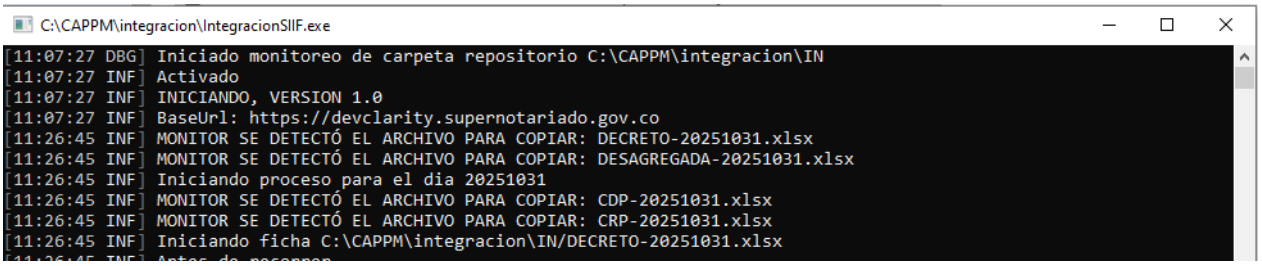
VISTA AMBIENTE DE PRUEBAS: SERVICIO INSTALADO Y EN EJECUCIÓN



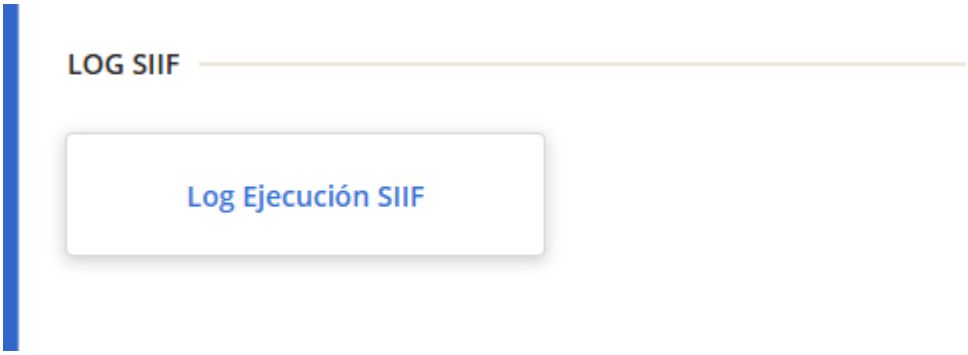
VISTA DEBUG CONSOLA SERVICIO ACTIVO ESPERANDO ARCHIVOS:



SERVICIO RECIBIENDO ARCHIVOS DE INTEGRACION – PROCESANDO PRIMER ARCHIVO



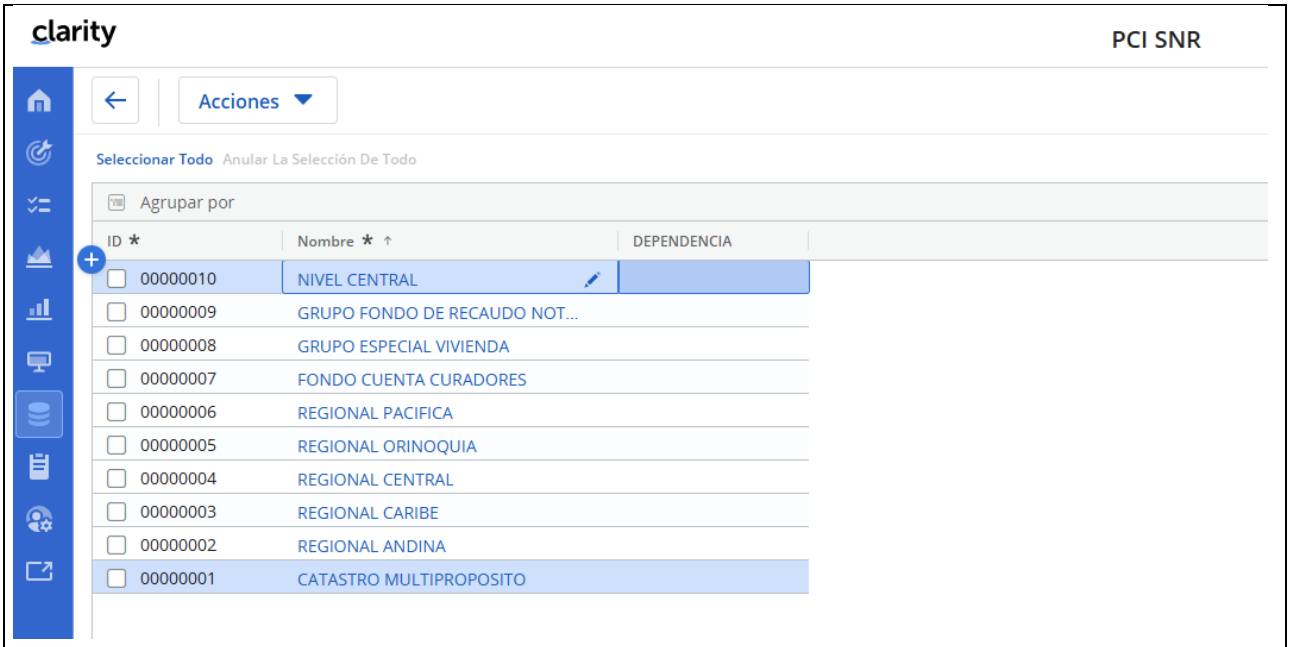
MODULO LOG. Este módulo permite al administrador, visualizar si la carga de archivos y procesamiento fue exitosa



PPM / Modulo PCI

Este módulo permite administrar e interoperar con los CDP generados, facilitando el cruce de información financiera necesario para mantener un control y una gestión precisa sobre los techos presupuestales. Esto aplica no solo a nivel general de gastos, sino también por cada PCI asociada dentro de la entidad.

DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.



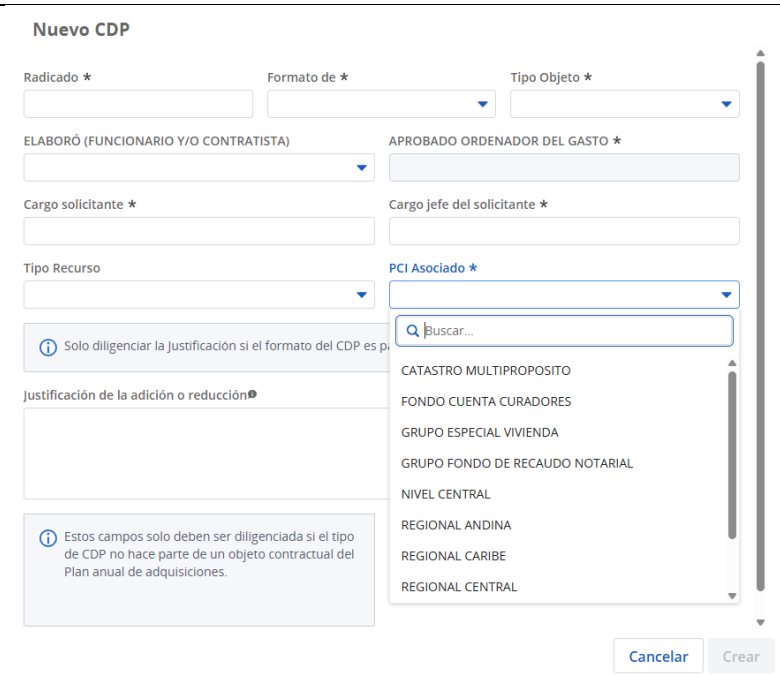
PPM / CDP (Certificado de Disponibilidad Presupuestal)

Con este ajuste, la gestión de los Certificados de Disponibilidad Presupuestal (CDP) se integra directamente con el proceso automatizado de cargue financiero proveniente de SIIF y con el módulo PCI, permitiendo un control presupuestal en tiempo real. Aunque el módulo de CDP ya se encontraba configurado en SUPRA, este requerimiento incorpora un funcionamiento basado en información dinámica y actualizada automáticamente a partir de los archivos SIIF (Decreto y Desagregado) cargados por los funcionarios de la Superintendencia de Notariado y Registro.

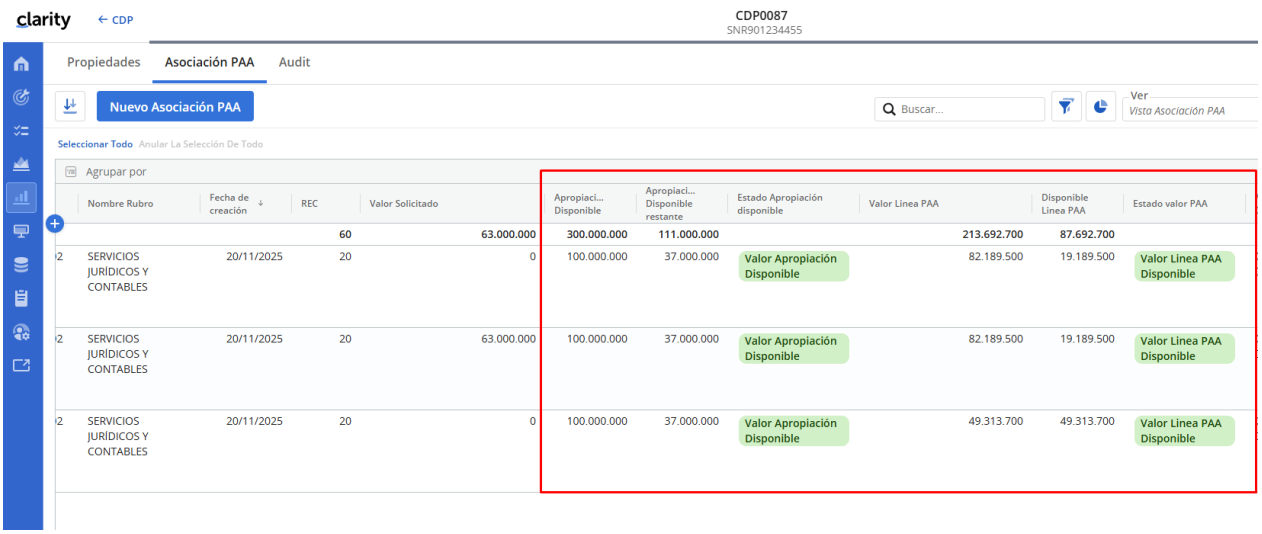
Con este módulo, Clarity PPM procesa los archivos provenientes de SIIF y genera un techo presupuestal temporal y vigente, utilizado como referencia inmediata para validar la creación de nuevos CDP. Cada nuevo cargue reemplaza por completo al anterior, garantizando que todas las solicitudes se verifiquen contra la información financiera más reciente y oficial. Este mecanismo asegura que no se comprometan recursos más allá de los límites disponibles y mantiene la coherencia presupuestal tanto a nivel general como por centro de costos (PCI).

Con este requerimiento, se fortalece la trazabilidad y la disciplina financiera dentro del proceso: cada solicitud de CDP se valida automáticamente contra el techo presupuestal generado a partir de los últimos datos del SIIF, permitiendo una gestión precisa, auditable y plenamente alineada con el estado real del presupuesto institucional.

DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

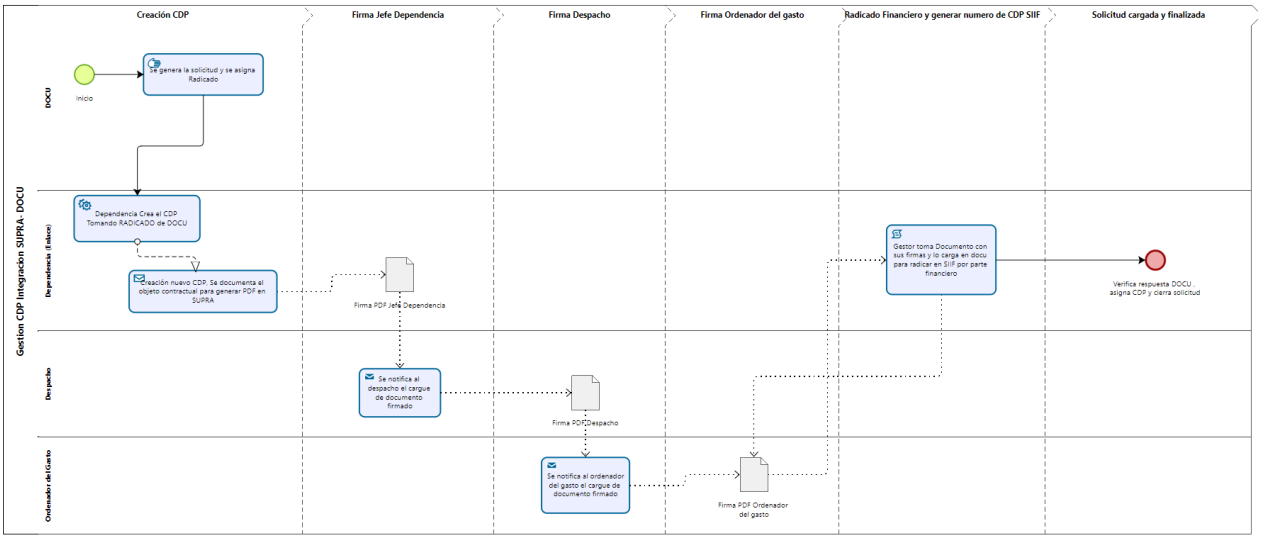


SUPRA, dependiendo el objeto permite generar una solicitud de CDP enfocada en las líneas del plan anual de adquisiciones, logrando interoperar con la gestión del PAA y detallando por cada rubro los valores de apropiación provenientes de SIIF.



DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

PPM / CDP - PROCESOS

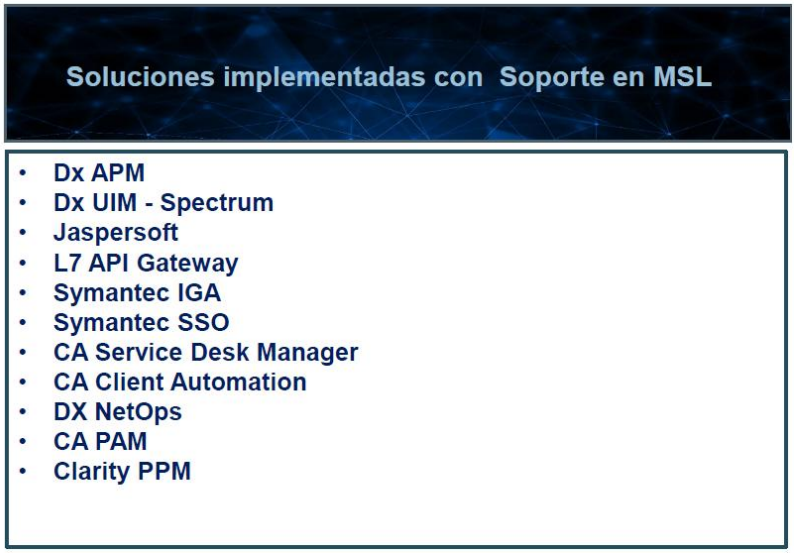


Proceso funcional de gestión del CDP con integración SUPRA - DOCU

1. **Inicio y solicitud del CDP**
   El proceso comienza desde el sistema DOCU, donde se genera la solicitud y asignación de un radicado**.**
2. **Creación del CDP en SUPRA**
   La dependencia (enlace) toma el número de radicado y procede a crear el CDP en SUPRA, documentando el objeto contractual y generando el PDF correspondiente para firmas.
3. **Flujo de firmas (PDF)**
   El documento PDF pasa por una cadena de validaciones que incluyen:
   - Firma del jefe de dependencia
   - Firma del despacho
   - Firma del ordenador del gasto
     En cada etapa, SUPRA notifica automáticamente a los responsables y permite la carga del documento firmado, asegurando trazabilidad.
   - Gestor Dependencia
   - Cuando el gestor de la dependencia tome el documento con las firmas, puede devolverlo directamente al ordenador del gasto o tramitarlo ante DOCU para generar en SIIF por parte del gestor financiero.
4. **Registro financiero y generación de número CDP**
   Una vez firmado el documento por todos los actores, el gestor financiero toma el número de CDP del SIIF y lo ingresa manualmente en SUPRA**,** lo que marca el cierre administrativo del trámite.
5. **Finalización del proceso**
   Finalmente, el sistema verifica que el número del CDP o el campo de aprobación (check) esté diligenciado**,** lo que permite finalizar formalmente la solicitud dentro de SUPRA.

DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

10. SOPORTE



- El Soporte técnico solo se brinda las soluciones configuradas e implementadas por MSL mientras estas se hayan mantenido las condiciones óptimas de mantenimiento.
- Se excluye de la atención de Soporte casos relacionados con hardware y sistemas operativos de servidores o usuarios.
- Todos los eventos atendidos por Soporte deben tener creado un caso en la Mesa de Servicios de MSL, aunque la comunicación de las novedades se haya realizado por correo, llamada, comunicación verbal, chat o cualquier otro medio disponible.
- Cada tipo de requerimiento debe tener un caso único en la Mesa de Servicios, no se deben relacionar varios tipos de errores diferentes o múltiples solicitudes en un solo registro.
- Los casos de Soporte que no correspondan a una solución implementada por MSL o a las condiciones pactadas por contrato, se devuelve para atención desde Notariado y Registro

Procedimiento General:

- Al recibir una solicitud de atención, se crea en la Mesa de Servicios de MSL un registro de ticket único, el cual es el canal oficial asignado para seguimiento y comunicación desde su apertura hasta la solución y posterior cierre
- Al registrar cada caso se debe incluir la siguiente información: Producto afectado, descripción clara del caso, cantidad de personas afectadas, impacto, urgencia, nombre y contacto de quien hace la solicitud.
- Adjuntar la información relevante para la atención del caso como imágenes, videos, archivos o todo aquello que consideren importante y esté relacionado con la novedad.
- El caso es asignado a un analista o consultor disponible del área de Ingeniería de MSL, quien a su vez dependiendo de la complejidad puede escalar o transferir a otro ingeniero e inclusive a Fabricante hasta entregar la solución requerida.

DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

- En algunas ocasiones es necesario agendar con el usuario funcional afectado sesiones de entendimiento, de revisión, mantenimiento y otras similares asociados con la resolución del caso, las cuales se coordina con previa disponibilidad de Cliente y el Servicio técnico de MSL.
- El caso se considera 'Resuelto' cuando el usuario confirme la solución y/o esté de acuerdo con la respuesta entregada a la atención del caso.
- Una vez resuelto el caso, se hace el cierre automático al día siguiente de notificada solución. En este lapso se puede reabrir el caso en caso de presentar inconformidad en la resolución del ticket.
- No se reabrirá casos que ya se encuentren en estado 'Cerrado'

Clasificación del caso:

10. Una vez recibida la solicitud de atención, MSL analiza y clasifica el caso de la siguiente manera: INCIDENTE: Fallo, caída, degradación, anomalía o mal funcionamiento de la solución instalada
11. SOLICITUD: Requisición adicional, complementaria o nueva dentro de la solución instalada. No se atenderá solicitudes de capacitaciones, transferencia de conocimientos, pruebas de proyectos en curso
12. CASO DE SOPORTE: Caso asociado al mantenimiento o garantía de las soluciones ya instaladas.
13. GARANTÍA: Caso reabierto y correspondiente a un defecto en la resolución entregada del caso.

Clasificación de Prioridad:

Una vez recibida la solicitud de atención, MSL analizará y clasificará el nivel de prioridad indicada inicialmente por el usuario para determinar el tiempo de solución de la siguiente manera: **Severidad 1:** Fallo inminente, grave, caída en el servicio en sus funciones fundamentales**.**

- **Severidad 2:** Degradación o fallo en algunos de los comportamientos normales del servicio, pero que no impide su ejecución
- **Severidad 3:** Ajuste, falla o comportamiento que se debe atender pero que no implica comportamiento inusual**.**
- **Severidad 4:** Incidencia menor

Al determinar la severidad del caso, se procede a gestionar dentro del tiempo de atención que se indica en la siguiente página

ANS:

DESCRIPCION DE LOS TIEMPOS DE SEVERIDAD		
SEVERIDAD	TIEMPO DE ATENCION	DESCRIPCION
1	2 horas en jornada laboral.	"System Down" (Sistema Abajo), una condicion inoperante del producto que afecte el ambiente de producción para el cual no haya un Workaround disponible de manera inmediata
2	4 horas en jornada laboral.	Significa una condición de negocio de alto impacto posiblemente poniendo en riesgo un ambiente de producción
3	8 horas en jornada laboral.	Significa una condición de negocio de Bajo Impacto con la mayoría de las funcionalidades del sofware en condiciones de uso
4	96 horas en jornada laboral	Significa un problema o cuestión menor que no afecte el funcionamiento de Software

DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

Matriz de escalamiento técnico:

La matriz de escalamiento técnico se refiere al personal designado para atender según la complejidad del caso. El canal de comunicación establecido para cualquier contacto con el personal técnico es la Mesa de Servicios de MSL, desde allí también se enviarán notificaciones automáticas en cada etapa de la atención del caso

A continuación, se relacionan a quienes forman parte del área de soporte técnico definido para la operación de Soporte en SNR

	Dx APM	DX IM	Jaspersoft	IGA	SSO
Nivel 1	N/A	N/A	Juan David Orjuela	Rafael Páez	N/A
Nivel 2	Giovanny Mancera	Giovanny Mancera	Juan David Orjuela	Rafael Rivera	Julian Caicedo
Nivel 3	Giovanny Mancera	Giovanny Mancera	Tibco-Jaspersoft	Rafael Rivera	Julian Caicedo
Nivel 4	Broadcom	Broadcom		Broadcom	Broadcom

	API Gateway	SDM	Clarity PPM	ITCA	PAM
Nivel 1	N/A	Miguel Rusinque	Ana Beltrán	N/A	N/A
Nivel 2	Reinaldo Santos	Neimar García	Andrés Cárdenas	Miguel Rusinque	Simón Jiménez
Nivel 3	Julián Caicedo	Neimar García	Andrés Cárdenas	Miguel Rusinque	Simón Jiménez
Nivel 4	Broadcom	Broadcom	Broadcom	Broadcom	Broadcom

11. CAPACITACIONES.

Objetivo del Programa de Capacitación
El programa de capacitación en soluciones Broadcom está diseñado para fortalecer las habilidades técnicas, operativas y estratégicas de los equipos de TI, asegurando una adopción adecuada de las plataformas, una operación eficiente y una maximización del retorno de inversión en las soluciones implementadas. Busca habilitar a los participantes para operar, administrar y optimizar cada herramienta de manera autónoma, segura y alineada a las necesidades del negocio.

Objetivo General
Brindar al equipo de la organización los conocimientos y habilidades necesarias para administrar, operar y aprovechar al máximo las soluciones de Broadcom implementadas con soporte en MSL, fortaleciendo la eficiencia operativa, la seguridad, la analítica y la gestión tecnológica.

Metodología de Capacitación
- Sesiones teórico-prácticas.
- Material de apoyo y documentación.

DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

Valor para la Organización:
Las capacitaciones permiten aumentar la autonomía operativa, mejorar tiempos de respuesta, reducir incidentes, optimizar costos tecnológicos, fortalecer la seguridad, garantizar continuidad del negocio y maximizar el retorno de inversión en las soluciones Broadcom.

Capacitaciones por Solución:

DX APM
Capacitación enfocada en el monitoreo del desempeño de aplicaciones, diagnóstico proactivo, análisis de transacciones y uso de dashboards para mejorar la disponibilidad y experiencia del usuario.

DX UIM - Spectrum
Entrenamiento en monitoreo de infraestructura, descubrimiento de dispositivos, gestión de eventos y generación de alertas para garantizar continuidad operativa.

L7 API Gateway
Capacitación en administración del ciclo de vida de APIs, seguridad, integración, políticas y monitoreo.

IGA
Entrenamiento en gestión de identidades, automatización de procesos de acceso, cumplimiento y gobernanza.

SSO
Formación en acceso unificado, autenticación segura, federación y experiencia de usuario sin fricciones.

CA Service Desk Manager
Capacitación en gestión de incidentes, problemas, cambios, autoservicio y mejores prácticas ITIL.

CA Client Automation
Entrenamiento en automatización de despliegues, gestión de activos, parches y control de endpoints.

CA PAM
Capacitación en gestión de accesos privilegiados, controles de seguridad, auditoría y cumplimiento.

Clarity PPM
Entrenamiento en portafolio de proyectos, gestión financiera, asignación de recursos y reporting.

DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

12. ASSESSMENT

- Se elabora la documentación con la situación actual de las soluciones, mejoras a realizar y Roadmap de las soluciones
- Se elaboran los planes de trabajo detallados con las actividades a implementar de acuerdo con lo que se proponga de los resultados del Assessment y las solicitudes que requiera el cliente para las soluciones de CA
- Se realizan entrevistas con los lideres de cada solución a fin de identificar las necesidades de la Entidad
- Los días 15 y 20 de octubre se realizan las sesiones para presentarle al Administrador del contrato, el gerente del proyecto y los lideres de la entidad los resultados de los Assessment.

Item	Solución	Consultor MSL Latam	Lider OTI	Fecha y Horario Revisión Cliente
1	MONITOREO IM	Giovanny Mancera	Santiago Garcia Hernan Cortes	15/10/2025. 2:00 PM
2	MONITOREO APM		Santiago Garcia Hernan Cortes Anggie Ovalle	
3	PAM	Simon Jimenez	Santiago Garcia Alejandro Vargas Hernan Cortes Samuel Camarillo	15/10/2025. 2:20 PM
4	SSO	Julian Caicedo	Jairo Buitrago Samuel Camarillo Hans Carlosama	15/10/2025. 2:40 PM
5	IGA	Rafael Rivera	Jairo Buitrago Guillermo Becerra Ana Diaz Samuel Camarillo Hans Carlosama	15/10/2025. 3:00 PM

Item	Solución	Consultor MSL Latam	Lider OTI	Fecha y Horario Revisión Cliente
1	SDM	Neimar Garcia	Astrid Villar Ricardo Parra Santiago Venegas	20/10/2025. 9:00 AM
2	ITCA	Miguel Rusinque	Guillermo Becerra Ramiro Garcia Santiago Garcia Santiago Venegas	20/10/2025. 9:20 AM
3	PPM	Andres Cardenas Pinzon	Oscar Montes Jorge Serrano	20/10/2025. 9:40 AM
4	API	Jonathan Ardila	Nelson Rodriguez Mario Perdomo	20/10/2025. 10:00 AM

DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

13. SDM / Integración de CHATBOT con CA SDM (Versión Interna)

Alcance: Este Bot permite la gestión de solicitudes de las distintas mesas de ayuda de LIA por medio de WhatsApp, como también integra la comunicación en tiempo real con asesores para solicitudes que requieren atención personalizada.

Chatbot LIA se logró desarrollar y entregar a SNR hasta la fase 1. Dicho desarrollo comprende lo siguiente:

- Funcionalidad en las mesas tecnológicas, SIR y SIN, de navegar a través de submenús integrados en cada mesa con la finalidad de realizar una solicitud más específica al asesor que gestiona los chats.
- Validación de correo institucional al inicio de la conversación.
- Contadores de inactividad por sesión.
- Opciones de navegabilidad, como retornar a un menú anterior o terminar una conversación.
- Integración con Front de atención de casos gestionado por los asesores. Dicho Front cuenta con autenticación SSO y la capacidad de gestionar varias conversaciones entrantes por el rol de los gestores de chats.
- Capacidad de manejar varias conversaciones simultáneamente.
- Guardar y respaldar las conversaciones diarias realizadas en el chatbot, hacia la Base de Datos de auditoría del cliente.
- Enviar el historial de conversación con el Bot y el asesor, al momento de terminar cada conversación realiza

Plan de trabajo:

Item	Actividad	Tarea	Vobo Priorización cliente
1	Revisión de información entregada	Revisión del material proporcionado por el cliente y resolución de dudas.	1
2	Construcción del documento de casos de uso	Identificación y documentación de los casos de uso principales, detallando actores, flujos principales y alternos, con base en los requerimientos funcionales.	3
3	Conexiones y credenciales (Entorno de Pruebas)	Validación de la conexión entre el servidor y los endpoints de ServiceDesk en el entorno de pruebas.	1
4	Conexiones y credenciales (Entorno de producción)	Validación de la conexión entre el servidor y los endpoints de ServiceDesk en el entorno de producción.	1
5	Ajuste Activación y Registro de Usuarios	Endpoint que habilita acceso, verificación en base SSO Botón de activación, tabla de usuarios pendientes	15
6	Desarrollo en Api gateway	Contruir desarrollo en el API Gateway SNR para consultar los roles específicos asignados a cada mesa en ServiceDesk. Esta información es posteriormente consumida por la aplicación LIA, encargada del control de roles y autorizaciones.	5
7	Ajustes a nueva tecnologia Autenticación y Autorización SSO (Node SAML)	Integración con proveedor SAML, validación de token Control de sesión SSO, login automático	23
8	Actividades IGA	Configuracion Roles Carrito de compras	1
9		Configuracion de Politica para asignacion de Grupo del DA	1
10		Configurar rol para visualizar roles en carrrito de compras	1
11	Actividades SSO	mapear atributos del DA en SSO (predecesoras 5 y 6)	1
12		ajustar integración con url final de LIA (predecesoras 5 y 6)	1
13		Ajustar ULR de cierre de sesión y redirección (predecesoras 5 y 6)	1
14	SDM / Astrid Villar	Roles de las mesas	3
15	Desarrollo backend del fujo de selección mesa	Desarrollo de la logica para crear el flujo principal donde se seleccionará la mesa correspondiente al usuario.	8
16	Desarrollo lógica de ingreso de datos	Desarrollo de la lógica correspondiente a las acciones de solicitud de datos (correo, nombre) previas a la selección de las mesas	8
17	Desarrollo backend flujo mesa ayuda tecnológica	Desarrollo de la lógica de cada acción dentro de la mesa de ayuda tecnológica (Creación, Cargue, Soporte, Seguimiento, Regreso al menú anterior)	15
18	Desarrollo backend flujo mesa SIR	Desarrollo de la lógica de cada acción dentro de la mesa de ayuda tecnológica (Gestión Usuarios, Gestión Turnos, Otros, Seguimiento, Regreso al menú anterior)	11
19	Desarrollo backend flujo mesa Soporte SIN	Desarrollo de la lógica de cada acción dentro de la mesa de ayuda tecnológica (Aplicativo Apostilla, Envío Facturas, Aplicativo SIN, Soporte Correo, Seguimiento Caso, Regreso al menú anterior)	11

DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

20	Desarrollo del módulo de integración de inserción y búsqueda de mensajes entrantes en BD, mediante implementación de sockets	Desarrollo de los flujos pertenecientes al chat con asesor, configurando los sockets y credenciales necesaria para establecer una comunicación con la base de datos que alojará las respuestas de los asesores y los clientes.	11
21		Ajuste integración del SSO con la aplicación de Mesa de Ayuda	16
22		Explicación del proceso de configuración y envío de certificados en el SSO, con el fin de realizar las pruebas correspondientes.	6
23	Pruebas funcionales (Entorno de Pruebas)	Validación funcional del flujo completo entre bot, frontend, ServiceDesk y la base de datos.	8
24		Aplicación de ajustes necesarios.	2
25		Documentación correspondiente.	2
26	Despliegue (Entorno de Producción)	Preparación y ejecución del plan de despliegue.	4
27		Configuración del servidor y sus dependencias en el entorno de producción.	4
28	Pruebas funcionales (Entorno de Producción)	Validación funcional completa del flujo entre bot, frontend, ServiceDesk y la base de datos en producción.	8
29		Ajustes necesarios y documentación de resultados.	3
30		Documentación de las pruebas funcionales	3
31	Documentación del cierre de la implementación	Elaboración de la memoria técnica y manual del desarrollador.	3
32		Ajustes finales en la documentación de cierre.	0

14. API / Despliegue e implementación de API Developer Portal:

Alcance: El Portal para Desarrolladores de API de Layer7 (API Portal) permite a los Administradores de API controlar cómo se publican, permite a los Consumidores descubrir qué servicios están disponibles y ayuda a los equipos de operaciones a supervisar el rendimiento de las API mediante la integración con herramientas de monitorización de API de nivel empresarial. API Portal simplifica el descubrimiento de APIs para los Desarrolladores y les proporciona acceso a datos para crear aplicaciones rápidamente. Las relaciones e interacciones con desarrolladores, socios y terceros se gestionan fácilmente.

Los desarrolladores pueden usar API Portal para:

- Descubrir qué API están disponibles y solicitar acceso.
- Recibir autorización para usar las API y obtener llaves de API.
- Comenzar a desarrollar más rápido con herramientas educativas que incluyen aplicaciones de ejemplo, API Explorer y generación de código.

API Portal utiliza una arquitectura contenerizada que es compatible con los entornos donde residen sus aplicaciones y API facilitando la implementación, la migración y la carga de trabajo de las actualizaciones. Los componentes del portal se implementan en contenedores Docker, lo que facilita el intercambio o la sustitución de contenedores a medida que se implementan nuevas funcionalidades. Independientemente de dónde implemente, la solución utiliza la misma interfaz para administrar sus API y a sus desarrolladores. Las API integradas del portal aprovechan las herramientas de desarrollo existentes para optimizar la integración entre la gestión de API y los datos de los sistemas CI/CD. Las API permiten la integración con herramientas integradas y almacenes de datos existentes, o bien realizan fusiones entre datos empresariales y datos de API.

- 100% Instalación y configuración de la plataforma.
- Montaje de sitios de pruebas y producción
- 100% Integración con Layer 7 API Gateway (Enrolamiento).
- 100% Transferencia de conocimiento operativo a rol Administrador de la plataforma.
- 3 APIs publicadas en sitio de pruebas como parte práctica de la transferencia de conocimiento.

DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

Plan de trabajo:

Total de horas			80
Ítem	**Actividad**	**Tarea**	**Horas reales planeadas**
1	**Instalación y configuración.**	Instalación y Configuración Capa de Base de datos.	2
2		Instalación API Developer Portal	7
3		Enrolamiento de Ambientes SNR a Portal (Pruebas)	2
4		Verificación del sistema y servicios servidor Portal.	5
5		Tenants (por defecto y definidos por el usuario).(SETUP)	5
6		Configurar Proxies(SETUP)	2
7		Enrolamiento de Ambientes SNR a Portal(Producción)	7
8		Verificación del sistema y servicios servidor Portal.	5
9		Tenants (por defecto y definidos por el usuario).	5
11		Configuración de Autenticación.	2
12		Configuración de Registro de Usuarios.	2
13		Configuración de Flujos de Trabajo (Workflows)	2
14		Configuración de Servidor de Correos	2
15		Personalización de Páginas de Portal	2
16		Logs de Auditoría	2
17		Configurar APIs	2
18		Configurar Aplicaciones	2
19		Configurar EULAs	2
20		Configurar Proxies(TRAINING)	2
21		Configurar Organizaciones	2
22		Tipos de Usuario, Roles y Permisos	2
23		Arquitectura Multi-tenant	2
24		Mantenimiento del Sistema	2
25	**Auditoria / Monetización**	Configurar Uso de APIs	2
26	**Analitica**	Dashboard	6
27	**Entrega**	Capacitación / entrega al cliente	4

15. API / Interoperabilidad SNR – Catastro:

Alcance:

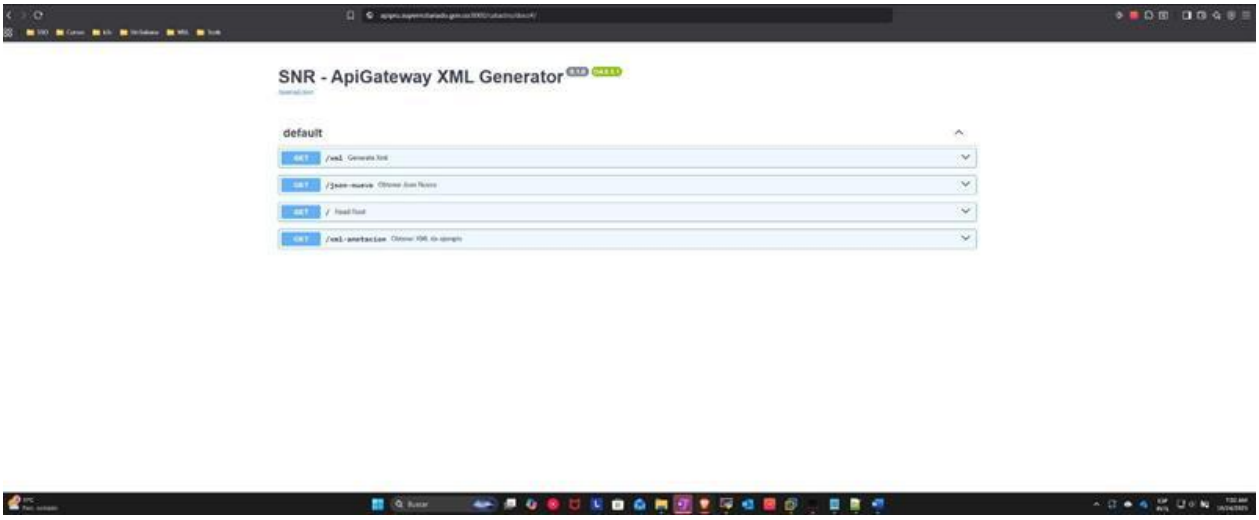
El presente desarrollo tiene como propósito la modernización del proceso de generación y publicación de información catastral en SNR, reemplazando los mecanismos manuales y dependientes de código heredado por una solución automatizada, segura y escalable. El desarrollo se centró en la implementación de un servicio a la medida que permite generar información proveniente de la base de datos en formato BD-XML, correspondiente al histórico de los últimos propietarios de los predios registrados en toda la base catastral, discriminados por municipio. Este proceso —conocido como mutaciones— considera que la codificación geográfica de los municipios puede variar de una oficina a otra, ya que cada gestor catastral administra diferentes territorios según su jurisdicción. El nuevo servicio fue diseñado para adaptarse dinámicamente a dichas variaciones, garantizando la coherencia en la consulta y la correcta identificación de los registros históricos por jurisdicción.

DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

La solución fue desarrollada bajo un enfoque de arquitectura orientada a microservicios y publicada de forma controlada y segura mediante el API Gateway de Broadcom, lo que permite su consumo a demanda por parte de aplicaciones y sistemas externos, asegurando la autenticación, autorización y trazabilidad de todas las solicitudes. Con esta implementación, se busca mejorar la eficiencia operativa, estandarizar la gestión de información catastral y asegurar la evolución tecnológica del entorno actual hacia una plataforma moderna, interoperable y alineada con las políticas institucionales de seguridad y gobierno de datos.

El desarrollo del servicio de generación y publicación de información catastral en formato BD-XML se encuentra actualmente en un estado avanzado de implementación. La solución fue desplegada en el ambiente de desarrollo y publicada exitosamente en el API Gateway de Broadcom, donde se han realizado pruebas de conectividad, seguridad y validación funcional de los datos generados. Las pruebas iniciales han sido satisfactorias, demostrando estabilidad, tiempos de respuesta óptimos y correcto manejo de la autenticación y autorización a través del API Gateway de SNR.

En esta fase, el proyecto se encuentra en la etapa final de pruebas y ajustes, enfocada principalmente en la validación de la codificación geográfica por municipio y en la revisión de los resultados históricos de propietarios según las jurisdicciones catastrales, también se está validando temas de tamaño debido a un volumen de información. Aunque la solución está técnicamente madura y funcional, se continúa con la afinación de detalles menores y ajustes de validación para garantizar la total precisión de la información antes de su paso a producción.

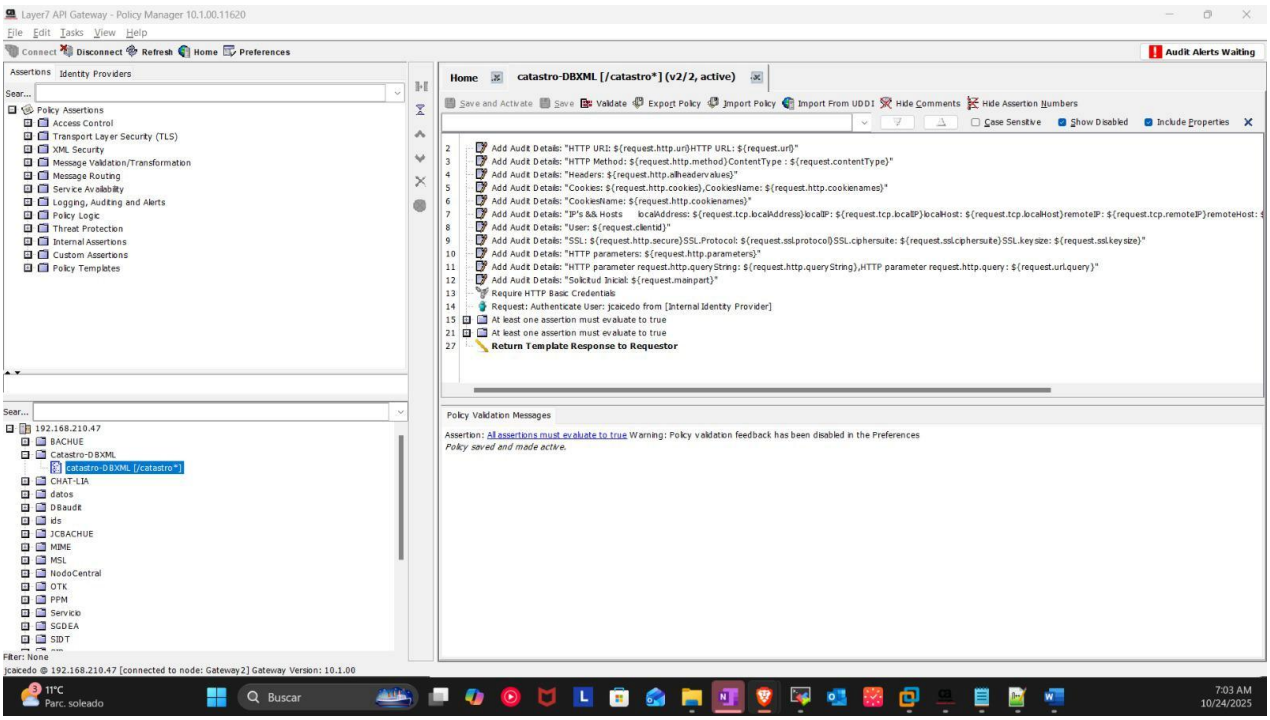


DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

Plan de trabajo:

Total de horas			300
Ítem	Actividad	Tarea	Horas Cliente
1	**Planeación y Requisitos**	Identificar BDs Oracle 7 y 11c	6
2		Confirmar compatibilidad del cliente Oracle	6
3		Definir etiquetas XML de salida	6
4		Determinar estructura del servidor	9
5		Validar autenticación y seguridad de conexión	5
6		Definir frecuencia y volumen de exportación	5
7	**Instalación del entorno**	Instalar sistema operativo y configurar servidor	7
8		Instalar Node.js y dependencias	14
9		Instalar Oracle Instant Client y validar conexión payara con Oracle 7	28
10		Configurar variables de entorno	6
11	**Desarrollo del servicio**	Iniciar proyecto Node.js	7
12		Configurar archivo .env	3
13		Crear pools de conexión por BD	7
14		Escribir módulo de consultas	7
15		Crear plantilla de XML	5
16		Generar exportación XML	5
17	**Validación**	Probar conexión con cada BD	12
18		Validar estructura del XML	14
19		Probar consultas y etiquetas	8
20	**Despliegue**	Configurar CRON o node-cron	7
21		Configurar logs y monitoreo	7
22		Desplegar con PM2	5
23	**Seguridad**	Configurar .env seguro	4
24		Respaldo en almacenamiento externo (conexión a la BD folio)	4
25		Revisar reglas de red/firewall (Conexión a la BD folio)	5
26	**Api Gateway**	Crear servicio para consumir a demanda	21
27		Aserciones, política y lógica para ws	21
28	**Pruebas y ajustes**	Pruebas conexiones y etiquetas XML (conexión a la BD folio)	5
29		Pruebas Checklist para nuevas BDs (conexión a la BD folio)	5
30		Ajustes y pruebas (conexión a la BD folio)	7
31	**Documentación**	Set de pruebas evidencias (conexión a la BD folio)	7
32		Manual de Desarrollador	28
33		Manual de administración	14

DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.



16. SSO / FACELOGIN SIR.

Alcance:

El presente desarrollo tuvo como alcance la implementación de un mecanismo de autenticación multifactor (MFA) basado en reconocimiento facial (FaceLogin) dentro del flujo de acceso gestionado por Symantec SiteMinder (SSO) en SNR, con el objetivo de fortalecer los niveles de seguridad y control de identidad de los usuarios finales.

La solución se diseñó de forma que, tras la validación inicial de credenciales a través del login protegido por SiteMinder (SSO), se invoque un proceso adicional de autenticación biométrica utilizando reconocimiento facial, permitiendo así una segunda capa de verificación antes de la emisión de la cookie de sesión. Para lograr esta integración, se hizo uso del API Gateway de Broadcom que dispone actualmente la SNR, el cual actúa como componente intermedio para la comunicación segura entre el portal de autenticación y el servicio de FaceLogin, gestionando la lógica de intercambio de datos, validación de tokens, y respuesta de éxito o rechazo del factor facial.

Adicionalmente, se realizaron ajustes en el flujo del login HTML y en las políticas de autenticación de SiteMinder, garantizando que el proceso MFA se ejecute únicamente tras una autenticación primaria exitosa, y que la sesión se establezca solo si se completa de manera satisfactoria la verificación biométrica. Este desarrollo incluyó la personalización de interfaces, la configuración de endpoints seguros en el API Gateway, y la validación integral del flujo completo de autenticación, asegurando compatibilidad con las directrices de seguridad y los estándares corporativos definidos por la organización.

El proyecto de integración de autenticación multifactor (MFA) con reconocimiento facial en el entorno de Symantec SiteMinder (SSO) en SNR se encuentra actualmente en el ambiente de desarrollo, donde ha sido implementado y probado exitosamente tanto a nivel técnico como funcional.

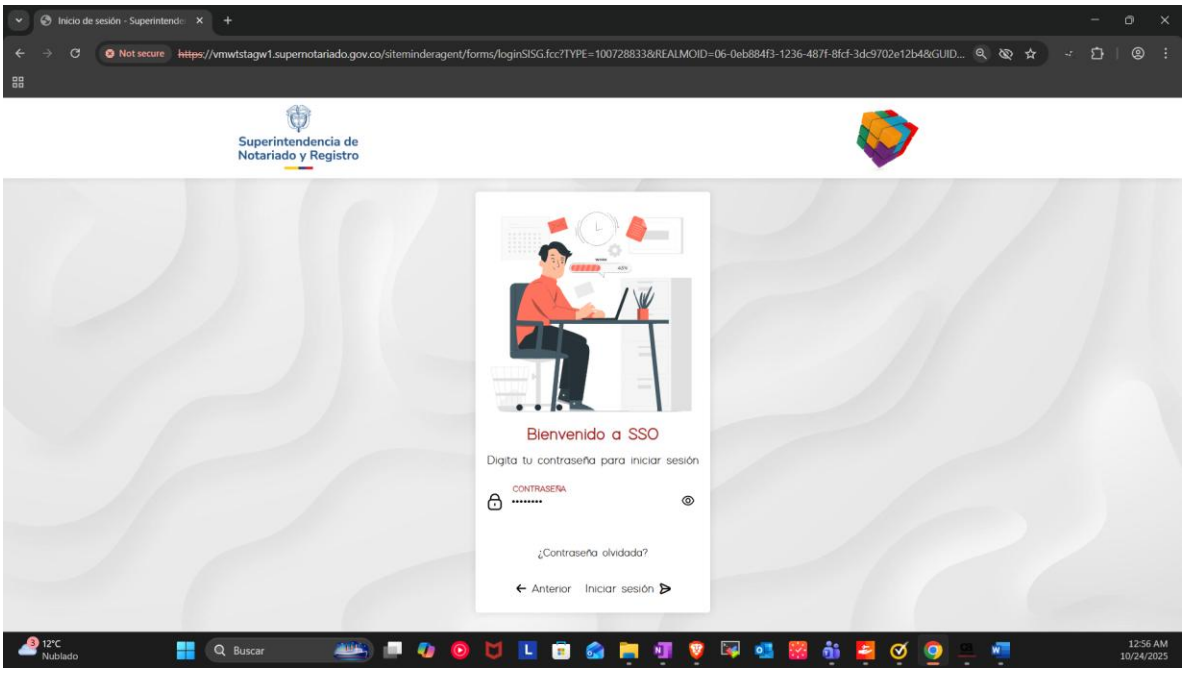
La solución integra el servicio de FaceLogin como segundo factor de autenticación, utilizando el API Gateway de Broadcom como componente intermediario para la validación y orquestación del proceso biométrico. Durante las pruebas internas y con el área funcional, se verificó el correcto funcionamiento del flujo completo de autenticación, incluyendo la validación primaria de credenciales, la activación del reconocimiento facial y la posterior generación controlada de la sesión de SiteMinder únicamente tras la validación biométrica exitosa. Adicionalmente se probó el registro correcto de nuevos vectores faciales asociados a un usuario dentro del aplicativo FaceLogin.

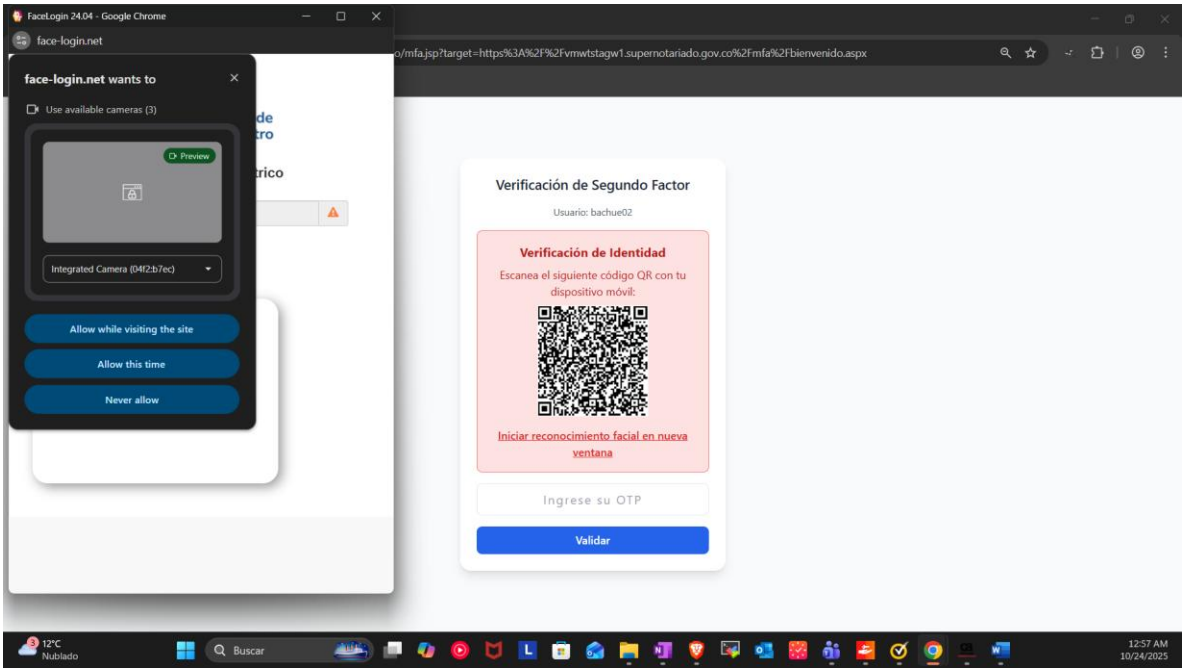
Los resultados obtenidos confirman que el mecanismo es estable, seguro y cumple con los requerimientos definidos, logrando una experiencia de autenticación fluida Actualmente, el proyecto se encuentra listo para avanzar hacia las etapas de producción una vez el SNR de la autorización.

Plan de trabajo:

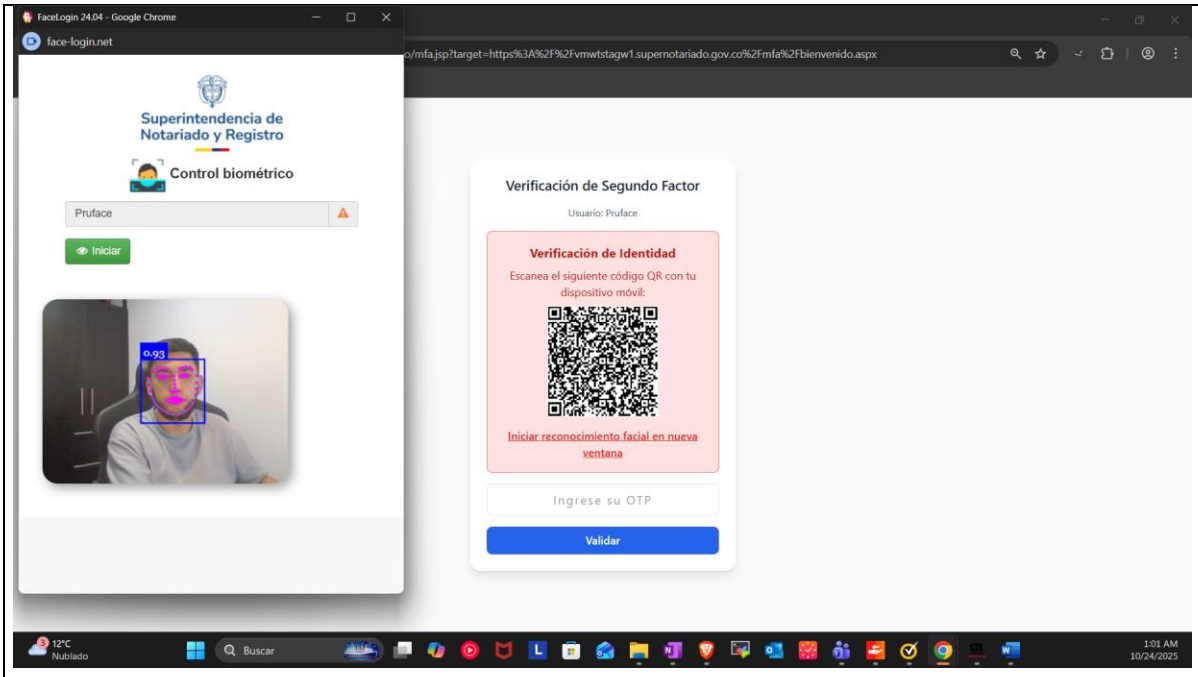
Total de horas			100
Ítem	**Actividad**	**Tarea**	**Horas Cliente**
1	**Atención Vulnerabilidades / Plan de trabajo**	Crear el formulario de login personalizado para autenticación básica con SiteMinder.	10
2		Configura el formulario de login personalizado para autenticación HTML con SiteMinder.	3
3	**ApiGateway, front y backend OTP**	Desarrollo página iframe OTP, Crear la página HTML que se cargará en el iframe para mostrar estado de validación OTP.	9
4		Implementar backend que valide OTP y comunique resultado al iframe.	8
5		Pruebas sobre WS de otp, facelogin	2
6		Desarrollar comunicación entre iframe y página padre usando postMessage para validar OTP.	5
7	**Configuración integración entre API y recurso protegido**	Configurar integración en ws de ApiGateway para que acepte sólo peticiones autenticadas vía SiteMinder	10
8		Generación de usuarios parciales	12
9	**Pruebas**	Pruebas completas de login, validación OTP, comunicación iframe y acceso a ws (Ajuste del proceso por tipo de autoenrolamiento	20
10	**Producción**	Migrar login, configuraciones y ws Producción	4
11		Pruebas	2
12	**Documentación**	Memoria técnica api y Siteminder	10
13		manual desarrollador api	5

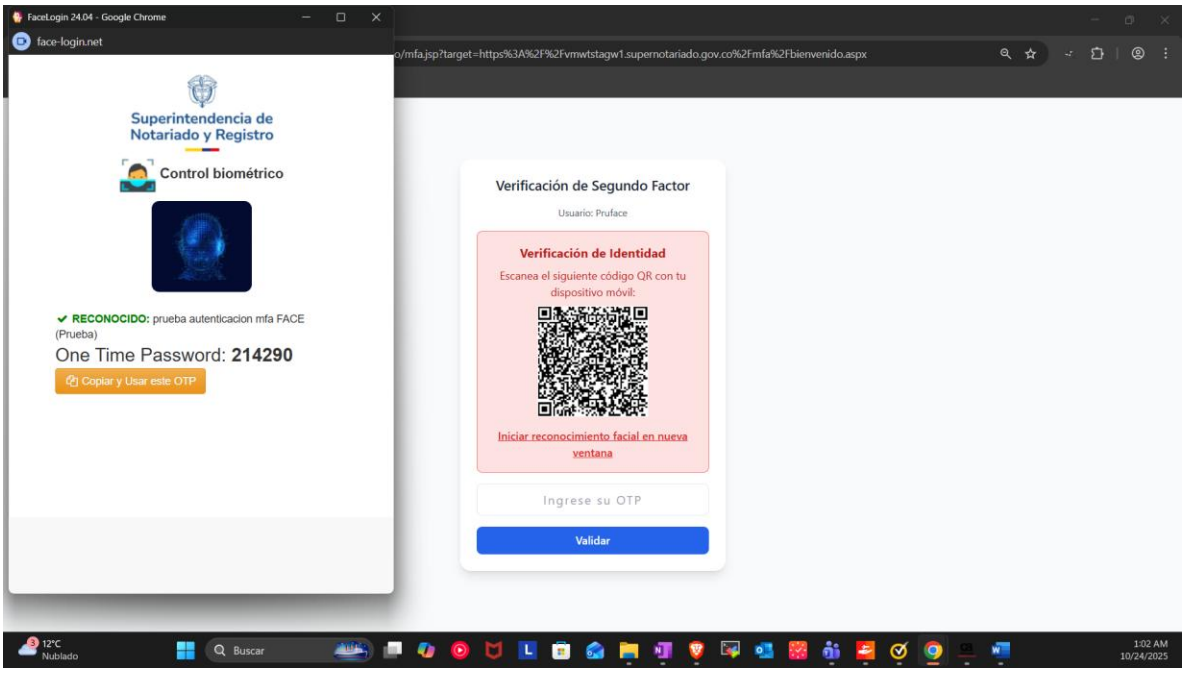
DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

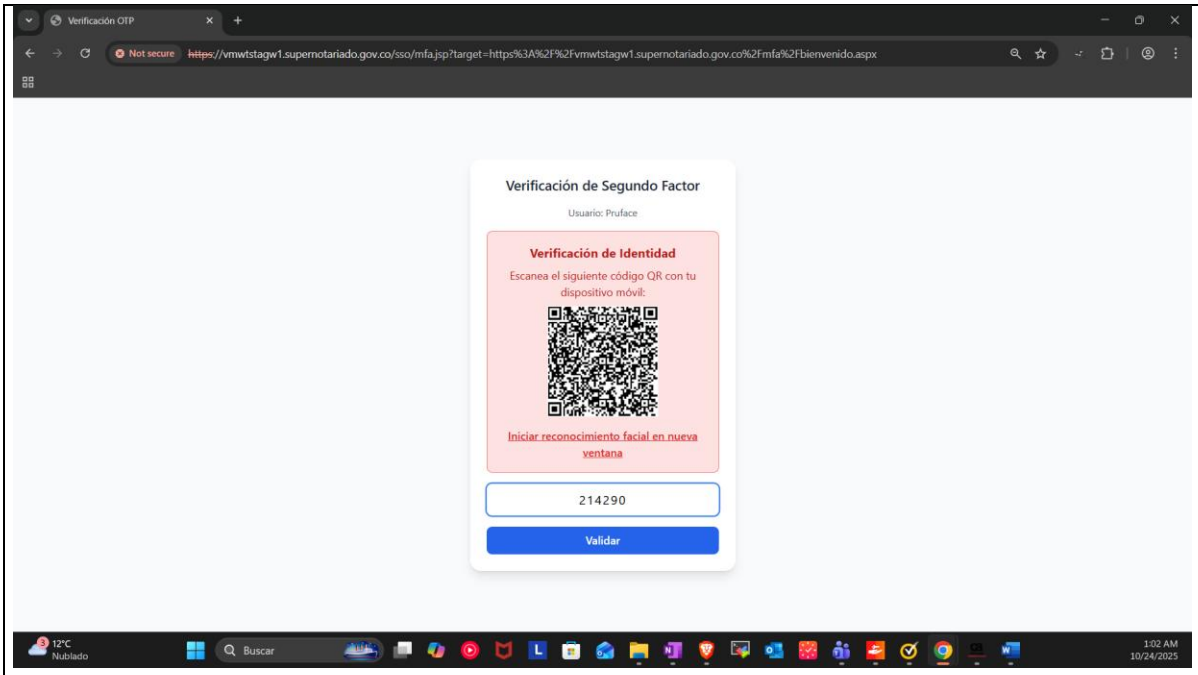


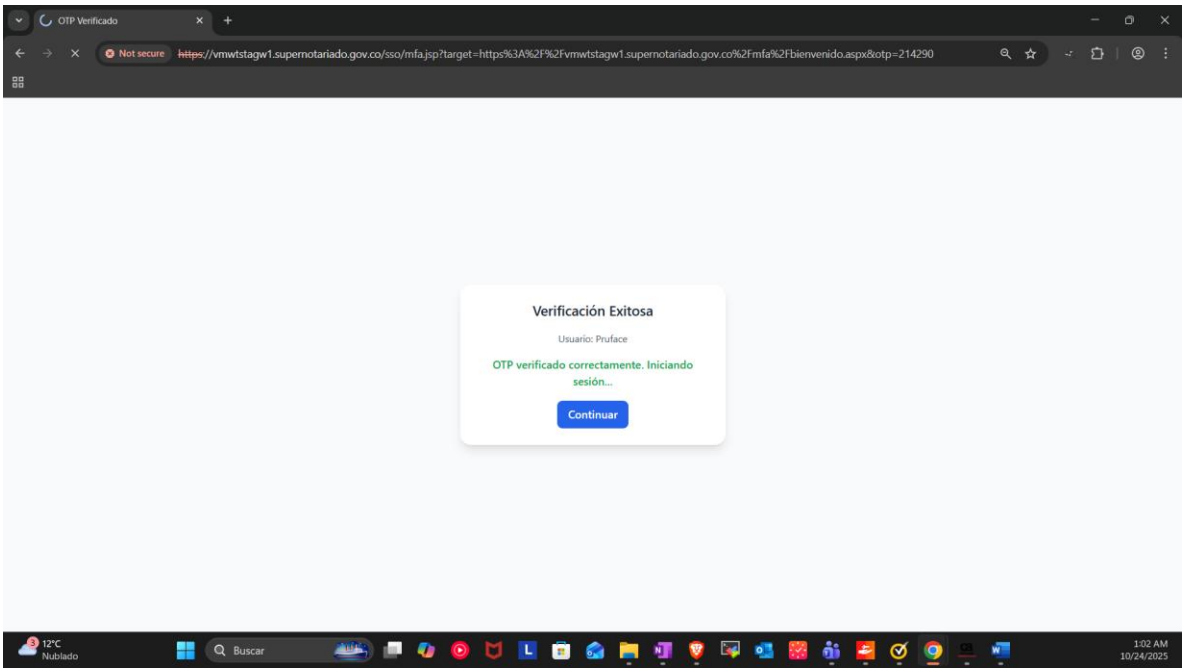


DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.


FaceLogin 24.04 - Google Chrome
face-login.net
Superintendencia de Notariado y Registro
Control biométrico
Pruface
Iniciar
0.93
Verificación de Segundo Factor
Usuario: Pruface
Verificación de Identidad
Escanea el siguiente código QR con tu dispositivo móvil:
Iniciar reconocimiento facial en nueva ventana
Ingrese su OTP
Validar
12°C Nublado
Buscar
1:01 AM 10/24/2025


FaceLogin 24.04 - Google Chrome
face-login.net
Superintendencia de Notariado y Registro
Control biométrico
RECONOCIDO: prueba autenticacion mfa FACE (Prueba)
One Time Password: 214290
Copiar y Usar este OTP
Verificación de Segundo Factor
Usuario: Pruface
Verificación de Identidad
Escanea el siguiente código QR con tu dispositivo móvil:
Iniciar reconocimiento facial en nueva ventana
Ingrese su OTP
Validar
12°C Nublado
Buscar
1:02 AM 10/24/2025





DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.

ENTREGA	RECIBE A SATISFACICÓN
MSL DISTRIBUCIONES Y CIA S.A.S **NOMBRE:** ANGELA LILIANA ORTIZ Gerente de Proyecto FIRMA_____	**SUPERINTENDENCIA DE NOTARIADO Y REGISTRO** **NOMBRE:** OSCAR FABIAN CORREDOR CAMARGO Supervisor FIRMA_____

DOCUMENTO CONFIDENCIAL MSL Distribuciones & CIA S.A.S.