CONSENSUS

SAP Business One

Políticas de Seguridad para el Cloud Control Center

Autor: Carlos González
Fecha de Creación: agosto de 2020
Fecha de Modificación: septiembre de 2020

CONSENSUS

Contenido

1. INTRODUCCIÓN 2

2. OBJETIVO 2

3. ALCANCE 2

4. DEFINICIONES 2

5. POLÍTICAS 3

5.1. Políticas de confidencialidad 3

5.2. Políticas de Uso 3

5.3. Políticas de red 3

5.4. Políticas Administrativas y de Instalación 4

5.4.1. Software Propietario de SAP 5

5.4.2. Software Complementario 7

5.5. Políticas de Respaldo 8

6. CUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD. 8

7. CONTACTO 8

1. Introducción

Actualmente Consensus en compañía con Gigas, cuentan con una plataforma de SAP Business One Cloud Control Center como servicio, en la cual se procesa y genera información principalmente de los clientes que se encuentran bajo esta arquitectura.

Las Políticas de Seguridad son las directrices de índole técnica y de organización que se llevan adelante respecto de un determinado sistema de computación a fin de proteger y resguardar su funcionamiento y la información en él contenida.

Siendo la información un factor valioso de nuestros clientes y teniendo en cuenta que el despliegue de una plataforma Cloud es un ambiente compartido, se hace necesario la definición e implementación de políticas de seguridad que permitan el uso adecuado del sistema, verificando que no se comprometa el rendimiento y seguridad de la información de ningún cliente.

Este documento tiene como finalidad dar a conocer las Políticas de Seguridad, que deben aplicar y acatar los usuarios, consultores y terceros que hagan uso del Cloud Control Center, entendiendo como premisa que la responsabilidad por la seguridad de la información es de todos y cada uno.

2. Objetivo

Definir e implementar una política de seguridad que den pautas para la gestión y uso adecuado del software instalado o a instalar en cada uno de los servidores del Cloud Control Center de Consensus.

3. Alcance

Estas políticas de seguridad están orientadas a toda la información almacenada, procesada y transmitida por diferentes medios que se encuentren dentro de los servidores del Cloud, estas políticas deben ser conocidas y cumplidas por usuarios finales, consultores de Consensus, proveedores que apoyan la gestión y terceros o grupos de interés que utilicen la información generada de los diferentes clientes, y por quienes hagan uso de los servicios tecnológicos.

4. Definiciones

Gigas: Aliado estratégico de Consensus en la implementación del Cloud, actúa como proveedor de los servidores donde se tiene instalada toda la arquitectura y presta soporte sobre estos servidores para garantizar la seguridad y óptimo funcionamiento.

PaaS: Plataforma como servicio, es un entorno completo en la nube, con recursos de hardware que permiten el uso de aplicaciones, para Consensus este servicio es proporcionado y soportado por Gigas.

Cloud Computing: Conjunto de computadoras de alta capacidad conectadas a través de una red de alta velocidad que pueden trabajar en conjunto.

SAP Business One Cloud Control Center: Arquitectura desarrollada por SAP en la cual se puede contar con el ERP de SAP Business One, mediante una conexión a internet, bajo una arquitectura PaaS.

Bases de datos: Una base de datos es una colección de información organizada de forma que un programa pueda seleccionar rápidamente los fragmentos de datos que necesite. Una base de datos es un sistema de archivos electrónico.

Instancia: entorno donde se alojan varias bases de datos.

SAP HANA: Implementación de SAP que usa una tecnología de base de datos en cargada en memoria RAM.

Tenant/Schema: Base de datos alojada en una instancia de SAP HANA

Backups: Respaldo de información.

5. Políticas

5.1. Políticas de confidencialidad

Toda la información recibida y producida en el uso de los servicios prestados por Consensus en su plataforma Cloud, pertenece al cliente, por lo tanto, Consensus nunca hará divulgación, ni extracción de esta información bajo ningún concepto.

Todas las copias de información que no hagan parte del esquema de Backups establecido por Gigas, se realiza bajo solicitud en la plataforma de soporte, no se realizará por parte de los consultores, copias no autorizadas de información.

Ningún usuario podrá visualizar, copiar, alterar o destruir información que no se encuentre bajo su custodia y propiedad.

Ningún usuario podrá interceptar datos informáticos en su origen, destino o en el interior del sistema informático, sin autorización de la Administración del Cloud y previa solicitud realizada en la plataforma de soporte.

5.2. Políticas de Uso

El espacio en disco duro de los equipos de cómputo será ocupado únicamente con documentos relevantes para el uso de SAP Business One y el cliente, no se hará uso de ellos para almacenar información de tipo personal.

Ningún usuario podrá impedir u obstaculizar el funcionamiento o el acceso normal al sistema, datos informáticos allí contenidos, o red de telecomunicaciones, salvo el personal autorizado por Gigas o Consensus en aplicación de las políticas o medidas de seguridad.

Todas las cuentas de acceso a los sistemas y recursos del Cloud son personales e intransferibles, cada usuario es responsable por las cuentas de acceso asignadas y las transacciones que con ellas se realicen.

Son permitidos hasta 5 intentos de ingreso en el servidor de presentación, después del quinto intento el usuario será bloqueado y solo podrá desbloquearse por la Administración del Cloud mediante caso en la plataforma de soporte.

El usuario podrá modificar la contraseña inicial de acceso que le sea asignada, siempre y cuando cumpla las políticas de seguridad de contraseñas establecidas por Gigas en los servidores, para esto debe presionar las teclas ctrl+alt+fin y presionar la opción change password, las políticas se mostraran al momento de intentar cambiar la contraseña en el servidor.

Ningún usuario, debe almacenar o utilizar información, archivos, imagen, sonido, software u otros que estén protegidos por derechos de autor de terceros sin la previa autorización de estos.

5.3. Políticas de red

El internet en los servidores esta inactivo, solo se tiene acceso a páginas relacionadas con las funciones y actividades de SAP Business One y sus complementos.

Los puertos abiertos internamente son los establecidos en la guía de administración de SAP Business One, cualquier apertura de puerto adicional, debe solicitarse a la Administración del Cloud mediante caso en la plataforma de soporte.

Los puertos abiertos externamente varían por cada una de las services unit, para el consumo de un servicio en específico desde internet debe solicitarse la URL y puerto a la Administración del Cloud mediante caso en la plataforma de soporte.

5.4. Políticas Administrativas y de Instalación

La sesión de usuario de terminal y office 365 se cierra automáticamente después de un tiempo de inactividad.

Las bases de datos productivas deben iniciar con la pablara SBO_ Seguido del nombre de la base de datos, este nombre no debe superar los 23 caracteres.

Las bases de datos de pruebas deben iniciar con la palabra TEST_ Seguido del nombre de la base de datos, este nombre no debe superar por ningún motivo los 23 caracteres.

No debe existir dentro de las carpetas compartidas, backups de bases de datos ni archivos con contraseñas.

La instalación y desinstalación de software, la configuración lógica, conexión a red, instalación y desinstalación de dispositivos, será realizada únicamente por personal Autorizado de Gigas o Consensus.

Consensus no se hace responsable por la administración y licenciamiento de software diferente al definido en este documento, cualquier software de terceros debe ser soportado y licenciado directamente por su fabricante o proveedor.

Las modificaciones realizadas a software de terceros siempre deben realizarse con acompañamiento de un consultor de Consensus y/o Gigas, mediante solicitud en la plataforma de soporte.

No se brindarán contraseñas administrativas a personal ajeno a Consensus.

Cada cliente tiene un usuario de base de datos con el cual puedan realizar labores de consultoría en sus propias bases, a través de Crsytal report o HANA Studio, Consensus no se hace responsable por los querys ejecutados con estos usuarios ya que son responsabilidad propia de cada cliente.

Consensus cuenta con usuarios de base de datos para labores de soporte, calidad y desarrollo, cualquier ejecución de querys realizada con estos usuarios es responsabilidad de Consensus.

No esta permito a ningún aplicativo o desarrollo la ejecución directa de querys en el motor, cualquier ejecución de consultas sobre la base de datos debe hacerse mediante una conexión establecida bajo uno de los siguientes métodos:

- Conexiones mediante controlador HDBODBC o B1CRHPROXY.
- Service Layer.
- DIAPI.
- Vistas.
- B1IF.

Las conexiones con aplicativos o servicios externos debe realizarse mediante protocolos seguros y siguiendo las siguientes directrices.

- Los servicios deben establecer comunicación mediante puertos seguros https, TLS, etc.
- En caso de ser requerido establecer conexión VPN punto a punto (costo adicional).
- Establecer reglas en firewall donde se permita la comunicación solo desde ciertas IP Publicas.

La instalación de cualquier software adicional debe ser solicitado a través de la plataforma de soporte, este debe ser aprobado por Consensus y/o Gigas, en la solicitud debe enviarse los requerimientos mínimos para su funcionamiento.

El cliente debe pagar por el consumo de recursos adicionales ocasionado por un software de terceros, que sea para uso propio.

El software mínimo instalado en los servidores debe ser el indicado dentro de la guía de implementación de SAP Business One Cloud Control Center y que el software complementario cumpla con los lineamientos de seguridad establecidos en este documento. A continuación, se define el software propietario de SAP y complementario a instalar en cada en cada uno de los siguientes servidores.

Servidor controlador de Dominio PDC.
Servidor Cloud Control Center CCC.

Servidor de licencias.
Servidor de base de datos.
Servidor de Servicios.
Servidor de Presentación.
Servidor de User Access Portal.
Servidor de Integraciones.

Name	HANA	Shared or SU	Applications or services
PDC		Shared	Primary Domain Controller
CCC		Shared	CCC***, SAP HANA Studio, RSP, HANA Client*, Shared Folders, Chrome
LS		Shared	License Server, HANA Client*
HANA01		SU01	SAP HANA Database & AFL, HANA Client*, SLD Agent**
SERVICES01		SU01	xApp Framework, Analytics***, Mailer, Job Service, Backup Service, Service Layer
PS0101		SU01	B1 Client / DI-API, BA Gatekeeper***, Add-ons, DTW, CR, HANA Client*, SLD Agent
PORTAL		Shared	IIS with RDS Portal, User Access Portal (BA)***
B1IF01		SU01	B1 Integration Framework*** + B1 Client, HANA Client*

Software Propietario de SAP

De acuerdo con la guía de administración de SAP Business One Cloud Control Center en la siguiente imagen se visualiza la aplicación o servicio a instalar en cada uno de los servidores:

5.4.1.1. Servidor controlador de Dominio (PDC).

Es un servidor con sistema operativo Windows Server donde se instala el controlador de dominio que permite el ingreso a todos los servidores mediante SSO.

Este servidor es administrado únicamente por el proveedor del PaaS, ni los clientes, ni Consensus tiene acceso a este servidor.

5.4.1.2. Servidor Cloud Control Center (CCC).

Servidor donde se tiene el landscape y base de datos del Cloud Control Center, en este servidor corre el servicio que permite la administración local y remota de todas las tareas administrativas del Cloud.

Solo los administradores de Consensus tienen acceso a este servidor, dentro del Software instalado se encuentra:

- SQL Server: Software propietario de Microsoft donde se almacena la base de datos estándar de SAP SLDDATA.
- Landscape de CCC: Servicio estándar de SAP que permite la administración de la base SLDDATA mediante navegador WEB de manera local y externa.
- SAP Hana Studio: Software propietario de SAP para la gestión de las bases de datos de los clientes.
- RSP: Software propietario de SAP que permite comunicación directa con soporte de SAP Global, esta herramienta se usa para la ejecución de tareas que permiten la corrección de incidentes, envío de reportes o bases de datos SAP Global, Gestión de Backups automáticos.
- Hana Client: Driver propietario de SAP que permite la comunicación entre servidores de Windows y Linux.
- SLD Agent: Servicio propietario de SAP para ejecución de tareas automáticas ejecutadas desde el landscape.

5.4.1.3. *Servidor* de licencias (LS):

Servidor SLES donde se instala el servicio estándar de SAP Business One License Manager, este servicio se conecta directamente al landscape del CCC para la gestión del licenciamiento de los usuarios finales.

En este servidor también se instala el cliente de hana, driver que permite la comunicación con el servicio que administra la base SLDDATA

Solo los administradores del Cloud tienen acceso a este servidor.

5.4.1.4. Servidor de base de datos (HANA).

Servidor SLES donde se instalan los siguientes componentes:

- SAP HANA Database: Instancia donde se almacenan las bases de datos de los clientes, en esta instancia se crean usuarios de bases de datos para administración y usuarios de bases de datos para los clientes con permisos restrictivos.
- AFL: Librerías propietarias de SAP instaladas en la instancia de hana, permiten realizar procesamiento analítico avanzado. Predicción, Grafos, Análisis de texto, etc.
- Hana Client: Driver propietario de SAP que permite la comunicación entre servidores de Windows y Linux.
- SLD Agent: Servicio propietario de SAP para ejecución de tareas automáticas ejecutadas desde el landscape.

Solo los administradores del Cloud tienen acceso a este servidor.

5.4.1.5. Servidor de Servicios (SERVICES).

Servidor SLES donde se instalan los siguientes componentes:

- xApp Framework: Framework propietario de SAP para desarrollo de aplicaciones.
- Analitycs: Servicio que permite gestionar las librerías AFL.
- Job Services: Servicio que permite el envío de correos y notificaciones desde SAP Business One.
- Backups Services: Servicio que permite la generación automática de Backups, a través del landscape, RSP o HANA Studio
- Service Layer: API de SAP que tiene como propósito consumir datos y servicios de SAP Business One.
- Mobile Services: Servicio de SAP exclusivo para el uso de aplicativos móviles de SAP Business One.
- Web Client: Ultimo Servicio liberado para SAP 10, está basado en los principios de diseño de SAP Fiori encapsulando los procesos clave de SAP Business One y la lógica de negocio junto con una experiencia de usuario avanzada.
- SLD Agent: Servicio propietario de SAP para ejecución de tareas automáticas ejecutadas desde el landscape.

Solo los administradores del Cloud tienen acceso a este servidor.

5.4.1.6. Servidor de Presentación (PS):

Servidor donde ingresa el usuario final.

- SAP Business One Crystal Reports: Herramienta de SAP que permite crear reportes personalizados e importarlos a SAP Business One.
- SAP Business One Data Transfer Workbench (DTW): Herramienta externa de SAP Business One para carga de datos masivos a través de plantillas.
- SAP Business One Client: Interfaz de usuario que permite interactuar con la base de datos de SBO a través de escritorio remoto.

- SAP Business One Browser Access Server: Interfaz de usuario que permite interactuar con la base de datos de SBO a través de navegador web
- SAP Business One DIAPI: API que permite realizar procesos en SAP por SDK.
- SAP Business One Excel Reports and Interactive Analysis: Herrameinta de SAP que permite gestionar informes analíticos desde Excel.
- SAP HANA Studio: Herramienta que permite gestionar las bases de datos contenidas en la instancia de HANA.
- SLD Agent: Servicio propietario de SAP para ejecución de tareas automáticas ejecutadas desde el landscape.

5.4.1.7. Servidor de User Access Portal (PORTAL).

- SAP Business One User Access Portal: Servicio de SAP que controla el acceso de SAP Business One Gatekeeper.
- SLD Agent: Servicio propietario de SAP para ejecución de tareas automáticas ejecutadas desde el landscape.

5.4.1.8. Servidor de Integraciones (B1IF).

- B1IF: Servicio que permite la integración de datos hacia SAP Business One, tal como integraciones tipo POS.
- SLD Agent: Servicio propietario de SAP para ejecución de tareas automáticas ejecutadas desde el landscape.
- Manager SCCO: Para SAP Customer Checkout se debe tener instalado el manager que permita hacer seguimiento y trazabilidad a los documentos tipo POS

5.4.2. Software Complementario

Adicional se tiene instalado software complementario o adicional que permiten facilitar la implementación o uso de SAP Business One, este software se lista a continuación:

5.4.2.1. Servidor Cloud Control Center (CCC):

- 7-Zip: Herramienta libre que permite descomprimir paquetes de cualquier tipo.
- Google Chrome: Navegador oficial de Google usado para la administración del Cloud a nivel interno.
- Notepad ++: Herramienta libre que permite la validación de logs y código fuente de manera sencilla.
- Putty: Herramienta libre que permite la administración remota por ssh de los servidores SLES.
- Zabixx Agent: Herramienta que permite el monitoreo continuo de los diferentes servidores.

5.4.2.2. Servidor de presentación (PS)

- Office 365: Herramienta de microsoft usado por aquellos clientes que tienen licencia de office 365.
- Foxit rader/Acrobat Reader: Herramienta que permite visualizar documentos tipo PDF.
- Biable: AddOn externo que permite generar informes en excel, basado en la información contenida en la base de datos de SAP Business One, establece una conexión por HDBODBC.
- BPAC: AddOn de Consensus que permite adaptar SAP Business One a la normalidad tributaria colombiana, establece conexión por DIAPI.
- Integración de Nomina: Integración entre Consensus y Designer que permite cargar la nómina mensualmente a la base de datos de SAP Business One, establece conexión por HDBODBC.

- Enterpryze: Integración entre Consensus e Enterpryze que permite integrar datos maestros y documentos con un aplicativo móvil, establece conexión mediante un servicio.
- Visual Studio 2010 y 2015: Software usado por Consensus que permite realizar seguimiento por código fuente a las diversas incidencias del addOn BPAC que no sea posible determinar su causa por consultoría o soporte.
- Servicios de Facturación electrónica: Servicio de Consensus que permite el envío de documentos de marketing generados por SAP Business One a la DIAN, establece una conexión mediante service layer.
- Servicio de Mi portal: Servicio de Consensus que permite generar reportes en PDF a sus diferentes proveedores y/o clientes por internet, establece una conexión mediante service layer..
- 7-Zip: Herramienta libre que permite descomprimir paquetes de cualquier tipo.
- Google Chrome: Navegador oficial de Google usado para la administración del Cloud a nivel interno.
- Notepad ++: Herramienta libre que permite la validación de logs y código fuente de manera sencilla.

5.5. Políticas de Respaldo

En las características de seguridad de Windows el firewall local aparece como deshabilitado.

Sin embargo, el proveedor PASS administra todas la conexiones entrantes y salientes a través de hardware perimetral como los siguientes:

- FIREWALL AVANZANDO
- SISTEMAS PREVENCIÓN DE INTRUSOS
- ESCANEADO DE ANTIVIRUS EN EL PERÍMETRO
- CERTIFICACION ISO 27001
- SEGURIDAD FÍSICA
- PROTECCIÓN DE REDES ZOMBIES

Adicional se cuenta con un esquema de backups mediante tareas programadas en el servidor de Base de datos SLES, estos backups se copian diariamente a un servidor en la nube bajo la siguiente política:

- Diario para los 14 últimos días.
- Quincenal para las últimas dos quincenas.
- Mensual para los últimos 11 meses.
- En total se guardan 27 backups.

6. Cumplimiento de las Políticas de Seguridad.

Consensus SAS, Gigas y los Clientes, son responsables de conocer y asegurar la implementación de las políticas de seguridad, dentro de sus áreas de responsabilidad, así como del cumplimiento de las políticas por parte de su equipo de trabajo.

7. Contacto

Si desea hacer sugerencias a Consensus o Gigas para mejorar los contenidos, la información y los servicios ofrecidos debe dirigirse, al correo electrónico sac@consensussa.com.