ESPECIFICACIONES DE INFRAESTRUCTURA

Logo

Description automatically generated

Infraestructura

Tabla de contenido

[Confidencialidad 5](#_Toc142663837)

[Descripción general SAC 6](#_Toc142663838)

[Infraestructura SaaS 7](#_Toc142663839)

[Ecosistema de tecnologías y metodologías 10](#_Toc142663840)

[Esquema general de producto 12](#_Toc142663841)

[Componentes globales del sistema Sac 13](#_Toc142663842)

[Directorio activo Azure 15](#_Toc142663843)

[Monitoreo y disponibilidad 16](#_Toc142663844)

[Normativa, administración y seguridad 17](#_Toc142663845)

[Mecanismo de continuidad y seguridad 18](#_Toc142663846)

[Procesos de apoyo 18](#_Toc142663847)

[Ciberseguridad 18](#_Toc142663848)

[Conectividad y transferencia 19](#_Toc142663849)

[Propiedad de la información 19](#_Toc142663850)

[Plan de continuidad 20](#_Toc142663851)

[Estrategia de continuidad 20](#_Toc142663852)

[Sistemas operativos 20](#_Toc142663853)

[Sitios web 20](#_Toc142663854)

[Bases de datos 20](#_Toc142663855)

[Verificación de respaldos 20](#_Toc142663856)

[Posibles escenarios de falla 21](#_Toc142663857)

[Falla de uno de los servidores web 21](#_Toc142663858)

[Falla del servidor de bases de datos principal 21](#_Toc142663859)

[Ataque Rasonware 21](#_Toc142663860)

[Clasificación de los incidentes 22](#_Toc142663861)

[Tiempos de respuesta 22](#_Toc142663862)

[Disponibilidad de servicios Azure 23](#_Toc142663863)

[Disponibilidad de servicios SAC 23](#_Toc142663864)

[Mecanismos de integración y acceso 24](#_Toc142663865)

[Sac API 26](#_Toc142663866)

[Entidades de datos 28](#_Toc142663867)

[Integraciones 29](#_Toc142663868)

[Integración Marcador Telefónico 29](#_Toc142663869)

[Integración Eva Platform 30](#_Toc142663870)

[Integración SacDialer 31](#_Toc142663871)

[Requerimientos 32](#_Toc142663872)

[Integración con sistemas SMS 34](#_Toc142663873)

[Integración a través de servicios web 34](#_Toc142663874)

[Generación de archivos 34](#_Toc142663875)

[Integración con correo electrónico 35](#_Toc142663876)

[Integración a través de servicio web 35](#_Toc142663877)

[Envío de mensajes a través de protocolo SMTP 36](#_Toc142663878)

[Generación de archivos 36](#_Toc142663879)

[Integración con sistemas IVR 37](#_Toc142663880)

[Integración a través de servicios web 37](#_Toc142663881)

[Generación de archivos 37](#_Toc142663882)

[Límites de almacenamiento en la nube 38](#_Toc142663883)

[Requerimientos técnicos equipos de escritorio 39](#_Toc142663884)

[Requerimientos técnicos equipos móviles 39](#_Toc142663885)

[Componentes requeridos 40](#_Toc142663886)

[Contáctenos 41](#_Toc142663887)

[Colombia 41](#_Toc142663888)

[Perú 41](#_Toc142663889)

[Estados Unidos 41](#_Toc142663890)

# Confidencialidad

Este documento y cualquier archivo anexo son de uso exclusivo y confidenciales de Effective Computer Solutions S.A.S. y el cliente o empresa para el cual fue generado. Queda estrictamente prohibido la utilización, copia o reimpresión de este por cualquier persona sin la debida autorización de Effective Computer Solutions S.A.S.

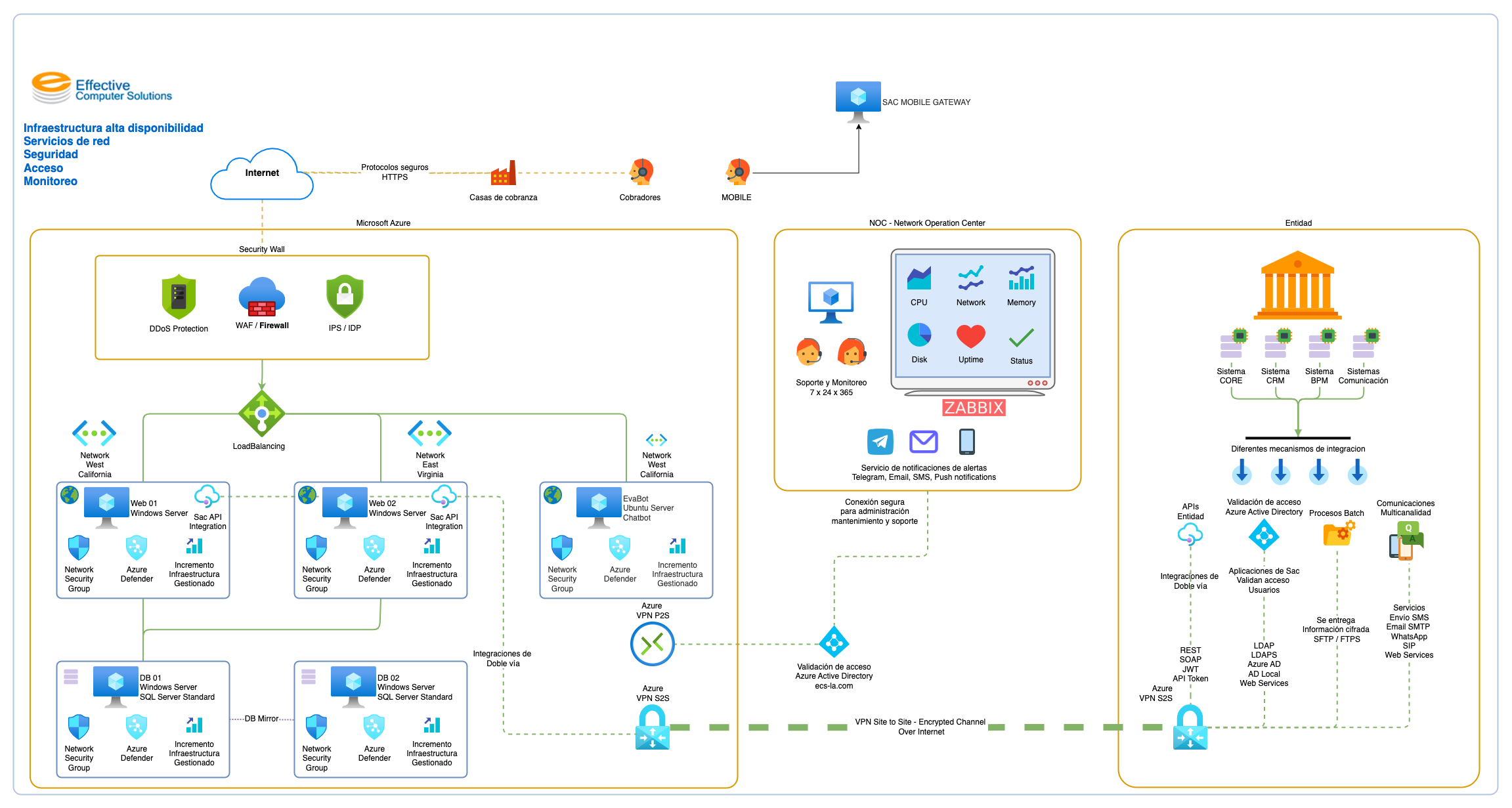
# Descripción general SAC

Logo

Description automatically generated

SAC (Sistema de Administración de Cobranzas) es un software diseñado, desarrollado e implementado con el objetivo de facilitar, estructurar y potencializar la gestión de cobro de cartera en todas sus etapas y aspectos, optimizando la productividad, eficiencia y la eficacia de los agentes gestores encargados de dicha función, proveyendo información detallada y en tiempo real.

# Infraestructura SaaS



Esta imagen corresponde al esquema de infraestructura general para cada una de nuestras nubes con las cuales brindamos el servicio de SAC, en la cual se describen los componentes básicos requeridos para el funcionamiento en esquema de alta disponibilidad y las posibles integraciones que se puedan presentar con nuestros clientes.

Respecto a la transferencia de información, se aclara que todas las comunicaciones se encuentran cifradas a través de certificados SSL TLS 1.2, y que desde internet solo se puede utilizar el protocolo HTTPS, otros protocolos como RDP, FTPS/SFTP, MSSQL solo pueden ser usados a través de conexión VPN ya sea Site to Site (Entre entidades) o Point To Site (Personas a entidades). Con esto se aclara que la entidad que se conecta con el servicio Sac también debe cumplir o acoplarse con los mecanismos de seguridad indicados debido a que hacen parte de las practicas más seguras en la actualidad. Si la entidad indica que trabaja con estándares mayores como por ejemplo TLS 1.3 ECS adecuará su infraestructura para estar al nivel de lo solicitado por la entidad.

Los canales de comunicación de las nubes que ofrece la plataforma Sac, pertenecen y son gestionadas y garantizadas por Microsoft Azure, entregando anchos de banda de 1000 Mbps/125 MBs.

Cada usuario consume un ancho de banda de 128 KB. Se sugiere que por cada usuario se utilice un promedio para el cálculo de 128 kb con el objetivo de poder cargar toda la información de un cliente para su gestión de entre 1 a 3 segundos.

El servicio será ofrecido en modalidad de alta disponibilidad y los componentes que conforman la nube que brinda el servicio, tendrá contingencia N+1 y sus componentes estarán ubicados en zonas geográficas distantes que para este caso será la región de Estados Unidos, y las zonas Virginia y California.

La infraestructura de SAC puede ser incrementada en cualquier momento generando una interrupción mínima, este incremento será controlado y previamente autorizado y coordinado con la entidad.

Los entornos que muestran la gráfica son entornos únicamente productivos, aparte del entorno productivo se otorga el entorno de certificación y a su vez a nivel del equipo de desarrollo también se cuenta con entorno diferente con lo cual se quiere aclarar que los entornos se encuentran separados.

Este diagrama corresponde a un esquema de funcionamiento SaaS de alta disponibilidad donde para cada componente hay otro componente igual que reemplazará su funcionamiento en caso de falla.

**Firewall:** Es un componente especializado que evita que el producto sea objeto de hackeos aprovechando vulnerabilidades del producto o la infraestructura aún no conocidas.

**Balanceador:** Se encarga de redirigir las peticiones Http entre los servidores Web.

**Servidores Web:** Se encargan de publicar las diferentes aplicaciones de la plataforma SAC.

**Servidores de bases de datos:** Se encargan de poner en servicio la base de datos y mantener al día la réplica. Se rec

**Redes:** Los componentes de la red de alta disponibilidad se encuentran distribuidos en la región Estados Unidos y en diferentes zonas geográficas; Este y Oeste. Dependiendo de la entidad esta región y zona se pueden modificar con el objetivo de lograr un mejor tiempo de respuesta (latencia).

**Servidor EvaBot:** Contiene funcionamiento de bot con inteligencia artificial para mantener conversaciones con clientes a través de la API de Whatsapp o WebChat.

**Comunicación:** El esquema de conectividad seguro proporciona protocolos cifrados para cualquier transferencia, ej.; HTTPS, FTPS, SFTP, LDAPS, etc.

**Gestión y monitoreo:** Contamos con un centro de monitoreo que se encuentra disponible 7x24x365. Se utiliza el software de monitoreo Zabbix que evalúa los elementos más importantes para el estado y la disponibilidad de la infraestructura.

El soporte a la infraestructura se realiza a través de conexión VPN controlada a su vez por Azure Active Directory.

Los administradores de la infraestructura reciben alertas de seguridad por diferentes medios; correo electrónico, mensajes de texto, y notificaciones push.

**Crecimiento:** El crecimiento de la infraestructura se realiza con base en comportamiento histórico y evaluación de tendencias de crecimiento, una vez se detecta la necesidad se establece con la entidad la correspondiente autorización para realizar los cambios que permitan soportar los nuevos requisitos de capacidad.

**Conexión con entidad:** Para garantizar conexión segura a los servicios internos de la entidad, se establece una conexión VPN Site to Site con los mecanismos de cifrado más seguros. Sobre esta conexión VPN se consumen servicios en doble vía. Algunos de los servicios más usados sobre la VPN son: Autenticación, transferencia de archivos de datos de interfaces, consumo de servicios de telefonía SIP, integración con marcadores telefónicos, comunicación con sistemas Core para reportar compromisos, acuerdos de pago, costos de cobranza, pagos en línea, consultas generales para conocer el estado en línea de las obligaciones del cliente o disponible en sus cuentas del pasivo, integración con servicios CRM, integración con sistemas BI entre otros.

**SAC API:** Corresponde al sistema de integración de SAC con sistemas externos con el cual se podrá tener comunicación de doble vía entre los sistemas de la entidad y la plataforma de cobranzas. Se detalla más adelante.

# Ecosistema de tecnologías y metodologías

Diagram

Description automatically generated

Sac utiliza los lenguajes de programación provistos y soportados por Microsoft en su mayoría C# a través de .Net Core LTS y .Net Framework. Para el desarrollo de las aplicaciones móviles se usa el lenguaje de programación Swift para dispositivos iOS provista directamente por Apple, y Android Studio provista directamente por Google para dispositivos Android. Relacionado a la base de datos se utiliza Microsoft SQL Server en su versión Estándar. Importante destacar que SacMobile al ser desarrollado como aplicaciones nativas se puede utilizar con eficiencia la posibilidad del trabajo sin red/conexión debido a que cuenta con mecanismos de sincronización y trabajo offline.

Los productos que conforman la plataforma Sac son desarrollados con componentes web estándar poniendo como prioridad la usabilidad del sistema y la orientación a los procesos y procedimientos del usuario.

En cuanto a componentes se aclara que Sac está construido con componentes entregados por Microsoft, Google y Apple, y que estos componentes no requieren que nuestros clientes adquieran licencias adicionales para su uso. Las licencias de sistema operativo y de motor SQL se encuentran incluidos dentro del servicio y nuestros clientes no tienen que adquirir licencias por este concepto.

ECS tiene certificado vigente ISO 27001 y CMMI DEV Y SRV, lo cual garantiza en gran medida que los integrantes del equipo de trabajo desarrollan nuestros productos con los estándares de calidad y seguridad requeridos por el mercado. Nuestro producto se encuentra desarrollado con tecnología Microsoft, Google y Apple. El motor de base de datos principal es Microsoft SQL Server. Para las aplicaciones iOS y Android se utiliza desarrollo nativo con el fin de aumentar el nivel de compatibilidad y también la velocidad de las aplicaciones. Las aplicaciones web y las APIs se publican mediante servidor web Internet Information Server de Microsoft que corre sobre Windows Server. Las aplicaciones son desarrolladas en metodología MVC interconectadas a sistemas API para la interacción con la base de datos. Nuestro proceso de desarrollo incluye la verificación de código fuente en busca de vulnerabilidades mediante la herramienta SonarQube.

**CMMI:** El propósito del modelo CMMI es evaluar la madurez de los procesos de una organización y proporcionar orientación sobre cómo mejorar los procesos, con el objetivo de mejorar los productos.

**ISO27001:** SO 27001 es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. El sistema se construyó orientado a las mejores prácticas Owasp y a nivel de infraestructura se realizan pruebas de vulnerabilidad.

# Esquema general de producto

Diagram

Description automatically generated

# Componentes globales del sistema Sac

Timeline

Description automatically generated

En este esquema se puede ver cómo interactúan los diferentes componentes de la plataforma Sac.

**Sistema Core:** Corresponde al sistema de la entidad que genera los datos relevantes para la cobranza.

**Otros sistemas:** Corresponde a otros sistemas que dependiendo de las necesidades del negocio se pueden integrar con Sac a través de nuestro sistema estándar SacAPI.

**Datos requeridos:** Corresponde a los insumos necesarios para que el gestor de cobranzas pueda realizar una cobranza efectiva, a nivel general se requiere información de; Clientes, obligaciones, pagos, direcciones, teléfonos, codeudores, garantías, entre otros.

**Múltiples tecnologías de integración:** Sac recibe los datos requeridos del core a través de diferentes tipos de tecnologías. Estas tecnologías se usan dependiendo de cada entidad y sus necesidades específicas. Entre las tecnologías más comunes de intercambio de información se encuentran; Archivos de texto, Conexión directa a base de datos, Servicios web, entre otros. Adicional a ello, esta información puede ser entregada por mecanismos seguros de transferencia como lo pueden ser Ftps, Linked Server, Web Service HTTPs entre otros.

Comunicación segura: Toda la transferencia de información se realiza a través de protocolo HTTPS con certificado SSL/TLS1.2.

**Procesos diarios:** Corresponde a la automatización a través de procesos de carga de datos provenientes del core y el análisis de estos para disponer de la mejor manera los datos con el objetivo de entregarlos al gestor para que pueda realizar su trabajo de manera eficiente. Este proceso actualiza la información de clientes y sus obligaciones, calcula el nivel de recaudo, carga nueva información de contactabilidad entre otros.

**Bases de datos:** Sac utiliza el motor SQL de Microsoft desde la versión 2008 en adelante. La edición recomendad es la estándar.

**Servidor Web:** Sac utiliza IIS de Microsoft. Este producto viene como componente estándar del sistema operativo Windows Server.

# Directorio Activo Azure

Diagram

Description automatically generated

Para realizar la conexión con el directorio es necesario registrar la aplicación en el directorio de la entidad y posterior a ello la entidad debe entregar la información relacionada a:

1. DomainName
2. TenantId
3. ClientId
4. AppId
5. ObjectId

Sac trabajará con las políticas que tenga implementadas el directorio activo de Azure, incluyendo los factores de múltiple asignación.

Sac soporte autenticación LDAP/LDAPS, si la entidad cuenta con validación AAD (Azure Active Directory) ya no es necesario utilizar LDAP/LDAPS, sin embargo, se aclara que su uso puede ser habilitado.

Sac puede consultar el Directorio Activo de la entidad y crear el usuario de manera automática, si es que este usuario se encuentra inscrito a un grupo nombrado de determinada manera, por ejemplo; si un usuario se encuentra en el grupo SupervisoresCobranza, este será creado dentro del grupo de Supervisores de Sac.

# Monitoreo y disponibilidad

Graphical user interface, application, Excel

Description automatically generated Graphical user interface, application

Description automatically generated

Effective Computer Solutions facilita a las entidades conocer el estado de la infraestructura que tiene contratada para brindar el servicio SaaS. Estas herramientas permiten evaluar cada uno de los componentes involucrados en el servicio, específicamente en los factores relacionados con; uso de la CPU, uso de la memoria, ocupación del espacio en disco, respuesta y uso de la red. A su vez, se brinda información relacionada al tiempo en línea del servicio con lo cual se puede hacer un seguimiento al cumplimiento de los SLA.

La disponibilidad de la plataforma Sac es ofrecida garantiza un 99.95% de disponibilidad del sistema mes a mes.

Esta disponibilidad se puede ver afectada por los pasos a producción o ajustes del sistema o aplicación de parches y actualizaciones. Estas afectaciones serán informadas por lo menos con una antelación de 72 horas y no afectará la operación.

La información de monitoreo y logs de eventos se puede entregar mediante diferentes mecanismos de integración que serán evaluados y configurados al momento de la implementación de ser requerido.

Adicional al monitoreo que se realiza desde el Zabbix y Uptime, desde Azure se cuenta con alertas de capacidad e informes de vulnerabilidades entre otros.

# Normativa, administración y seguridad

El centro de datos por defecto para brindar los servicios en la nube de la plataforma Sac es Microsoft Azure. Este proveedor de servicios en la nube cuenta con reportes SOC 1, 2 y 3 vigentes, que garantizan que cuentan con controles estrictos para el acceso a sus instalaciones, contingencia N+1 de todos los componentes involucrados (canales de comunicación, electricidad, espacio, control de incendios, etc.).

Revisar los informes SOC vigentes y el cumplimiento de normativas en:

Información:

[Azure compliance documentation | Microsoft Learn](https://learn.microsoft.com/en-us/azure/compliance/)

Reportes:

[Controles del sistema y de la organización (microsoft.com)](https://servicetrust.microsoft.com/viewpage/SOC)

Respecto a los procesos internos de ECS se debe aclarar que son compatibles y se alinean con los procesos de seguridad que brinda Microsoft Azure, y que, a su vez, ECS cuenta con certificación vigente ISO27001 y CMMI SRV/DEV.

Ampliar detalle en:

Políticas de calidad:

[Calidad | SAC SAAS (sac-saas.com)](https://www.sac-saas.com/calidad)

Privacidad y Habeas Data:

[Política tratamiento de datos | SAC SAAS (sac-saas.com)](https://www.sac-saas.com/pol%C3%ADtica-tratamiento-de-datos)

# Mecanismo de continuidad y seguridad

## Procesos de apoyo

Para garantizar la continuidad del servicio ECS protege sus infraestructuras con firewall perimetral, endurecimiento de la seguridad de los servidores y componentes que conforman el servicio, copias de respaldo o snapshots de máquinas virtuales cada 4 horas, copias de respaldo de la base de datos diaria por 7 días, semanal por 4 semanas y replica de almacenamiento web externas a las máquinas virtuales.

Otros mecanismos con los cuales se apoya la continuidad del servicio son a través de las auditorías que se realizan a los procesos de Backups, pruebas de restauración de los backups, y pruebas al desarrollo de los planes de continuidad, todo esto asociado a las buenas prácticas y a lineado a las definiciones de procesos y políticas de calidad y seguridad de ECS. Se puede ampliar esta información con el manual de seguridad de la información de ECS entregado al momento de la contratación.

## Ciberseguridad

Otro nivel de protección en una capa a más alto nivel; se cuenta con Azure Cloud Defender, el cual protege todas las máquinas virtuales a través de Antivirus, Antispyware, Anti Ransomware y ofrece análisis de vulnerabilidades y alertas de seguridad que nos permite como que les permiten a los administradores actual de manera proactiva ante posibles brechas de seguridad.

Los productos desarrollados para la plataforma Sac pasan por un proceso de calidad y seguridad mediante Per Review de código, escaneos de seguridad a través de SonarQube, actividades de Pentesting y auditorìas de red por parte de terceros, entre otros.

Los datos en las bases de datos se tienen encriptados a través de la tecnología Microsoft TDE (Transparent Data Encription) la cual permite que los datos de backups realizados no puedan ser consultados si no se tiene una llave/certificado de seguridad. Esta información se encuentra en custodia del departamento de infraestructura y la gerencia general de ECS.

## Conectividad y transferencia

Desde Internet solo se hace visible la comunicación a través de HTTPS por lo cual, para asuntos de administración y el uso de otros protocolos se hace necesario establecer una VPN S2S o P2S desde la cual solo los administradores y operadores autorizados mediante Azure Active Directory pueden ingresar a realizar actividades de configuración, diagnostico, corrección y ajustes. La transferencia de información solo puede ser usada por la entidad hacia el protocolo FTPS/SFTP establecido, con esto se aclara que la entidad no puede ingresar a la infraestructura por otro medio.

## Propiedad de la información

Se aclara que todos los datos son propiedad de la entidad y como tal una vez que se termine el contrato, se garantiza que toda la información será entregada y posterior a dicha entrega y confirmación de recepción se realizará un borrado seguro de la información.

Con el objetivo de dar mayor seguridad a los datos, en los entornos diferentes al productivo (certificación, pruebas, desarrollo), se realizará un proceso de ofuscación de la información de clientes, obligaciones, referencias, direcciones y teléfonos, de tal manera que no sea posible identificar a quien pertenece los datos y que de esta manera no se convierta en un riesgo de fuga de datos.

# Plan de continuidad

## Estrategia de continuidad

### Sistemas operativos

Todos los servidores se encuentran protegidos mediante copia de seguridad tipo snapshot con copia cada 4 horas, esta copia se mantiene durante todo el mes. La copia protege al sistema operativo y todo lo que se encuentre en la unidad C. Esta configuración se realiza independiente del tipo de ambiente, es decir, se protege; Producción, Certificación y Pruebas.

### Sitios web

Se realiza una copia de seguridad cada 8 horas de los sitios web, estos sitios se copian en un almacenamiento externo (Azure File Storage), es decir, queda una copia en uso (local) y copia remota. La copia remota se comprime y se mantiene por un mes.

### Bases de datos

El servicio cuenta con backup diario que se mantiene durante una semana, backup semanal que se mantiene durante 4 semanas y backup mensual que se mantiene por 12 meses.

Una copia de la base de datos se pondrá a disposición de la entidad mediante protocolo FTP Seguro para que la mantenga en sus instalaciones como parte de la estrategia de continuidad.

### Verificación de respaldos

Diariamente se revisa que los procedimientos de backup se estén ejecutando sin novedad, si se presentan novedades se procede a crear incidente de seguridad y realizar seguimiento hasta su resolución.

Cada mes se realiza un proceso de auditoría de las copias de seguridad realizadas donde se verifica el acceso a la información una vez restaurados los datos. Este proceso genera un informe que puede ser entregado a la entidad cuando lo soliciten.

## Posibles escenarios de falla

### Falla de uno de los servidores web

RTO: Inmediato

RPO: Inmediato

la estrategia de continuidad consiste en que el segundo servidor lo reemplaza de manera automática. El balanceador de cargas distribuye el tráfico hacia uno solo de los servidores.

La estrategia para recuperar el servicio consiste en restaurar la imagen del servidor web que se realiza cada 4 horas.

### Falla del servidor de bases de datos principal

RTO: 5 minutos

RPO: Inmediato

La estrategia de continuidad consiste en habilitar el segundo servidor que en su funcionamiento normal se encuentra en modo espejo. Se redireccionan las aplicaciones al servidor secundario.

La estrategia para recuperar el servicio consiste en restaurar la imagen del servidor de bases de datos que se realiza diariamente.

### Ataque Rasonware

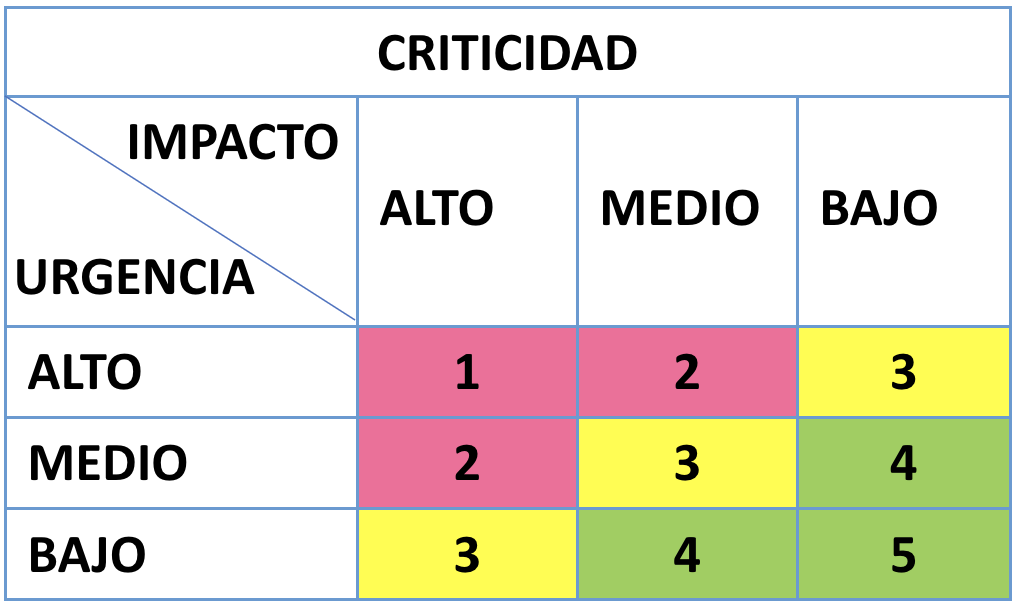
RTO: 4 horas

RPO: Sitios web 4 horas.

RPO: Bases de datos 16 horas.

La estrategia de continuidad consiste en reconfigurar los sistemas operativos, aplicaciones y bases de datos en nuevas máquinas virtuales.

## Clasificación de los incidentes



Seguridad de la información / GI\_PRE\_CRITICIDAD\_INCIDENTES

## Tiempos de respuesta

Table

Description automatically generated

Seguridad de la información / GI\_PRE\_CRITICIDAD\_INCIDENTES

# Disponibilidad de servicios Azure

|  |  |  |
| --- | --- | --- |
| **Producto** | **Disponibilidad** | **Observación** |
| Máquinas virtuales | 99.9 | 729.27 de 730 horas mes |
| Máquinas virtuales SQL | 99.9 | 729.27 de 730 horas mes |
| Application Gateway | 99.95 | 729.63 de 730 horas mes Incluye VPN S2S y P2S |
| VPN Gateway | 99.9 | 729.27 de 730 horas mes |
| Azure Virtual Network | 99.9 | 729.27 de 730 horas mes |
| Azure Backup | 99.9 | 729.27 de 730 horas mes |
| Azure Storage Account | 99.9 | 729.27 de 730 horas mes |

**Nota:** Effective Computer Solutions realizará procesos de mantenimiento previamente coordinado con nuestros clientes, estas ventanas de mantenimiento a pesar de generar indisponibilidad no afectarán el cálculo de SLA por su naturaleza, es decir, es una indisponibilidad coordinada/aceptada con nuestros clientes.

# Disponibilidad de servicios SAC

La disponibilidad del servicio SAC es de 99.67%, lo que corresponde a 727.59 de 730 horas al mes.

# Mecanismos de integración y acceso

Graphical user interface, diagram, application

Description automatically generated

Sac usa múltiples mecanismos de acceso para lograr integraciones con los sistemas de nuestros clientes, entre ellos se encuentran:

* Conexión VPN de sitio a sitio para establecer un mecanismo seguro de envío. La VPN se establece a través de Azure VPN.
* Conexión a través de sistema de transferencia de información segura como por ejemplo SSH/FTPS en el cual solo se autoriza acceso a una IP específica. Las IPS que se conectan a este servicio deben ser IPS públicas fijas y solo se permitirán los puertos específicos, es decir, no se abre la comunicación a todos los puertos, sino que solo se aceptan conexiones a los puertos FTP o SSH respectivamente.
* Cuando se trata de Sac OnPremisse podemos realizar conexiones directas a carpetas de red con la seguridad provista por la red interna de la entidad. Para este caso se solicita que los permisos de red de lectura y escritura sean otorgados a nombre propio y que no se habiliten los permisos para todos los usuarios.

Los mecanismos de integración también son muy variados y dependen mucho de las posibilidades que tenga la entidad, con esto se quiere aclarar que ECS se acomoda a la tecnología que posea la entidad de tal manera que se puedan agilizar los tiempos. Entre los mecanismos que podemos utilizar para transferir la información son:

* Sitio FTP Seguro ya sea por SSH o FTPS, si se trata de FTP la conexión se debe obligar a TLS 1.2/SSL.
* Azure File Storage
* AWS Buckets
* GCP Buckets
* Servicios web a la medida para la cual se solicita que la autenticación sea a través de API Key o API Token y origen autorizado a través de CORS.
* Recurso compartido dentro de la red local con los privilegios de lectura y escritura a nombre propio y no para todos los usuarios.
* Transferencia directa entre bases de datos autorizando únicamente el usuario en específico que realiza la transferencia.

A través de los mecanismos mencionados, se logra realizar procesos de Importación/Exportación de datos de manera eficiente entre la entidad y el servicio de Sac.

# Sac API

Corresponde al sistema de integración de SAC con sistemas externos con el cual se podrá tener comunicación de doble vía entre los sistemas de la entidad y la plataforma de cobranzas. Se detalla más adelante.

|  |  |  |
| --- | --- | --- |
|  |  |  |
| **Categoria** | **Nombre** | **Descripción** |
| Auth | login | Método para realizar autenticación. Después de ejecutar este método se establecerá los parámetros de seguridad para consultar los demás métodos. El token recibido tendrá una vigencia o vencimiento. |
| Cliente | addEmailAdreess | Permite agregar una nueva dirección de correo electrónico. |
| Cliente | addPhoneNumber | Permite agregar un nuevo teléfono. |
| Cliente | addPhysicalAdreess | Permite agregar una nueva dirección. |
| Clientes | getCustomerInfo | Entrega información básica del cliente incluyendo la última gestión realizada y el estado de gestión actual del cliente. Entrega los datos de contactabilidad del cliente; Teléfonos, direcciones, correos. |
| Gestión | addPromise | Permite agregar un compromiso de pago a un cliente en específico. |
| Gestión | addVisit | Permite agregar una solicitud de visita a un cliente en específico. |
| Gestión | getAssignment | Entrega la lista de trabajo que determinado usuario tiene pendiente por gestionar. |
| Gestión | getCustomerManagementHistory | Entrega un listado con las gestiones que se le han realizado al cliente.  El listado se encuentra ordenado de manera descendente por fecha de gestión. |
| Gestión | getLatestManagement | Entrega la última gestión realizada al cliente consultado. |
| Gestión | getWhatsappConversation | Método especializado que permite iniciar continuar una conversación a través de la herramienta Whatsapp.  Para poder usar este método es requerido que el módulo especializado de gestión digital esté configurado. Para usar este método previamente se debe haber conseguido el id de conversación el cual se obtiene mediante la ejecución del método startWhatsappConversation |
| Gestión | loadManagementHistory | Permite la carga de gestiones masivas a SAC cuyo origen es gestión externa o gestión masiva digital desde otros sistemas de información. |
| Gestión | sendEmail | Permite el envío correos electrónicos. Antes de usar este método se debe realizar la configuración del proveedor de correos electrónicos en el módulo de notificaciones. |
| Gestión | sendSms | Permite el envío de mensajes SMS. Antes de usar este método se debe realizar la configuración del proveedor de servicios de mensajes sms en el módulo de notificaciones. |
| Gestión | startWhatsappConversation | Método especializado que permite iniciar una conversación a través de la herramienta Whatsapp.  Para poder usar este método es requerido que el módulo especializado de gestión digital esté configurado. |
| Jurídico | addLegalProcess | Permite agregar un proceso jurídico. El estado del proceso se puede omitir, en consecuencia se creará con estado activo. Los demás valores opcionales serán cargados como nulos o vacíos. |
| Jurídico | addLegalProcessAudience | Permite agregar audiencias a un determinado proceso jurídico. Para usar este método se debe conseguir la identificación del proceso jurídico mediante el método: getLegalProcesses. |
| Jurídico | addLegalProcessStep | Permite agregar una etapa a determinado proceso jurídico. Para usar este método se debe conseguir la identificación del proceso jurídico mediante el método: getLegalProcesses. El estado de la etapa se puede omitir, en consecuencia se creará con estado activo. |
| Jurídico | getLegalProcesses | Entrega un listado con los procesos jurídicos que los abogados han creado a los diferentes deudores. |
| Jurídico | getLegalProcessSteps | Entrega el listado de las etapas del proceso jurídico consultado.  Para usar este método se debe conseguir la identificación del proceso jurídico mediante el método: getLegalProcesses. |
| Pagos | addPayment | Permite agregar un pago realizado por el cliente en un sistema de información externo. |
| Pagos | getPayments | Entrega el listado de pagos realizado por un cliente en un rango determinado de tiempo. Si no se envían fechas el método retorna todos los pagos registrados para el cliente enviado en los parámetros.  Si no se envía el número del crédito, el sistema devuelve los pagos que el cliente ha realizado a todos sus créditos. |

# Entidades de datos

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Interfaces de entrada** | | | | | | | |
|  |  | |  | |  |  | |
| **N** | | **Interfaz** | **Descripción** | | **Tabla** | | **Frecuencia sugerida** |
| 1 | | Clientes | Clientes, codeudores, garantes | | t\_intermedia\_clientes | | Diaria en la madrugada |
| 2 | | Teléfonos | Teléfonos de los clientes, codeudores, garantes | | t\_intermedia\_telefonos | | Diaria en la madrugada |
| 3 | | Direcciones | Direcciones de los clientes, codeudores, garantes | | t\_intermedia\_direcciones | | Diaria en la madrugada |
| 4 | | Obligaciones en servicios | Préstamos de los clientes | | t\_intermedia\_obligaciones | | Diaria, a demanda |
| 5 | | Pagos en servicios | Pagos de los préstamos de los últimos 5 días | | t\_intermedia\_pagos | | Diaria en la madrugada, inmediata mediante servicio web |
| 6 | | Correos | Correos electrónicos de los clientes, codeudores, garantes | | t\_intermedia\_correos | | Diaria en la madrugada |
| 7 | | Referencias | Referencias de los clientes | | t\_intermedia\_referencias | | Diaria en la madrugada |
|  |  | |  | |  |  | |
| **Interfaces de salida** | | | | | | | |
|  |  | |  | |  |  | |
| **N** | **Interfaz** | | **Descripción** | **Tabla** | | | **Frecuencia sugerida** |
| 1 | Historial de gestiones | | Contiene la información detallada de gestiones realizadas. | t\_intermedia\_salida\_clientes | | | Diaria o de acuerdo a las necesidades del negocio. |
| 2 | Teléfonos | | Teléfonos nuevos creados por los gestores de cobranzas | t\_intermedia\_salida\_telefonos | | | Diaria o de acuerdo a las necesidades del negocio. |
| 3 | Direcciones | | Direcciones nuevas creadas por los gestores de cobranzas | t\_intermedia\_salida\_direcciones | | | Diaria o de acuerdo a las necesidades del negocio. |
| 4 | Acuerdos de pago | | Base de datos de los acuerdos de pago con información al día | t\_intermedia\_salida\_historia\_gestion | | | Diaria o de acuerdo a las necesidades del negocio. |

# Integraciones

## Integración Marcador Telefónico

Diagram

Description automatically generated

La implementación y sus requisitos depende del marcador telefónico de la entidad y de sus capacidades de integración.

## Integración Eva Platform

Diagram

Description automatically generated

Para brindar el servicio de EVA es requerido por parte de la entidad que dispongan de una troncal SIP estándar para la comunicación con la planta telefónica del servicio EVA.

Si la planta telefónica de la entidad es una planta OnPremisse se debe contar adicional con el establecimiento de una VPN Site To Site entre la entidad y la infraestructura de Eva Platform en Microsoft Azure. Si por el contrario la planta de la entidad está en Internet a nivel público, no es necesario establecer una VPN S2S sino gestionar las correspondientes autorizaciones a nivel IP.

## Integración SacDialer

Diagram

Description automatically generated

Diagram

Description automatically generated

SacDialer utiliza el estándar SIP para realizar llamadas, con esto se quiere indicar que una planta telefónica que soporte SIP y tenga a disposición extensiones SIP estándar puede ser utilizada por SacDialer para realizar llamadas. Se debe considerar que sea estándar SIP, de lo contrario se tendrán inconvenientes en la comunicación como por ejemplo que el audio no se escuche de unos de los extremos.

### Requerimientos

* Requerimientos mínimos para equipos de computo de los usuarios: Procesador i3 Octava generación o equivalente, 4 GB Ram, 128 GB espacio en disco, cualquier sistema operativo.
* Los usuarios deben usar un navegador compatible y actualizado (Chrome, Edge, Firefox, Safari)
* Apertura de puertos entre el componente de EVA y el navegador del usuario
* Protocolo SIP Estándar
* Información de las extensiones asignadas a cada usuario. Esta información se configura en Sac. que el componente de EVA OnPremisse
* Requiere que el componente de EVA OnPremisse pueda establecer conexión con Azure
* Las grabaciones serán eliminadas posterior a 6 meses para evitar que el storage se sature (Comparte almacenamiento con sistema de backups)
* Se requiere instalar componente en servidor Linux o en su defecto Docker (Linux), 8 CPU, 8 GB RAM, 64 GB Storage (Estos valores son mìnimos y su aumento depende de la cantidad de usuarios concurrentes que vayan a realizar llamadas,)

## Integración con sistemas SMS

Sac puede integrarse a sistemas de envío de mensajes SMS a través de consumo de servicios web o archivos de texto.

### Integración a través de servicios web

Sac puede integrarse a sistemas de envío de mensajes de mensajes SMS a través de consumo de servicios web, para esto es requerido conocer la URL del servicio, el sistema de seguridad, el método para autenticar y por último la definición del método para el envío de los mensajes.

Los requisitos para realizar esta integración son:

1. URL: Dirección en Internet del servicio expuesto para este fin.
2. Sistema de seguridad: Indicar si el servicio requiere de ser invocado desde una IP en específico o si el servicio requiere un API Key o un API Token
3. Obtener token: Indicar el método por el cual se puede obtener el token para realizar peticiones al servicio, en esta información debe venir también el usuario y clave para realizar la solicitud del token.
4. Método para el envío de mensajes: Se requiere el nombre del método y la documentación de su uso.

Nota: A excepción del punto 4, la información indicada se requiere por cada entorno de trabajo; Desarrollo, Pruebas, Producción.

### Generación de archivos

En caso tal que la entidad no tenga un servicio SMS para recibir las peticiones directamente de Sac, lo que se recomienda es configurar un reporte que permita descargar la información de acuerdo con los lineamientos del proveedor, y siempre y cuando la información requerida se encuentre en las tablas de Sac.

## Integración con correo electrónico

La integración entre Sac y un sistema de envío de mensajes de correo electrónico se puede realizar mediante varios mecanismos:

1. Conexión a proveedor de envíos a través de servicio web.
2. Conexión a servidor de correo a través de protocolo SMTP.
3. Generación de archivos desde Sac para enviar al proveedor

### Integración a través de servicio web

Sac puede integrarse a sistemas de envío de mensajes de correo a través de consumo de servicios web, para esto es requerido conocer la URL del servicio, el sistema de seguridad, el método para autenticar y por último la definición del método para el envío de los correos.

Los requisitos para realizar esta integración son:

1. URL: Dirección en Internet del servicio expuesto para este fin.
2. Sistema de seguridad: Indicar si el servicio requiere de ser invocado desde una IP en específico o si el servicio requiere un API Key o un API Token
3. Obtener token: Indicar el método por el cual se puede obtener el token para realizar peticiones al servicio, en esta información debe venir también el usuario y clave para realizar la solicitud del token.
4. Método para el envío de mensajes: Se requiere el nombre del método y la documentación de su uso.

Nota: A excepción del punto 4, la información indicada se requiere por cada entorno de trabajo; Desarrollo, Pruebas, Producción.

### Envío de mensajes a través de protocolo SMTP

Sac puede enviar mensajes de correo electrónico a través del uso del protocolo SMTP el cual es un estándar. Se puede utilizar servidores OnPremise o servicios en la nube como por ejemplo Microsoft 365 (Office.com).

Los requisitos para realizar esta integración son:

1. Servidor SMTP: Ip o nombre DNS del servidor.
2. Usuario y clave de la cuenta de correo con privilegios de conexión y envío. Este punto es relevante debido a que servicios como por ejemplo Office 365 deben dar los privilegios correctos a esta cuenta para que esta se pueda conectar y enviar el mensaje.
3. Privilegios de conexión SMTP.

### Generación de archivos

En caso tal que la entidad no tenga un servicio SMTP o un proveedor con servicio web para recibir las peticiones directamente de Sac, lo que se recomienda es configurar un reporte que permita descargar la información de acuerdo con los lineamientos del proveedor, y siempre y cuando la información requerida se encuentre en las tablas de Sac.

## Integración con sistemas IVR

Sac puede integrarse a sistemas de envío de mensajes IVR a través de consumo de servicios web o archivos de texto. Sac puede enviar el texto del mensaje que debe ser dicho al cliente al ser llamado o puede indicar una url de un audio específico para este fin. El Servicio web debe soportar este funcionamiento.

### Integración a través de servicios web

Sac puede integrarse a sistemas de envío de mensajes de mensajes SMS a través de consumo de servicios web, para esto es requerido conocer la URL del servicio, el sistema de seguridad, el método para autenticar y por último la definición del método para el envío de los mensajes.

Los requisitos para realizar esta integración son:

1. URL: Dirección en Internet del servicio expuesto para este fin.
2. Sistema de seguridad: Indicar si el servicio requiere de ser invocado desde una IP en específico o si el servicio requiere un API Key o un API Token
3. Obtener token: Indicar el método por el cual se puede obtener el token para realizar peticiones al servicio, en esta información debe venir también el usuario y clave para realizar la solicitud del token.
4. Método para el envío de mensajes: Se requiere el nombre del método y la documentación de su uso.

Nota: A excepción del punto 4, la información indicada se requiere por cada entorno de trabajo; Desarrollo, Pruebas, Producción.

### Generación de archivos

En caso tal que la entidad no tenga un servicio SMS para recibir las peticiones directamente de Sac, lo que se recomienda es configurar un reporte que permita descargar la información de acuerdo con los lineamientos del proveedor, y siempre y cuando la información requerida se encuentre en las tablas de Sac.

# Límites de almacenamiento en la nube

Garantizamos el almacenamiento por servicio, grupo y usuario durante el tiempo de vigencia del contrato, permitiendo a la entidad el crecimiento en espacio de almacenamiento.

Una vez se llegue a los límites de almacenamiento aceptados (ocupación de más del 70%) se procede a programar el aumento de dicho almacenamiento en un horario que no afecte la operación y previamente coordinado con la entidad.

El servicio cuenta con backup diario que se mantiene durante una semana, backup semanal que se mantiene durante 4 semanas.

# Requerimientos técnicos equipos de escritorio

|  |  |
| --- | --- |
| Procesador | Intel Celeron 1.8 GHz o superior |
| Memoria RAM | 4 GB |
| Sistema operativo | Windows 8.1 o superior, se recomienda que el sistema operativo tenga soporte de su fabricante. |
| Espacio en disco | 1 GB |
| Navegador | Google Chrome, Microsoft Edge, Firefox, Safari, o cualquier navegador compatible con soporte vigente. |

# Requerimientos técnicos equipos móviles

|  |  |
| --- | --- |
| Teléfono móvil | Smartphone |
| Memoria | 4 GB o superior |
| Sistema Operativo | Android 8.1 o superior |
| Sistema Operativo | iOS 12 o superior |
| Espacio en disco | 1 GB o superior |

# Componentes requeridos

Los componentes indicados a continuación, se utilizan de diferentes maneras en la creación y funcionamiento de la plataforma Sac, estos componentes son usados mientras que cuenten con soporte vigente por su fabricante, en caso que un componente deje de tener soporte, este se reemplazará por un componente equivalente que tenga soporte vigente.

* Windows Server 2019 o superior
* Microsoft SQL Server Standard 2008 o superior
* Internet Information Server 7 o superior
* .Net Framework 4 en adelante
* .Net Core 3 / 6
* URL Rewrite
* Filezilla FTP Server
* Navegadores soportados:
  + Google Chrome
  + Mozilla Firefox
  + Safari
  + Microsoft Edge Chrome
  + Opera
  + Nota: Se soporta cualquier navegador con soporte vigente del fabricante.
* Lenguajes de desarrollo:
  + C#
  + Swift
  + Android
  + SQL
  + JavaScript
  + Node.js
  + Angular
  + Python

# Contáctenos

[A picture containing logo

Description automatically generated](https://www.sac-saas.com/)

<https://www.sac-saas.com/>

## Colombia

Calle 72 No. 12-65 Of. 501

Bogotá, Colombia.

soporte@ecs-la.com , info@ecs-la.com

Mobile: +57 318 619 88 14 / 15 / 16

## Perú

Calle José María de la Jara y Ureta 470, Santiago de Surco

Lima, Perú

Tel: +51 977 804 634

## Estados Unidos

ECS Team LLC 66 W Flagler Street

Suite 900 - #5475

Miami, FL 33130

|  |  |
| --- | --- |
| [https://encrypted-tbn1.gstatic.com/images?q=tbn:ANd9GcTfbKdENDenXoOkEP1GCZ6AGAMbTWN-ICBeyVA1gaQ4azTiuHLsuw](https://twitter.com/EffectiveCS) | <https://twitter.com/EffectiveCS> |
| [https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcSYKkgPzL2AEpxv1ttafUpmlGYdUd_mmwpC1YkYdc2kIcSiXNZ63g](https://www.facebook.com/EffectiveCS) | <https://www.facebook.com/EffectiveCS> |
| [https://encrypted-tbn3.gstatic.com/images?q=tbn:ANd9GcSQccNo7XOW1wPUfGiYWAOLx64uK9oLBfHw8OL6RNFkW_nxtc5o](https://www.linkedin.com/company/ecs-la/mycompany/) | <https://www.linkedin.com/company/ecs-la/mycompany/> |