Políticas de Seguridad
Consensus Cloud Control Center

Autor: Carlos González
Fecha de Creación V1: agosto de 2020
Fecha de Modificación V2: septiembre de 2020
Fecha de Modificación V3: febrero de 2024

Contenido

1. Introducción

Teniendo en cuenta que para Consensus la seguridad es un aspecto crítico en cualquier entorno y especialmente en los servicios ofrecidos a nuestros clientes, queremos dar a conocer mediante el siguiente documento, las políticas de seguridad bajo las cuales se rige el servicio conocido como Consensus Cloud.

Con estas políticas no solo buscamos tomar medidas preventivas, sino que buscamos cubrir una necesidad absoluta actual, brindando directrices de índole técnica y de organización, a fin de proteger y resguardar nuestros sistemas y la información en ellos contenida.

Considerando que la información es el factor más valioso de nuestros clientes y que esta información se encuentra en un ambiente compartido, se hace necesario la definición e implementación de estas 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 bajo los conceptos de Confidencialidad, Integridad y Disponibilidad.

Por lo anterior, 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 servicio Consensus Cloud, entendiendo como premisa que la responsabilidad por la seguridad de la información es de todos y cada uno.

2. Objetivo

Definir e implementar unas políticas de seguridad, que den pautas para la gestión y uso adecuado del entorno Consensus Cloud, bajo los siguientes objetivos clave:

Seguridad: Mantener la confidencialidad, integridad y disponibilidad de los datos en el ambiente.

Acceso: Controlar permisos a los recursos, aplicaciones y servicios instalados.

Monitoreo: Auditar, identificar y mitigar posibles amenazas.

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.

Services Unit: Conjunto de servidores que cuentan con el hardware y software instalado para el uso de SAP Business One en una arquitectura OnDemand.

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.
- Por defecto, se tiene establecido un cierre de sesión automático por inactividad de dos horas.

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.
- Se tiene establecido por cada unidad de servicio una VLAN interna, que segmenta la red local y evita que se pueda tener comunicación directa entre otras unidades de servicio, esta política eleva en un alto porcentaje la seguridad y dificulta al atacante o malware, la intrusión o propagación de virus que pueda afectar los sistemas de información o arquitectura.
- Se tienen establecidos a nivel de firewall reglas de conectividad que permiten conectividad hacia los diferentes servidores de presentación y servicios, solo desde países en las cuales los clientes o Consensus tiene operación, evitando ser objetivo de atacantes o grupos de ciberdelincuentes que se encuentren en otros países donde no tenemos ninguna operación.
- 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

5.4. Políticas Administrativas y de Instalación

- La sesión de usuario de terminal se cierra automáticamente después de un tiempo de inactividad, estandarizado en una hora.
- No debe existir bajo ningún concepto dentro de las carpetas del perfil del usuario, 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.
- Con el fin de evitar posibles intrusiones en la plataforma de administración del CCC, se tiene configurado el doble factor de autenticación para el ingreso a esta, lo cual garantiza que solo el personal autorizado de Consensus tenga acceso a esta plataforma.
- 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.
- Con el fin de evitar ser atacados por vulnerabilidades conocidas, se deben realizar trimestralmente actualizaciones y parcheos de sistema operativos en todos los servidores Windows del Cloud.
- No está 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 ODBC, HDBODBC o B1CRHPROXY.
  - Service Layer.
  - DIAPI.
  - Modelamiento HANA
- Las conexiones con aplicativos o servicios externos debe realizarse mediante protocolos seguros y siguiendo las siguientes directrices.
  - Los servicios deben establecer comunicación mediante protocolos y puertos seguros https, TLS, etc.
  - Las conexiones por VPN, debe establecerse en una sesión en conjunto con el proveedor de infraestructura, Consensus y el cliente.
  - Establecer reglas en firewall donde se permita la comunicación solo desde ciertas IP Publicas.

5.5. Políticas de Respaldo

- Se cuenta con un esquema de backups de las bases de datos productivas 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 al año.
- Se cuenta con un esquema de backups completes de la instancia de los últimos 8 días.
- Ante una posible contingencia de secuestro de información o perdida de datos, se implementó un servidor exclusivo de backups, el cual envía los respaldos de las bases de datos productivas generadas diariamente, a un servidor el cual se integra a una cuenta OneDrive de Consensus, garantizando así, tener en nuestra custodia estos respaldos.
- Con el fin de garantizar una recuperación más eficiente ante un ataque informático, Se tienen implementados en los servidores centrales y de presentación, respaldos de información avanzados de la máquina virtual, los cuales se realizan con una periodicidad de ocho días.

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.