

Bogotá, 10 de febrero de 2023

Señores
Servicio Nacional de Aprendizaje, SENA
Bogotá D.C.

Respetados Señor(es)
Supervisor del Contrato Adobe ETLA No. CO1.PCCNTR.4533103

Supervisor Principal
Diego Armando Cristancho

Departamento de Sistemas
John Ricardo Calderón

ACTA DE CUMPLIMIENTO No. 009

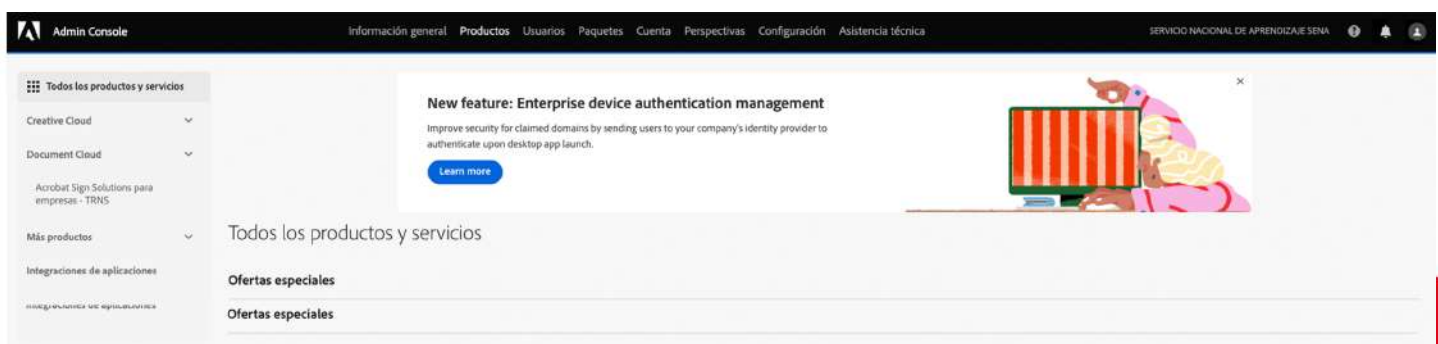
Por medio del presente comunicado se hace constancia del Acta N° 009, donde informamos las infraestructuras tecnológicas y de seguridad, dando cumplimiento al contrato No. CO1.PCCNTR.4533103., donde nos indica las **Obligaciones específicas del contratista:**

c) Disponer de la infraestructura física, tecnológica y de seguridad que garantice la prestación del servicio requerido.

Contamos con 6 infraestructura tecnológicas y de seguridad.

- Consola de Administración de las suscripciones de Adobe (AdminConsole)
- Portal de cursos de educación virtual (Media Pro)
- Plataforma de voucher de certificación adobe Certified Associate (ACA) (Certiport)
- Mesa de ayuda de soporte técnico (Plataforma GLPI)
- Plataforma de correos masivos (SendPulse)
- Software de creación de contenidos web (Articulate 360)

1. Contamos con una consola de administración donde encontramos el licenciamiento Creative Cloud.



LA INFRAESTRUCTURA TECNOLÓGICA ADOBE

La Adobe Admin Console es un espacio centralizado para administrar los derechos de Adobe de toda la organización.

La Admin Console se encuentra dividida por 8 pestañas de le permite realizar varias tareas.

1. Información general

En la sección Información general se recoge gran cantidad de información sobre licencias de productos. En ella figura el estado de las licencias de su plan, es decir, el número de licencias asignadas del total disponible.

Además, hay disponibles algunos enlaces rápidos para añadir usuarios y administradores.

Seleccionar organización

Un administrador puede pertenecer a varias organizaciones. Si una entidad tiene varias filiales que existen como organizaciones separadas o cada filial tiene un acuerdo de licencia independiente, puede asignarse el mismo administrador para todas ellas.

Si es administrador de varias organizaciones, puede cambiar de organización mediante la herramienta de selección de organizaciones. En la organización seleccionada aparecerá una marca de verificación verde junto al nombre de la organización.

Si la organización forma parte de una Global Admin Console, aparecerá el icono de la jerarquía junto al nombre de la organización. También verá la ruta de la organización y podrá determinar la posición de la organización dentro de la jerarquía. Por ejemplo, en la captura de pantalla, el administrador es miembro de la organización Athletic Shoe Division y la ruta de la Global Admin Console de dicha organización es ACME HQ > Athletic Shoe Division, donde Athletic Shoe Division es una organización secundaria de la organización ACME HQ.

2. Productos

Esta pestaña está visible para: administradores del sistema, administradores de productos y administradores de perfiles de productos

- Empresas

La página Productos de Admin Console ofrece opciones para administrar los productos y los perfiles de productos. Los perfiles de productos le permiten activar todos o parte de los servicios y aplicaciones de Adobe disponibles en un plan y personalizar la configuración asociada a un determinado producto o plan. De este modo, puede asignar administradores, denominados administradores de productos, a los perfiles de productos. Estos administradores son quienes añaden usuarios finales a los perfiles de productos que gestionan.

- Equipos

La página de productos de Admin Console permite asignar licencias de productos a usuarios. Para asignar una licencia de producto a un usuario o grupo, seleccione el producto deseado en la página Productos y haga clic en Añadir usuario.

Introduzca el nombre o la dirección de correo electrónico del usuario. Puede buscar los usuarios existentes o añadir un usuario especificando una dirección de correo electrónico válida y rellenando la información en la pantalla. Haga clic en Guardar. Se enviará un correo electrónico al usuario o grupo confirmando el acceso a la aplicación.

3. Usuarios

En la pestaña de Usuarios de Admin Console permite crear, buscar, actualizar y eliminar cuentas de usuario. Esas cuentas de usuario otorgan derechos a los usuarios finales de su organización para acceder a los productos y servicios de Adobe. También puede utilizar los flujos de trabajo de edición masiva para agregar usuarios o modificar los detalles de los usuarios y las asignaciones de licencias. Para obtener más información

4. Paquete

En la pestaña Paquetes de la Admin Console están disponibles las siguientes funcionalidades. Haga uso de ellas cuando tenga previsto implementar aplicaciones de Creative Cloud y Document Cloud para los usuarios finales en la entidad.

- Descargar paquetes preconfigurados utilizando Plantillas de Adobe.
- Crear paquetes personalizados de Licencias de usuario designadas o Licencias de dispositivo compartido (para centros educativos) con la configuración y las aplicaciones que quiera que tengan los usuarios finales.
- Activar las notificaciones por correo electrónico, de manera que se le notifique cuando estén disponibles nuevas versiones de productos.
- Ver los paquetes anteriores que hayan creado usted u otros administradores de su organización. También, ver detalles de un determinado paquete y seguir las actualizaciones disponibles para las aplicaciones del paquete.
- Descargar las herramientas de TI, como Remote Update Manager y Adobe Update Server Setup Tool.
- Descargar la herramienta de línea de comandos Adobe Extension Manager para instalar extensiones y complementos a partir del formato de contenedor de archivos ZXP.

5. Cuenta

La página Cuenta de Admin Console muestra los detalles de todos los contratos y acuerdos asociados con su organización. También muestra la fecha de aniversario o finalización del contrato con un indicador de contratos vencidos.

Si es un cliente de equipos de Adobe, vaya a Cuenta > Cuenta en la Admin Console para administrar fácilmente sus facturas y editar sus datos de pago o la dirección de facturación. Puede renovar sus licencias adquiridas a través del abono de equipos. También puede realizar las tareas siguientes:

- Ver los detalles de los productos y licencias del plan actual
- Ver período de renovación
- Añadir productos
- Editar los datos de pago
- Cambiar el propietario del contrato
- Ver detalles de la próxima factura
- Ver, imprimir y descargar las facturas

6. Perspectivas

Son los datos de asignación de licencias que permiten realizar un seguimiento de las licencias asignadas frente a las que se han adquirido. Los análisis de los datos se corresponden con todos los productos aplicables desde la última fecha de vencimiento o la fecha de entrada en vigor del Contrato de licencias de duración determinada para empresas (ETLA).

Los administradores del sistema pueden ver estos datos de asignación de licencias como gráficos en la pestaña Detalles de la Admin Console. Gracias a estos, las organizaciones (que hayan suscrito un ETLA) pueden hacer un seguimiento del registro de licencias asignadas. Los datos se representan en la vista Mes y la vista Año en curso.

Los administradores del sistema también pueden ejecutar un informe en cualquier momento para descargar los datos que se muestran en el panel.

Registro de auditoría

El registro de auditoría ayuda a garantizar la continuidad en el cumplimiento normativo, protege contra cualquier acceso sin autorización al sistema y audita comportamientos sospechosos dentro de su organización.

Como administrador del sistema, tiene visibilidad completa de los cambios realizados en Admin Console. Puede buscar en el registro de auditoría por tipo de acciones, cuándo ocurrieron y quién las realizó. Luego, vea y descargue estos informes para un análisis más detallado. Más información.

Informes de asignaciones

Mediante los informes de asignación de licencias, puede realizar un seguimiento de los datos de asignación de licencias de su organización y planificar las implementaciones de licencias de usuario. Los datos de asignación de licencias solo se usan para licencias de usuario designadas de productos de Creative Cloud y Document Cloud adquiridos en virtud del Contrato de licencias de duración determinada para empresas. Más información.

7. Configuración:

Esta pestaña está visible para: administradores del sistema y administradores de almacenamiento.

- Privacidad y contactos de seguridad

En caso de que se produzca un incidente de seguridad relacionado con las soluciones de software, se enviarán notificaciones a los responsables del cumplimiento correspondientes. Como administrador del sistema, debe especificar quiénes son los responsables de la seguridad, la protección de datos y el cumplimiento para garantizar una notificación rápida. Para obtener más detalles

- Configuración de la consola

Gracias a la configuración de la consola, puede añadir notas personalizadas para los usuarios finales y podrá utilizarlas para comunicarse con ellos acerca de cómo recibir ayuda si tienen problemas o requieren asistencia técnica.

Elija un idioma de correo electrónico predeterminado para la organización, para recibir mensajes de correo electrónico sobre el estado de las cuentas, como cambios de suscripción o de caducidad de tarjetas de crédito. Si tiene un abono de equipos comprado directamente en Adobe, puede cambiar el nombre del equipo desde la Configuración de la consola.

- **Registros de activos**

Como administrador del sistema, puede descargar informes detallados acerca de cómo trabajan los usuarios finales con los activos empresariales, como carpetas, archivos y bibliotecas. Estos informes se denominan registros de activos.

- **Identidad (solo para empresas)**

Tipos de identidad permite a las organizaciones tener diferentes niveles de control sobre la cuenta y los datos del usuario. Afecta a su organización a la hora de almacenar y compartir activos.

- **Configuración de activos (solo para empresas)**

La configuración de recursos ofrece a las organizaciones control sobre la forma en que los empleados comparten sus recursos fuera de la organización. La configuración de activos se usa junto con otros sistemas de aplicación de política organizativa (no proporcionados por Adobe) para asegurarse de que los activos se compartan únicamente con las personas y organizaciones externas adecuadas.

- **Configuración de autenticación (solo para empresas)**

Configuración de autenticación admite varios niveles de protección mediante contraseña y políticas que garantizan la seguridad en todo momento. Puede indicar un nivel de protección mediante contraseña y aplicarlo a todos los usuarios de su organización.

- **Configuración del cifrado (solo para empresas)**

Configuración del cifrado genera una clave de cifrado específica para capas adicionales de control y seguridad.

8. Asistencia técnica

Para ponerse en contacto con el Servicio de atención al cliente de Adobe, diríjase a la página Asistencia técnica de Admin Console, que le permitirá:

Administrar los casos de soporte (solo empresas)

Crear casos (solo empresas)

Conectar con representantes del Servicio de atención al cliente de Adobe

Programar sesiones con el servicio de expertos

Examinar los temas de ayuda y los foros más populares

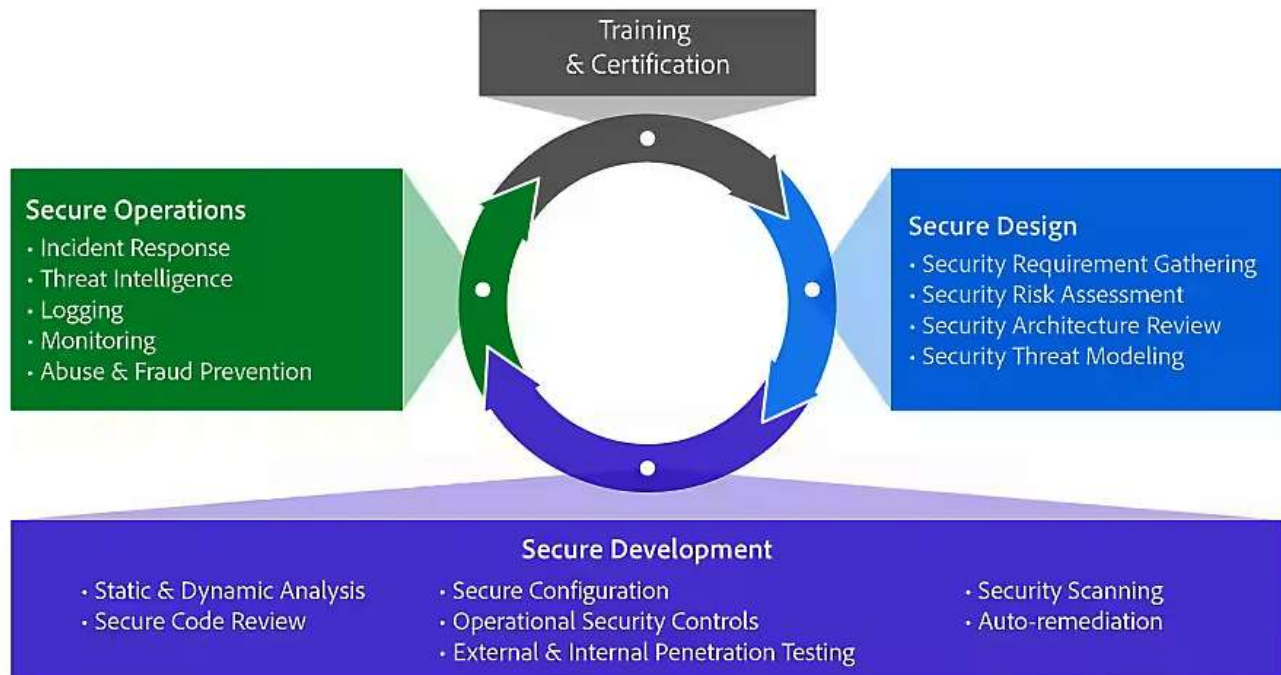
INFRAESTRUCTURA DE SEGURIDAD DE PRODUCTO ADOBE

El ciclo de vida del producto seguro de Adobe (SPLC)

Integrado en varias etapas del ciclo de vida del producto, desde el diseño y el desarrollo hasta el control de calidad, las pruebas y la implementación, Adobe Secure Product Lifecycle (SPLC) es la

base de la seguridad en Adobe. Adobe SPLC, un conjunto riguroso de varios cientos de actividades de seguridad específicas que abarcan prácticas, procesos y herramientas de desarrollo de software, define procesos claros y repetibles para ayudar a los equipos de desarrollo a incorporar seguridad en los productos y servicios y evoluciona continuamente para incorporar las mejores prácticas más recientes de la industria. Los investigadores de seguridad de Adobe brindan orientación completa sobre SPLC para los productos y servicios en función de una evaluación de posibles problemas de seguridad. Complementado por la participación continua de la comunidad, Adobe SPLC evoluciona para mantenerse actualizado a medida que ocurren cambios en la tecnología, las prácticas de seguridad y el panorama de amenazas.

Adobe SPLC está organizado en cuatro áreas clave que reflejan el diseño completo, el desarrollo, la implementación y el ciclo de vida operativo continuo de los productos y servicios de Adobe. Los controles de SPLC incluyen hojas de ruta de servicio, herramientas de seguridad y métodos de prueba que guían al equipo de seguridad para ayudar a abordar las 10 fallas de seguridad de aplicaciones más críticas del Open Web Application Security Project (OWASP) y los 25 errores de software más peligrosos de CWE/SANS.



Estrategia de seguridad de las aplicaciones de adobe

La estrategia de seguridad de aplicaciones de Adobe se centra en resolver los problemas de seguridad desde la raíz en lugar de tratar los síntomas. Hacemos esto “shifting left” e introduciendo seguridad temprano en el ciclo de vida del desarrollo de aplicaciones. Mediante el establecimiento de controles y mecanismos de seguridad en las fases de requisitos, arquitectura, diseño y codificación del desarrollo, ayudamos a “bake in” los controles de seguridad y reducir el alto costo de los cambios introducidos durante las pruebas posteriores etapas. Este enfoque también minimiza la posibilidad de riesgos de seguridad reales, lo que se traduce a una mejor seguridad para los clientes.

SPLC (el ciclo de vida seguro de los productos de adobe)

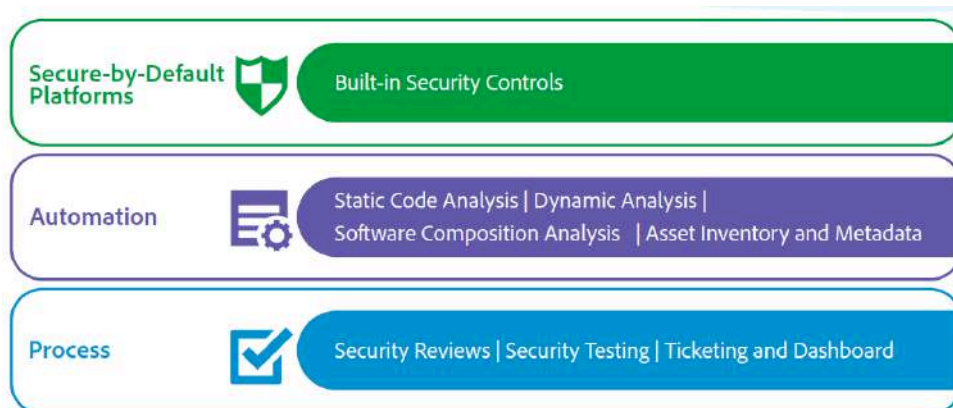
Integrado en el ciclo de vida del producto de software, desde el diseño y el desarrollo hasta la calidad seguridad, pruebas e implementación: el ciclo de vida seguro del producto (SPLC) de Adobe sirve como la base de todos los esfuerzos de seguridad en Adobe. Un conjunto riguroso de varios cientos de actividades específicas de seguridad, el SPLC define capacidades y procesos claros y repetibles para ayudar a los equipos de desarrollo que trabajan en los productos y servicios.

Adobe SPLC se implementa en toda la entidad y es verificado por investigadores de seguridad en el equipo de seguridad de las aplicaciones de Adobe, los cuales asesoran a los equipos de productos y servicios sobre las mejores prácticas para los controles de seguridad y estos controles se validan a través de la automatización. Los controles de SPLC incluyen hojas de ruta, herramientas de seguridad y métodos de prueba que guían al equipo de seguridad para abordar las 10 fallas de seguridad de aplicaciones más críticas de Open Web Application Security Projects (OWASP) y los 25 errores de software más importantes de CWE/SANS.

Application Security Stack

En Adobe, la creación de aplicaciones seguras comienza con Application Security Stack. Los equipos de productos comienzan usando plataformas que son seguras de manera predeterminada, verifican sus aplicaciones con varias capacidades de seguridad automatizadas y lo combinan todo con revisiones de seguridad y pruebas manuales.

Las tres (3) capas de proceso incluyen una variedad de herramientas y servicios basados en prácticas de seguridad modernas, enfocados en proteger los datos y los flujos de trabajo de los clientes, los cuales pueden ser utilizados por los equipos de productos de Adobe en su proceso de desarrollo para ayudar a garantizar que la seguridad esté integrada en cada aplicación de Adobe.



Plataformas seguras por defecto (Secure-By-Default Platforms)

Los desarrolladores de Adobe utilizan plataformas seguras por defecto preaprobadas para producir rutas bien estructuradas para el desarrollo rápido y seguro de los productos y servicios de Adobe. Estas rutas incluyen servicios de identidad y autorización verificados y aprobados, integraciones API, sistemas de mensajería, SDK y frameworks.

Las plataformas seguras por defecto no solo permiten una fácil escalabilidad, sino que también ayudan a verificar la correcta implementación de las funciones y configuraciones de seguridad. Basadas en dos principios fundamentales - detección y prevención-, estas plataformas incluyen un conjunto de soluciones de detección continua para identificar posibles usos inseguros, así como controles preventivos que ayudan a los desarrolladores de Adobe a lograr una postura segura por defecto para sus productos y servicios.

Las plataformas seguras por defecto ayudan a garantizar lo siguiente:

- **Uso seguro:** mediante el análisis continuo de un vasto conjunto de datos de configuración, registros y código fuente, se puede identificar rápidamente los errores de configuración de seguridad en los productos y servicios, descubrir cualquier desviación y alertar a los equipos de producto adecuados.
- **Controles de seguridad incorporados:** las inversiones en controles de seguridad que siguen las mejores prácticas, incluidos los mínimos privilegios, la denegación por defecto y la autenticación incorporada, ayudan a los equipos de productos a centrarse en su experiencia en el producto a la vez que protegen los datos y los flujos de trabajo de los clientes.

Automatización de la seguridad

En Adobe, la automatización permite que la seguridad de las aplicaciones se amplíe a toda la entidad y proporcione una cobertura de seguridad continua, a la vez que se mantiene al día con el rápido ritmo de la innovación.

Las iniciativas de análisis estático y dinámico, que tienen como objetivo el código de software, las colecciones de datos de configuración, el tráfico de solicitud/respuesta y los registros de aplicaciones, ayudan a Adobe a proteger todo el ciclo de vida de desarrollo del software.

Análisis estático de código: La plataforma automatizada de análisis de código aprovecha herramientas comerciales y de código abierto para escanear repositorios de código. Se proporciona la información directamente a los desarrolladores en línea con sus flujos de trabajo de desarrollo, cuando los problemas son más fáciles de mitigar. Estas herramientas, ayudan a Adobe a ofrecer la mayor seguridad posible en el código fuente.

Análisis dinámico: de forma similar a los enfoques del análisis estático del código, Adobe utiliza herramientas comerciales y personalizadas para identificar las vulnerabilidades de seguridad en tiempo de ejecución.

Análisis de la composición del software: Se hace un seguimiento de cerca al uso de componentes de terceros en los productos y servicios y se revisa periódicamente la postura de seguridad de estos componentes utilizando soluciones tanto internas como comerciales. Cuando se encuentra un componente vulnerable o que ha llegado al final de su vida útil, se alerta a los desarrolladores, lo que ayuda a garantizar una mitigación oportuna.

Inventario de activos y metadatos: un amplio conjunto de metadatos de toda la entidad ayuda a el equipo de seguridad de aplicaciones a obtener una visión más profunda de los productos y servicios de Adobe.

Proceso

La experiencia y los procesos de seguridad internos de Adobe constituyen la base de las iniciativas de seguridad. Se invierte continuamente en la formación tanto de los miembros del equipo de seguridad como de los estaciones de seguridad en tecnologías y enfoques emergentes. La gestión de multas, los paneles de control y la mitigación eficaz de los riesgos a través de la inteligencia de los adversarios y el modelado de amenazas crean el tejido que une las iniciativas de seguridad en una cadena eficaz.

Análisis de seguridad

Para proporcionar garantías de seguridad en todos los productos y servicios de Adobe, se comprometen en un proceso de colaboración para identificar problemas relacionados con la seguridad, determinar el nivel de seguridad y garantizar que los productos y servicios de Adobe sean seguros. Riesgo asociado a esas cuestiones, y tomar decisiones informadas sobre la mitigación o la aceptación del riesgo, entre ellas:

- **Modelado de amenazas:** la realización de un modelo de amenazas durante la fase de diseño ayuda a identificar los fallos de seguridad en una fase temprana del ciclo de vida del desarrollo y crea una base de seguridad sólida para cada producto y servicio de Adobe. Se lleva a cabo el modelado de amenazas para señalar las áreas en las que pueden ser necesarios cambios en la arquitectura para evitar amenazas conocidas. El uso de la automatización en el proceso de modelado de amenazas ayuda a escalar eficazmente mediante la generación automática de requisitos de seguridad, lo que hace que el proceso de revisión sea más eficaz.
- **Revisiones de código específicas:** en el caso de secciones específicas de código que traten datos confidenciales o de componentes reutilizados por varios servicios, los investigadores de seguridad realizan revisiones manuales del código para asegurarse de que cumple las mejores prácticas de seguridad.
- **Pruebas específicas:** los investigadores de seguridad de Adobe realizan pruebas de seguridad periódicas de los productos y servicios basándose en múltiples factores, entre los que se incluyen el interés de los adversarios y los patrones de ataque conocidos.

Pruebas de seguridad: Además de las revisiones de seguridad periódicas, Adobe lleva a cabo pruebas de penetración de los productos y servicios que ayudan a reforzar las áreas de puntos débiles identificados e involucra a la comunidad de usuarios con el programa de recompensas por errores para detectar y notificar problemas. Las actividades de pruebas de seguridad incluyen:

- **Pruebas de penetración internas:** los equipos de seguridad internos de Adobe realizan pruebas de penetración asistidas por código utilizando una combinación de técnicas automatizadas y manuales que se centran en las áreas de debilidad destacadas durante las revisiones de seguridad.

- **Pruebas de penetración externas:** Se contrata a las principales empresas de seguridad externas para realizar pruebas de penetración que pueden descubrir posibles vulnerabilidades de seguridad y mejorar la seguridad general de los productos y servicios de Adobe. Al recibir un informe de terceros, Adobe documenta las vulnerabilidades observadas, evalúa la gravedad y las prioridades y crea una estrategia de mitigación o un plan de corrección. Una vez resuelto el problema, volvemos a realizar las pruebas de penetración para ayudar a garantizar la corrección del problema.
- **Recompensas por fallos:** Adobe mantiene programas de recompensas por fallos internos y externos que recompensan a las personas que descubren y notifican fallos de software con reconocimiento público o compensación económica. Las recompensas por fallos internos aprovechan el talento en seguridad de la entidad y ayudan a promover la concienciación sobre la seguridad de las aplicaciones en todos los equipos de ingeniería. Además, Adobe aprovecha la comunidad externa de investigadores de seguridad para revelar de forma responsable las oportunidades de explotación que afectan a Adobe o a sus clientes. La divulgación responsable de problemas de productos específicos se incentiva mediante la concesión de pagos monetarios por envíos válidos.

Emisión de billetes y cuadros de mando

La emisión automatizada de tickets notifica a los equipos de producto las vulnerabilidades de seguridad conocidas o explotables, lo que les permite mitigar el problema con prontitud. Los tickets se asignan automáticamente a los equipos en función de sus habilidades, experiencia y conocimiento del producto. Mediante el uso de paneles e indicadores clave de rendimiento (KPI), el equipo de seguridad de aplicaciones puede medir el grado de adopción del módulo de seguridad de aplicaciones de Adobe en toda la entidad, así como determinar la eficacia de las soluciones de automatización de la seguridad.

Se trabaja con socios de la industria para compartir conocimientos y ayudar a mantener las mejores prácticas.

- Asociación de Seguridad de los Sistemas de Información (AISS)
- Consorcio Internacional de Certificación de Seguridad de Sistemas de Información (ISC)2
- Grupo de Trabajo Anti-Abuso de Mensajes, Malware y Móviles (M3AAWG)
- Proyecto de seguridad de aplicaciones web abiertas (OWASP)
- Foro de Software Assurance para la excelencia en el código (SAFECode)
- Detener. Pensar. Conectar.
- Consejo de OSC del Área de la Bahía
- Centro para la Seguridad en Internet (CIS)
- Alianza de seguridad en la nube (CSA)
- Foro de Mujeres Ejecutivas (EWF)
- Foro de Equipos de Seguridad y Respuesta a Incidentes (FIRST)
- Asociación de Auditoría y Control de Sistemas de Información (ISACA)

INFRAESTRUCTURA DE SEGURIDAD OPERATIVA DE ADOBE

Estrategia de operaciones de Adobe seguridad en Cloud

Al incorporar la seguridad en el núcleo de los procesos en la nube, Adobe ayuda de forma proactiva a prevenir posibles problemas que puedan surgir en el complejo panorama de la seguridad. A medida que la huella en la nube sigue creciendo e implica entornos de varias nubes y tecnologías emergentes, las configuraciones y políticas estándar, así como las herramientas de automatización, nos ayudan a reducir los errores humanos y a ofrecer garantías a los clientes de que las múltiples capas de la infraestructura están protegidas frente a posibles puntos débiles.

Para permitir que los desarrolladores se centren en las áreas de especialización y evitar errores de seguridad accidentales, se a creado configuraciones y políticas de seguridad estándar que se aplican a todos los servicios que implantamos en la nube. La incorporación de controles de seguridad en las primeras etapas del ciclo de vida de desarrollo ayuda a Adobe no sólo a reforzar la postura de seguridad de los servicios desde el diseño hasta la implantación, sino también a reducir el descubrimiento de agujeros de seguridad en las últimas etapas de desarrollo, cuando la corrección es más difícil. La aplicación automatizada de los controles de seguridad y políticas de seguridad en la nube ayuda a mejorar la postura general de seguridad corporativa, así como a garantizar a los clientes que su seguridad es la máxima prioridad.

The Adobe Operational Security Stack

Desarrollado por nuestro equipo especializado en seguridad operativa, Adobe Operational Security Stack (OSS) es un conjunto consolidado de herramientas que ayudan a garantizar que los productos y servicios de Adobe se diseñen teniendo en cuenta las mejores prácticas de seguridad. Teniendo en cuenta las necesidades de seguridad multi cloud de la empresa, el OSS de Adobe se basa en dos (2) principios fundamentales: estandarización y prevención. Para ello, el OSS de Adobe incluye un conjunto estandarizado de soluciones de flujo de trabajo y supervisión continua que permite a los equipos de servicio diseñar sus entornos de nube pública y privada teniendo en cuenta la seguridad, desde el principio, y ayuda a prevenir de forma proactiva los riesgos de seguridad.

El OSS de Adobe funciona en una variedad de recursos en la nube, proporciona seguridad a escala, ofrece capacidades estandarizadas para toda la organización y ayuda a garantizar la visibilidad de la seguridad en entornos operativos para los equipos de seguridad, auditoría y cumplimiento de Adobe. Al adoptar el mismo conjunto de herramientas y procesos en los equipos de productos y servicios, Adobe ayuda tanto a evitar errores de seguridad como a permitir que las aplicaciones se adapten a las soluciones de seguridad sin reinventar la rueda.

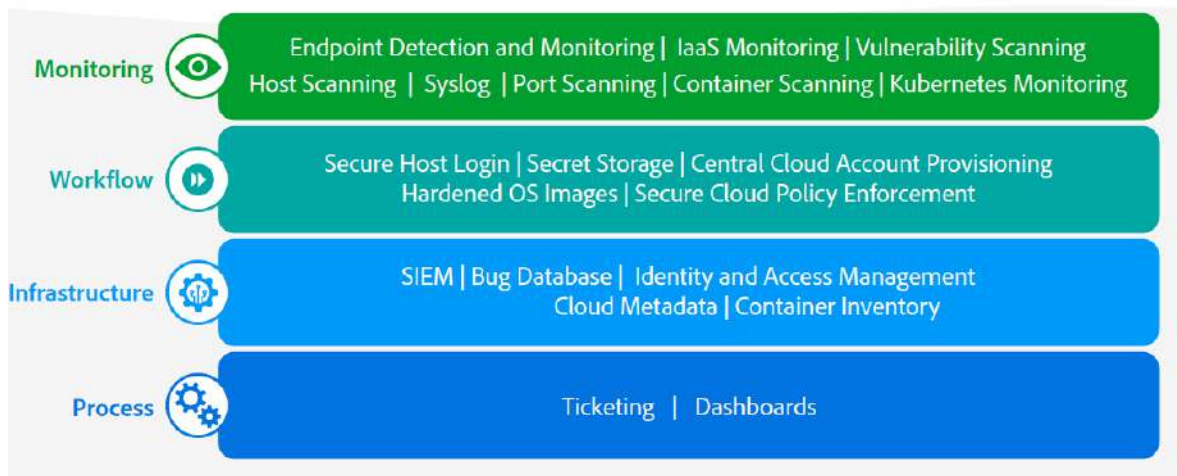


Figura 1: Componentes de seguridad operativa de Adobe

Con el objetivo de hacer que la elección segura sea la elección por defecto, el OSS de Adobe incluye cuatro (4) capas distintas, cada una de las cuales incluye una amplia gama de herramientas y servicios comunes que pueden ser aprovechados por cualquier equipo de productos de Adobe y les proporciona una forma de mantenerse al día de las mejores prácticas de seguridad que cambian con rapidez.

Supervisión - (Monitoring)

La capa de supervisión incluye herramientas para ayudar a introducir los datos de registro y configuración de todos los entornos de nube y regiones de Adobe en un almacén de datos central. Una vez introducidos, los equipos de seguridad y cumplimiento de Adobe, así como el Centro de operaciones de seguridad (SOC) de Adobe, se puede analizar estos datos para ayudar a medir la desviación de la seguridad y detectar las brechas de seguridad. Las brechas se pueden encontrar mediante la revisión manual de los datos por parte del equipo de seguridad o mediante herramientas automatizadas de detección de seguridad.

Además, los equipos de seguridad realizan periódicamente análisis de hosts y contenedores en los entornos en nube, tanto desde el punto de vista de las aplicaciones como de la red, para ayudar a detectar vulnerabilidades. Cualquier vulnerabilidad descubierta a través de estas exploraciones y pruebas de penetración se evalúa, se prioriza y se asigna a un plan de corrección, si es necesario.

Las siguientes herramientas se incluyen en la capa de supervisión del OSS de Adobe:

- **Detección y respuesta de puntos finales:** CrowdStrike Falcon, un agente de detección y respuesta de puntos finales (EDR) ligero y de última generación que se instala en todos los puntos finales, incluidos los servidores, dentro de Adobe, protege los datos y en los sistemas con una supervisión y recopilación continuas en tiempo real que nos permite identificar y responder rápidamente a las amenazas.

- **Supervisión de IaaS:** MAVLink, una herramienta de recopilación de datos de nube pública desarrollada por Adobe, consulta las API de Amazon Web Services (AWS) y Microsoft Azure para obtener datos de registro y configuración del entorno y, a continuación, introduce esta información en un almacén de datos Splunk. Mediante el uso de MAVLink, los desarrolladores permiten a los equipos de ingeniería de seguridad de Adobe ver el estado de la nube pública en un único punto en el tiempo desde el punto de vista de la seguridad. Los equipos de auditoría interna y cumplimiento de Adobe también pueden utilizar estos datos para determinar el cumplimiento de muchos elementos de las normas de seguridad tanto de AWS como de Azure.

- **Escaneado de vulnerabilidades:** con una variedad de herramientas comerciales y desarrolladas internamente, se escanea periódicamente los centros de datos de Adobe, así como toda la huella en la nube, ayudando a localizar posibles vulnerabilidades antes de que surjan.

- **Exploración de host:** mediante Hubble, un marco de cumplimiento de seguridad modular basado en Python desarrollado internamente y de código abierto para la comunidad externa, Adobe lleva a cabo las tres (3) actividades siguientes:

- **Auditoría:** compruebe si los sistemas host cumplen los archivos de políticas basados en el estándar del Centro para la Seguridad en Internet (CIS).

- **Consulta** - Recopile información del sistema a través de osquery para detectar intrusiones

- **Integridad de archivos** - Seguimiento de los cambios de archivos en directorios clave

- **Syslog** - Adobe recopila registros del sistema y mensajes de eventos de diferentes máquinas y los almacena en Splunk para su supervisión y revisión.

- **Exploración de puertos:** se explora continuamente cientos de miles de direcciones IP de Adobe, lo que reduce el tiempo que transcurre entre la exposición inicial y la corrección. Mediante la canalización de nmaps, los equipos pueden detectar rápidamente la exposición de los puertos del perímetro.

- **Exploración de contenedores:** Adobe registra y explora las imágenes de contenedores en busca de vulnerabilidades y exposiciones comunes conocidas (CVE, por sus siglas en inglés) tanto en la creación como en el tiempo de ejecución. Se cargan los análisis en Splunk y los equipos reciben un ticket de Jira para los problemas que requieren corrección.

- **Supervisión de Kubernetes:** mediante una herramienta de seguridad interna diseñada para supervisar los clústeres de Kubernetes, los ingenieros de seguridad de Adobe pueden obtener una instantánea de la configuración de solo lectura de cualquier clúster en un momento predefinido y ejecutar evaluadores personalizados para las brechas de seguridad.

Flujo de trabajo - (Workflow)

La capa de flujo de trabajo del OSS de Adobe se compone de herramientas que ayudan a los desarrolladores e ingenieros de productos a ofrecer la seguridad integral de los productos de Adobe y de la infraestructura de la empresa. Las herramientas disponibles en la capa de flujo de trabajo, que permiten a los equipos aplicar eficazmente las políticas de seguridad, facilitan la realización de operaciones seguras, entre las que se incluyen:

- **Inicio de sesión seguro en el host:** la gestión centralizada de las credenciales y el acceso ayuda a Adobe a mantener un control estricto sobre las máquinas virtuales en la nube mediante la aplicación de políticas de autenticación multifactorial (MFA) y principios de privilegio mínimo. También se registran todas las sesiones administrativas con fines de auditoría.

- **Almacenamiento de secretos:** Adobe utiliza un producto de bóveda de seguridad de terceros líder para proteger, almacenar y controlar estrictamente el acceso a tokens, contraseñas, certificados, claves API y otros secretos.

- **Provisión central de cuentas en la nube:** para agilizar la gestión y el control de la presencia de Adobe en la nube, los equipos de productos pueden crear y gestionar cuentas en la nube a través de un servicio central, lo que permite al equipo de control de Adobe gestionar más fácilmente la facturación de las cuentas en la nube, así como aplicar de forma centralizada las políticas operativas y de seguridad. Una única fuente de verdad para los metadatos de cuentas en la nube es fundamental para comprender el tamaño y la postura de seguridad de la huella en la nube, y el aprovisionamiento centralizado de cuentas nos permite comprender la propiedad correcta de las cuentas y su finalidad prevista.

- **Imágenes reforzadas del sistema operativo:** al proporcionar imágenes reforzadas centralizadas que se adhieren a los puntos de referencia del Centro para la Seguridad en Internet (CIS) y aplican tanto las actualizaciones de seguridad aprobadas por el CIS como las últimas herramientas de seguridad, Adobe ofrece una experiencia segura y lista para usar a todos los equipos de productos. Las imágenes, almacenadas en una aplicación desarrollada internamente llamada Image Factory, se analizan mediante las herramientas de seguridad internas antes de que se liberen para su uso a los equipos de ingeniería. Además, los equipos de producto pueden utilizar la API Image Factory para integrar la última imagen de máquina directamente en su canal de construcción.

- **Aplicación de políticas seguras en la nube:** aunque la mayoría de los proveedores de servicios en la nube ofrecen políticas seguras predeterminadas, Adobe utiliza una herramienta complementaria desarrollada internamente para automatizar la aplicación y corrección de políticas, así como para proporcionar una capa adicional de protección contra la desviación accidental de la seguridad y los servicios inseguros implantados en la nube. La herramienta utiliza servicios nativos de la nube, como Azure Policy, AWS Service Control Policies y AWSConfig Rules, para aplicar los requisitos de cumplimiento de políticas y recursos en todas las cuentas de nube pública de Adobe. Cualquier recurso no conforme en una cuenta de nube pública activa automáticamente la acción de política adecuada. A continuación, la herramienta registra la acción y la notifica a los equipos afectados para que puedan identificar qué ha provocado el evento de corrección.

Para proteger contra los errores de configuración más comunes, las políticas se centran en un conjunto de categorías que incluyen las vías de compromiso más utilizadas por los atacantes:

- Identidad y privilegios en la nube
- Privacidad e integridad de los datos
- Exposición de los extremos de la red
- Integridad de DNS

Además, nuestro modelo operativo de políticas en la nube dicta que las cuentas nuevas incluyan todas las políticas activas actuales en el momento de la provisión. Cuando Adobe publica una nueva política, nuestro proceso de aplicación automatizado hace cumplir las cuentas existentes a medida que se adaptan a la nueva política. Para acelerar el proceso de aplicación tras la publicación de una nueva política, aplicamos automáticamente las cuentas después de un periodo de reposo (unos 30 días) tras la publicación. Las cuentas no conformes reciben automáticamente un ticket para su rectificación, incluyendo una fecha límite para que la cuenta cumpla la normativa.

La aplicación automática permite a los desarrolladores centrarse en el trabajo de alto nivel para cumplir la política, mientras que el proceso garantiza la aplicación de la propia política.

Infraestructura - (Infrastructure)

Los metadatos sofisticados actualizados periódicamente son un componente clave de la capa de infraestructura en el OSS de Adobe, que proporciona la base para las capas de supervisión y flujo de trabajo. Utilizando estos metadatos, el OSS de Adobe puede asignar automáticamente las brechas de seguridad descubiertas al equipo propietario del recurso en la nube infractor. Otras herramientas de la capa de infraestructura son

- **Información de seguridad y gestión de eventos (SIEM):** mediante el uso de Splunk para buscar, supervisar, visualizar y analizar los datos de registro agregados recopilados en la capa de supervisión, el SOC de Adobe puede realizar un análisis más profundo de los eventos e incidentes relacionados con la seguridad.

- **Base de datos de errores:** para ayudar a proporcionar una única fuente de atribución, Adobe registra los errores en Jira utilizando su sistema automatizado de tickets para la responsabilidad y el seguimiento.

- **Gestión de acceso e identidades (IAM):** Adobe utiliza Microsoft Active Directory en combinación con otras herramientas estándar para gestionar la autenticación.

- **Metadatos en la nube:** Adobe realiza el seguimiento y la auditoría de los metadatos de todas las cuentas públicas en la nube y audita estos datos trimestralmente para ayudar a proteger las cuentas y garantizar el control de las políticas. El portal de metadatos en la nube ayuda a los equipos de productos y seguridad a incorporar nuevas cuentas en la nube de acuerdo con los flujos de trabajo prescritos. Además, los equipos pueden acceder a los metadatos en el almacén de datos para filtrar el ruido, eliminar los falsos positivos y ayudar a priorizar adecuadamente las amenazas críticas.

- **Inventario de contenedores:** Es un conjunto de metadatos para todo el ecosistema de contenedores de Adobe que ayuda a los equipos de productos a obtener una visión más profunda de la orchestration de contenedores. Además, los equipos pueden utilizar los metadatos de contenedores para supervisar y visualizar métricas, así como para obtener una visibilidad completa de cualquier entorno Kubernetes.

Proceso - (Process)

La capa de proceso permite a Adobe mejorar continuamente la postura de seguridad e implantar las mejores prácticas de seguridad. Los datos de las otras tres capas del OSS de Adobe se almacenan en un almacén de datos centralizado y se introducen en Jira (para la mitigación y resolución de las deficiencias de seguridad), en los paneles (para la visibilidad de la gestión) y en otros socios internos.

Utilizamos indicadores clave de rendimiento (KPI) para medir la eficacia de la implantación del OSS de Adobe en toda la empresa, así como para identificar los valores atípicos. La creación automatizada de fichas de Jira notifica a los equipos de productos cuando su servicio se desvía de un estado de seguridad reforzado y ayuda a los equipos de ingeniería y operaciones a cumplir varios dominios de control en el Marco de controles comunes de Adobe (CCF), como la gestión de la configuración y la gestión de activos.

Los componentes de seguridad operativa de Adobe en acción

Aprovechando la automatización, los controles a nivel del sistema y la estandarización, cada capa del OSS de Adobe funciona en concierto con las demás para ayudar a proporcionar seguridad a los recursos en la nube implantados.

Las herramientas de control de acceso y credenciales permiten una aplicación uniforme de las políticas de gestión de acceso e identidades en todos los servicios gestionados en la nube, mientras que el registro de las actividades de los usuarios proporciona una visión más profunda de las áreas potenciales para la mejora de las políticas de aplicación.

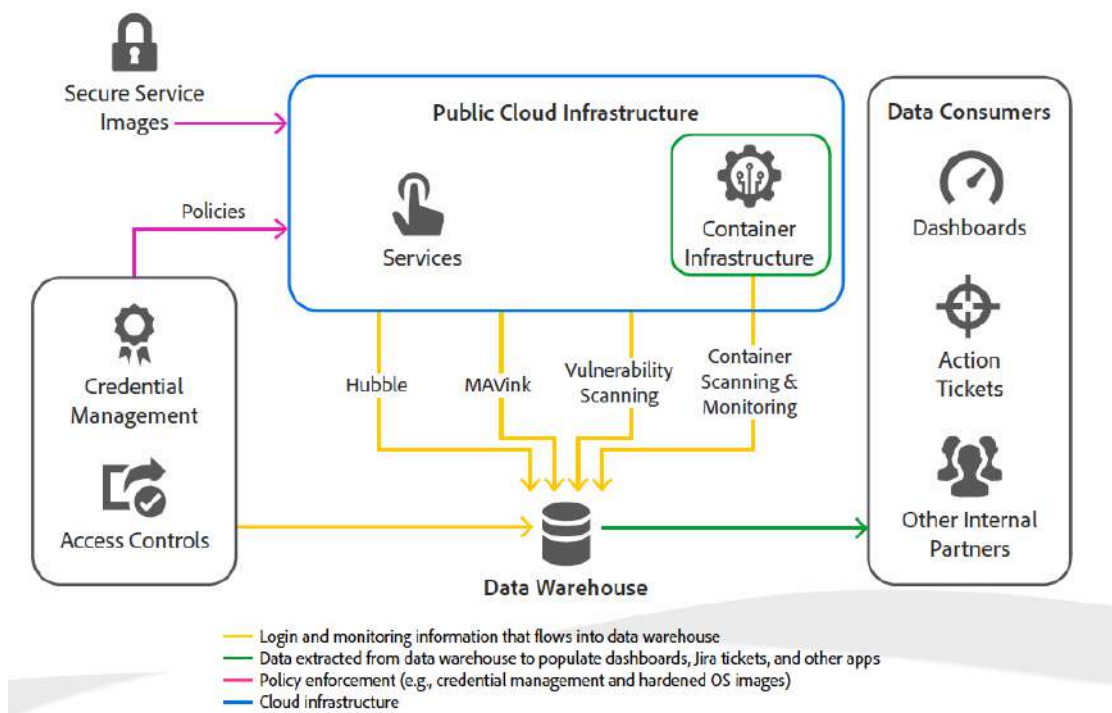
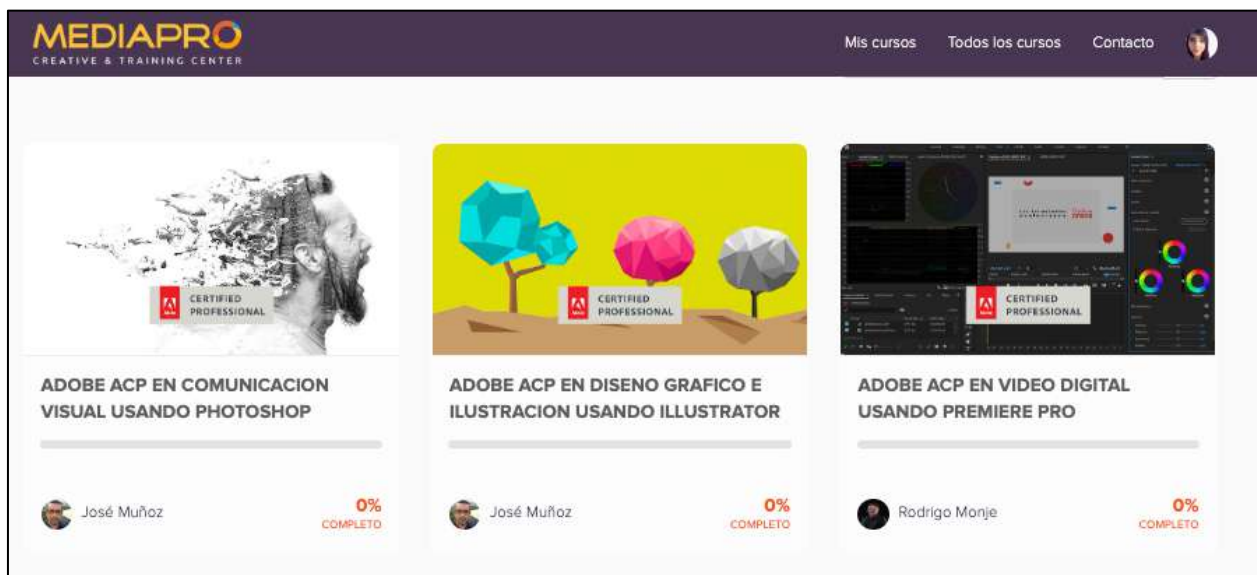


Figura 2: Flujo de datos de OSS de Adobe

Después de la implantación, la herramientas de supervisión observan continuamente los servicios, ya estén implantados en la nube o en la plataforma de contenedores, y envían registros y otra información relevante a un almacén de datos central. Los paneles de control, los tickets de Jira y otras aplicaciones de toda la empresa extraen datos de este almacén central para rellenar sus aplicaciones de cara al usuario.

2. Portal de cursos de educación virtual (Media Pro)

Es una plataforma que contiene 47 cursos online de forma ilimitada que comprende varios temas de uso de las aplicaciones de la suscripción de Adobe Creative Cloud.



LA INFRAESTRUCTURA TECNOLÓGICA DEL PORTAL DE CURSOS DE EDUCACIÓN VIRTUAL (Media Pro)

Cursos de consultores y evangelistas de Adobe

Aprenderás con los profesionales más reconocidos y destacados del mercado, con gran experiencia en el mundo Adobe.

Tutoría académica de primer nivel

Resuelve tus dudas con especialistas de diversos países y aprovecha su experiencia en los distintos campos creativos.

Certificado de Adobe

Recibe de manera exclusiva el certificado de la marca más reconocida a nivel mundial una vez que completes tu curso.

Proyectos reales

Aprenderás con proyectos y situaciones de la vida laboral, que te permitirán acortar el camino y desarrollar un flujo profesional.

Prepárate para las certificaciones internacionales

El portal es el único que te ofrece cursos para prepararte para las certificaciones internacionales. Toma el examen en tu país los exámenes internacionales de Adobe que ampliarán tu horizonte profesional.

Respaldo del mundo académico

El portal es utilizado en más de 30 proyectos en instituciones educativas en Latinoamérica. El mundo educativo confía en nosotros y en la calidad de los contenidos.

EXPERIENCIA DE LOS CONSULTORES ADOBE

El contenido está desarrollado por instructores y consultores oficiales de Adobe que, además dictan los cursos de manera presencial en algunos países, por lo que se obtiene toda la experiencia de ellos, llegando a conocer en detalle los software y flujos de trabajo.

Al aprobar cada curso del portal se emite un certificado oficial como Centro Autorizado Adobe, lo que te permitirá acreditar tus logros en redes sociales, CV y portafolios. Adicionalmente existe una validación en cada certificado que permite indicar la autenticidad del mismo.

CONTENIDOS DE LA PLATAFORMA

Para asegurar la mejor experiencia de aprendizaje, los cursos de preparación para las certificaciones

Adobe incluyen lo siguiente:

- Videos explicativos de las funcionalidades a detalle de los programas a capacitar. Este formato permite que los usuarios repitan el video todas las veces que requieran para aprender
- el uso de los programas y sus herramientas. Además, permite que los usuarios vayan creando y desarrollando ejercicios prácticos con el software correspondiente en tiempo real.
- Guías de apoyo para acceder a los contenidos y funcionalidades de manera secuencial y estructurada. Material y recursos digitales (fotos, textos, ilustraciones, PDF, videos, audios) para que los usuarios puedan aplicar a ejercicios o casos reales.

SOLICITUD DE CURSOS ONLINE

La solicitud de asignación de cursos se realiza diligenciando el siguiente formulario

<https://forms.office.com/r/p0Yn9AwSJY>

En el cual se solicita la siguiente información:

1. Cédula
2. Nombres completos
3. Programa al que pertenece
4. Centro al que pertenece
5. Correo con dominio misena.edu.co / soy.sena.edu.co / sena.edu.co /

Después encontrarán el listado de todos los cursos disponibles para realizar, los cursos serán asignados de 1 a 4 días hábiles; Cuando los cursos sean asignados, al correo del usuario le llegara una notificación de confirmación de cuenta.

Una vez confirmada el usuario ya podrá disfrutar de todo el contenido que ofrece la plataforma Media Pro. <https://online.mediaprotc.com/>

INFRAESTRUCTURA DE SEGURIDAD DEL PORTAL DE CURSOS DE EDUCACIÓN VIRTUAL (Media Pro)

Privacidad de datos

Existen diversas medidas técnicas de seguridad para proteger los sistemas:

- Los servidores y el tráfico de red son monitoreados por ambas herramientas estándar de la industria para detectar y responder a posibles violaciones de seguridad.
- Los servidores y servicios se ejecutan en la infraestructura de Amazon Web Service (AWS), utilizando la mejor de su clase herramientas de instrumentación que registran cambios en los servidores y detectan signos de un posible compromiso.
- Amazon Web Services utiliza una combinación de tecnologías de sandboxing estándar de la industria y un sofisticado sistema de detección de intrusos en la red para monitorear la actividad de la red en busca de signos de actividad maliciosa.
- El cifrado TLS es parte de la arquitectura de seguridad estándar. Los servicios básicos de transporte requieren cifrado, como SSH o HTTPS, para intercambiar información.
- La tecnología de cifrado se utiliza para proporcionar seguridad para la autenticación de usuarios en línea y sesiones de administrador.

Seguridad Técnica

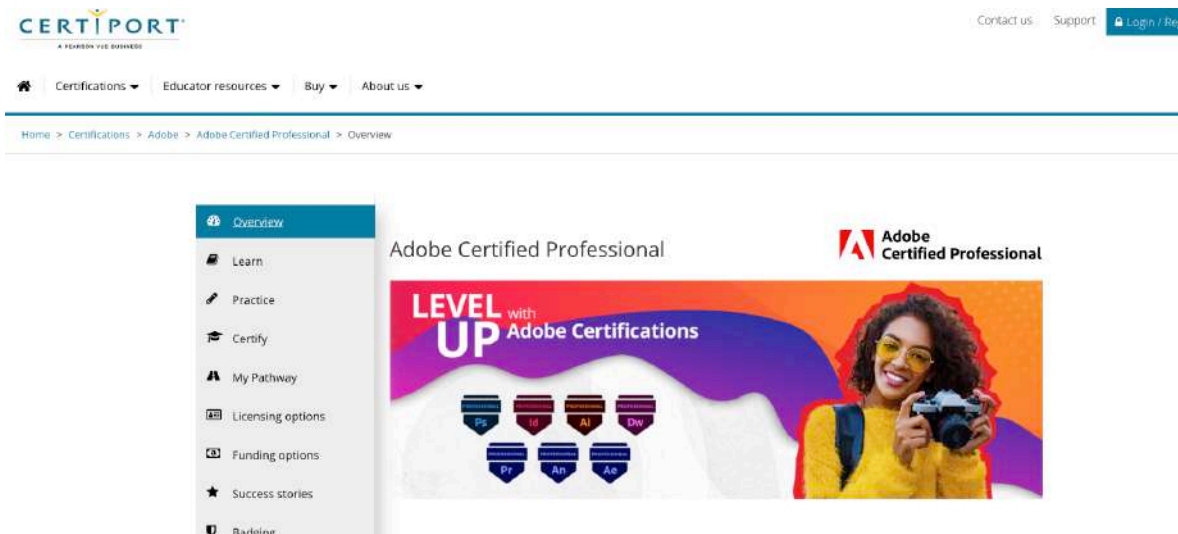
Hay una serie de medidas de seguridad técnica para proteger los sistemas:

- Los servidores y el tráfico de la red son monitoreados por ambas herramientas estándar de la industria para detectar y responder a cualquier posible brecha de seguridad.
- Los servidores y servicios se ejecutan en la infraestructura de Amazon Web Service (AWS), utilizando las mejores herramientas de instrumentación de su clase que registran los cambios en los servidores y detectan signos de un posible compromiso.
- Amazon Web Services utiliza una combinación de tecnologías de sandboxing estándar de la industria y un sofisticado sistema de detección de intrusos en la red para monitorear la actividad de la red en busca de signos de actividad maliciosa.
- El cifrado TLS es parte de la arquitectura de seguridad estándar. Los servicios de transporte básicos requieren cifrado, como SSH o HTTPS, para intercambiar información.
- La tecnología de cifrado se utiliza para proporcionar seguridad para la autenticación de usuarios en línea y las sesiones de administrador.

LA INFRAESTRUCTURA TECNOLÓGICA DE LA PLATAFORMA CERTIPOINT

Certiport, una entidad de Pearson VUE, es el proveedor líder de servicios de gestión de programas, entrega y desarrollo de exámenes de certificación que se entregan a través de una red expansiva de más de 12.000 centros de pruebas autorizados de Certiport en todo el mundo, entre ellos Grupo DECO Colombia.

Se de voucher de certificación adobe Certified Associate (ACA) (Certiport)



Incluyen las siguientes certificaciones de Adobe:

- SENA - Adobe Acp En Comunicación Visual Usando Photoshop
- SENA - Adobe Acp En Diseño Grafico E Ilustracion Usando Illustrator
- SENA - Adobe Acp En Impresión Y Publicación De Medios Digitales Con Indesign
- SENA - Adobe Acp En Video Digital Usando Premiere Pro
- SENA - Adobe Acp En Efectos Visuales Y Motion Graphics Usando After Effects
- SENA - Adobe Acp En Comunicación Web Usando Dreamweaver
- SENA - Adobe Acp En Animaciones Multiplataforma Usando Animate Cc

Para la preparación para examen: Se le otorgará acceso a la plataforma Media Pro que tiene contenidos de autoestudio para la preparación del examen internacional.

El Simulador:

GMetrix

Estas herramientas de evaluación y preparación de pruebas basadas en el desempeño ayudan a las personas a obtener credenciales de certificación. Muchos de sus estudiantes estarán ansiosos por evaluar su conocimiento de las aplicaciones antes de realizar los exámenes de certificación. Además, reconocemos la necesidad de que los educadores evalúen adecuadamente el conocimiento de un individuo. Certiport proporciona pruebas de práctica de CertPREP que funcionan con GMetrix. Estas pruebas, con funciones de informes e información incluidas, garantizan que sus estudiantes estén adecuadamente preparados para realizar su examen de certificación.

Se otorgará 2.000 simuladores Gmetrix ACP, con vencimiento a 1 año (Febrero 23 de 2024)

Las pruebas de práctica de CertPREP son personalizables, lo que le permite crear un entorno altamente efectivo que conduce al aprendizaje centrado en el estudiante. Las pruebas de práctica de CertPREP ofrecen dos modos diferentes:

Modo de prueba:

- Los estudiantes experimentan cómo serán los exámenes de certificación
- Las pruebas de práctica cronometradas presentan escenarios para realizar como el examen de certificación real

Modo de entrenamiento:

- Los estudiantes trabajan a su propio ritmo mientras reciben comentarios e instrucciones paso a paso para cada pregunta.

Duración: para cada certificación cuenta con 50 minutos

Tipo de examen: Respuesta selectiva y Live-in-the-Application.

El examen se divide en dos partes. La primera parte consta de preguntas como opción múltiple, Verdadero/Falso y Completar los espacios en blanco. La segunda parte consta de preguntas Live-in-the-App en las que se les pedirá a los examinados que completen tareas prácticas utilizando la aplicación real.

Todos los exámenes de Certificación son en español y se deben tomar de forma presencial en los Centros de Formación del SENA.

Condiciones de los programas para presentar las certificaciones

- Adobe Certified Professional 2023 Suite:
- After Effects
- Illustrator
- Photoshop
- Premiere Pro
- Other exams coming soon!

Adobe Certified Professional 2022, 2021, or 2020 Suites:

- After Effects
- Animate
- Dreamweaver
- Illustrator
- InDesign
- Photoshop
- Premiere Pro

Publicaciones de exámenes/idiomas

Esta página está dedicada a mantener a todas las audiencias actualizadas con los exámenes de certificación actuales y futuros y lanzamientos de productos de pruebas de práctica. Las fechas de lanzamiento planificadas que se enumeran aquí están sujetas a cambios.

Todas las actualizaciones serán reflejadas en este link

<https://certiport.pearsonvue.com/Educator-resources/Exam-details/Exam-releases#CC-2023>

✓+ = Publicado recientemente ✓ = Publicado

“Fecha” = Fecha de lanzamiento planificada

“En blanco” = No disponible/Indeterminado

“CertPREP” o “MeasureUp” = Prueba de práctica

Nombre del examen de Adobe 2023	Producto	es-nosotros	zh-cn	zh-tw	de-de	es-mx	fr-fr	ja-jp	ko-kr	nl-nl	por-favor	pt-br	ru-ru	vi-vn
Photoshop (versión 24.x)	Examen	✓+	Sep	Sep	Sep	Sep	Sep	Q4	Sep	Sep	Sep	Sep	Sep	
	CertPREP													Publicado recientemente
Ilustrador (versión 27.x)	Examen	✓+	Sep	Q4		Sep		Q4	Q4			Q4		
	CertPREP													
InDesign (versión 18.x)	Examen	Mar	Q4	Q4		Q4			Q4					
	CertPREP													
Premiere Pro (versión 23.x)	Examen	✓+	Q4		Q4	Sep		Q4	Q4					
	CertPREP													
Tejesueños (v 21.x)	Examen	✓	Puede	✓		✓+								
	CertPREP	✓		✓		✓								
Animar (v 23.x)	Examen	Mar	Q4	Q4		Q4								
	CertPREP													
After Effects (versión 23.x)	Examen	✓+	Q4			Q4								
	CertPREP													

Nombre del examen de Adobe 2022	Producto	es-nosotros	zh-cn	zh-tw	de-de	es-mx	fr-fr	ja-jp	ko-kr	nl-nl	por-favor	pt-br	ru-ru	vi-vn
Photoshop (versión 23.x)	Examen	✓+	Puede	✓+	✓+	✓+	✓+	Mar	Abr	✓+	✓+	✓+	✓+	
	CertPREP	✓+	✓	✓		✓								Publicado recientemente
	Examen	✓+	Puede	✓+		✓+		Mar	Abr			✓+		

Nombre del examen de Adobe 2023	Producto	es-nosotros	zh-cn	zh-tw	de-de	es-mx	fr-fr	ja-jp	ko-kr	nl-nl	por-favor	pt-br	ru-ru	vi-vn
---------------------------------	----------	-------------	-------	-------	-------	-------	-------	-------	-------	-------	-----------	-------	-------	-------

Ilustrador (versión 26.x)	CertPREP	✓+	✓	✓		✓								
InDesign (versión 17.x)	Examen	✓+	Puede	Mar		✓+			Abr					
	CertPREP	✓+	✓	✓		✓								
Premiere Pro (versión 22.x)	Examen	✓+	Puede		Abr	Abr		Mar	Abr					
	CertPREP	✓+	✓			✓								
Tejesueños (v 21.x)	Examen	✓	Puede	✓		✓+								
	CertPREP	✓		✓		✓								
Animar (versión 22.x)	Examen	✓+	Puede	Abr		Abr								
	CertPREP	✓+		✓		✓								
After Effects (versión 22.x)	Examen	✓+	Puede			Abr								
	CertPREP	✓+	✓			✓								

• Presentación de Exámenes:

Los exámenes de certificación se llevarán a cabo de manera presencial:

- **En sitio:** Los exámenes de certificación se llevarán a cabo de manera presencial, en los laboratorios dispuestos. Para tal fin, será necesario usar la plataforma de CERTIPORT denominada COMPASS.
- El Proctor/Administrador del centro, deberá estar presente y llevar a cabo la jornada de certificación de los candidatos. Para este proceso, programaremos una sesión de capacitación de 1hr con el fin de dar a conocer las recomendaciones, resolver dudas y aclarar la metodología.

• Vouchers:

- Los voucher corresponden a certificaciones individuales, los cuales pueden usar y distribuir sin restricciones.
- Los voucher de todas las herramientas cuentan, con la opción de retoma; lo que quiere decir que, si se pierde la certificación, cuenta con otra oportunidad para presentarlo nuevamente a las 24 hrs siguientes al primer intento y hasta por un periodo no mayor de 7 días calendario.

• Simulador Gmetrix

- Corresponde a la preparación para el examen oficial.
- Oportunidad para usarlo en 2 modalidades: Entrenamiento y modo prueba.

• **Modo entrenamiento:** Sin límite de tiempo, la herramienta da una retroalimentación, en el sentido que indica cuáles preguntas están bien y cuáles no.



- **Modo Prueba:** Con el mismo límite de tiempo de la certificación oficial y únicamente arroja el resultado que se obtendría al presentar la certificación oficial.

Seguridad del examen

Certiport se compromete a garantizar que sus exámenes de certificación sean respetados y valorados en el mercado. En consecuencia, Certiport toma las medidas adecuadas para garantizar que la integridad de sus exámenes no se vea comprometida y también responsabiliza a los Centros de pruebas autorizados por Certiport (CATC) de tomar las medidas adecuadas para prevenir y detectar fraudes y violaciones de seguridad de los exámenes.

Certiport realiza análisis forenses de datos periódicos para identificar patrones de anomalías en los resultados de los exámenes que ayudan a detectar trampas o piratería de contenido. Por ejemplo, los indicadores forenses como los tipos de respuestas, la latencia, las tasas de aprobación y las repeticiones pueden revelar patrones de trampa, colusión o piratería. Sin embargo, la prevención y la detección temprana son elementos críticos que requieren la estrecha colaboración de sus CATC.

Por lo tanto, además de depender de sus CATC para brindar monitoreo estándar de la industria durante las pruebas, Certiport requiere que sus CATC garanticen un entorno de prueba físico o virtual apropiado, y que los administradores y supervisores estén lo suficientemente capacitados para brindar una supervisión de buena calidad de las pruebas.

Los administradores y supervisores que observen violaciones de las reglas, o sospechen una violación de la seguridad de las pruebas, deben comunicarse de inmediato con el Servicio de atención al cliente de Certiport (o con el representante de socios autorizado de Certiport). Es muy importante documentar todos los hechos relevantes que respaldan la supuesta infracción. Los informes deben incluir la fecha, la hora y la ubicación del incidente, el nombre del candidato a la prueba y el nombre y la versión del examen realizado.

¡IMPORTANTE!

Los Centros de pruebas autorizados de Certiport (CATC) deben hacer cumplir estrictamente todos los procedimientos y reglas que se detallan en esta página.

Entornos de prueba físicos o virtuales

1. Asegúrese de que el área de evaluación sea un entorno profesional en el que los Candidatos puedan realizar el examen sin interrupciones. Fuera de la entrega virtual, las viviendas privadas, los hogares u otras instalaciones personales no son entornos de prueba aprobados y no deben usarse para administrar exámenes.
2. Asegúrese de que cada prueba sea supervisada activamente con una vista sin obstrucciones de cada candidato a la prueba en el área de prueba. Los métodos aceptables de supervisión incluyen:
 - **Pantalla de cámara/video** : el supervisor puede monitorear de forma remota al candidato a la prueba a través de una cámara con acceso a una vista completa del entorno de prueba.
 - **Ventana de observación** : el supervisor puede monitorear al candidato a la prueba a través de una ventana de observación con una vista completa del entorno de prueba.
 - **Supervisión en la sala** : el supervisor se encuentra en la misma sala que el candidato a la prueba. Este suele ser el método preferido para grupos más grandes de pruebas en el aula.

3. Si no hay particiones disponibles para las estaciones de prueba, asegúrese de que los candidatos a la prueba estén sentados lo suficientemente separados para minimizar las distracciones y evitar las trampas. La distancia recomendada es de cuatro pies.
4. Mientras se realizan las pruebas, no se permite el uso de equipos como impresoras, máquinas de fax, fotocopadoras, teléfonos u otros dispositivos electrónicos en el entorno de prueba.

Resumen del proceso

En la pantalla Verificar y desbloquear el examen en Compass, el administrador del examen (supervisor) verifica la identidad y el entorno del candidato a la prueba antes de desbloquear el examen.

Para facilitar el proceso de verificación, los administradores del examen pueden usar una plataforma de videoconferencia, como Zoom, Microsoft Teams, Google Meet, FaceTime u otras opciones. Los candidatos a la prueba necesitarán una cámara web u otro dispositivo con una cámara capaz de unirse a la videollamada en los centros de prueba donde se requiere verificación y monitoreo por video. Dado el marco de tiempo limitado de las sesiones de Exámenes desde casa, recomendamos realizar esto inmediatamente antes del inicio de la sesión de examen.

Tenga en cuenta: El uso de software de videoconferencia puede suponer una carga adicional para usted y el ancho de banda de su Candidato de prueba que puede exceder los requisitos técnicos básicos que hemos establecido para la solución Exámenes desde el hogar. El equipo de soporte técnico de Certiport tampoco podrá solucionar ningún problema relacionado con el uso de software de terceros.

Comprobación de identidad

Confirme la identidad del Candidato a la Prueba. Por ejemplo, en los centros de pruebas donde se requiere la verificación por video, si el candidato no es inmediatamente reconocible, el administrador del examen podría indicarle que presente una identificación con foto emitida por la escuela o el gobierno a la cámara web y luego comparar la foto con el candidato en vivo.

Comprobación del entorno

Valide que el candidato a la prueba haya seguido los pasos para preparar su entorno para realizar el examen

- El candidato debe estar en una habitación privada, tranquila y bien iluminada.
- El candidato debe despejar su espacio de trabajo:
 - El candidato solo debe tener su computadora y el teclado, el mouse y la cámara web que lo acompañan.
 - El candidato no puede usar múltiples monitores
 - El candidato no tiene permitido ningún dispositivo de grabación (incluidos papel, bolígrafos, lápices, cámaras, etc.)
 - A menos que el administrador del examen lo autorice específicamente como medio de comunicación con el candidato, el candidato no debe tener un dispositivo móvil al alcance
- El candidato debe quitarse todas las cubiertas para la cabeza no religiosa

Verificación de la identidad y el entorno del candidato

Desbloquear el examen

Cuando el candidato haya cumplido con los requisitos, marque la casilla para certificar que ha validado la identificación y el entorno del candidato, ingrese sus credenciales de supervisor y luego desbloquee el examen.

Seguimiento del candidato durante el examen

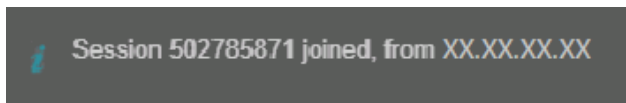
Después de verificar la identificación y el entorno del candidato y desbloquear el examen, los administradores del examen supervisan al candidato durante el examen.

En los centros de examen donde se requiere el monitoreo por video, puede indicar a los candidatos que se unan a una videollamada donde puede ver a todos los candidatos durante su examen.

Si sospecha que el candidato no cumple con las reglas del examen, comuníquese directamente con el candidato para verificar la situación. Si necesita finalizar la sesión debido a una infracción de un candidato, indíquele que cierre su navegador web y que se comunique con Certiport de inmediato. Si necesita soporte técnico.

Elementos adicionales a tener en cuenta:

En la herramienta Dashboard, cada máquina candidata solo debe tener una dirección IP para unirse y salir una vez durante la sesión. Si se une más de una dirección IP única, comuníquese con el candidato de inmediato. Asegúrese de que nadie más tenga acceso al enlace del candidato. Si la misma dirección IP se une y sale repetidamente, es posible que el candidato tenga problemas de conexión a Internet (estos cuadros de mensaje grises aparecen en la esquina inferior derecha de la pantalla).



En los centros de pruebas donde se requiere monitoreo por video, si el candidato deja la vista de la cámara web, alguien más ingresa al espacio privado o escucha actividad que no cumple con los requisitos, comuníquese con el candidato de inmediato.

Procedimientos de registro y examen de candidatos

1. El CATC es responsable de verificar la identidad del candidato a la prueba con al menos una forma de identificación válida (que contenga una fotografía y la firma del candidato a la prueba).
2. El CATC/Supervisor no debe permitir dispositivos de grabación o electrónicos en el área de prueba. Dichos dispositivos incluyen: papel, bolígrafos, lápices, cámaras, computadoras o teléfonos celulares. La propiedad adicional del candidato a la prueba, como libros o bolsas, debe almacenarse fuera del entorno de prueba o inaccesible durante el examen.
3. El CATC/supervisor puede permitir que un candidato a la prueba tome un descanso durante la prueba si así lo solicita, pero debe informar al candidato de la prueba que el reloj del examen no se puede detener durante el descanso. No se debe permitir que los candidatos a la prueba realicen actividades durante un descanso que puedan comprometer la seguridad del examen, incluido el uso de un teléfono y/o la comunicación con otros candidatos a la prueba.

4. El supervisor debe confirmar que la identificación del candidato a la prueba coincida con la información de la cuenta de Certiport en la pantalla de validación del supervisor antes de iniciar el examen.
5. Los supervisores pueden responder preguntas sobre la funcionalidad del software del examen, pero no pueden responder preguntas ni proporcionar instrucciones relacionadas con el contenido del examen.

Tiempo de asiento

Es importante tener en cuenta que la administración de un examen es más que simplemente dejar que el Candidato a la prueba realice la parte cronometrada del examen de certificación. Se requerirá tiempo adicional para administrar un examen de principio a fin con aportes tanto del supervisor/maestro como del candidato a la prueba. Este tiempo administrativo combinado con el tiempo de examen asignado se conoce como "Tiempo de asiento". Estas acciones adicionales pueden incluir tareas y logística, como la planificación del aula, el lanzamiento del software, el inicio de sesión, la posible descarga de actualizaciones del software y/o el contenido del examen, los tiempos de carga, la lectura y aceptación de los términos/condiciones, la realización de datos demográficos, la revisión del tutorial, enviar comentarios y cargar/ver los resultados del examen.

Formación en vídeo

<https://vimeo.com/513911245>

Trampa

Si se descubre que un candidato de la prueba hace trampa en un Centro de pruebas autorizado por Certiport (CATC) durante una sesión en persona o Exámenes desde el hogar, el supervisor/administrador del examen debe detener el examen de inmediato. Luego, el candidato de la prueba debe ser notificado de la infracción e informado de lo que se observó. También se debe enviar por correo electrónico un informe detallado de lo ocurrido a Certiport a customerservices@pearson.com.

En la mayoría de los casos, Certiport deferirá al supervisor/administrador del examen involucrado con respecto a cómo se maneja la situación internamente, incluso si el candidato de la prueba podrá volver a tomar el examen. Si Certiport requiere más información, se notificará al supervisor/administrador del examen y se proporcionarán los siguientes pasos.

Centros públicos de pruebas

- El personal que responda a las solicitudes de programación de exámenes debe estar completamente capacitado en las ofertas y procedimientos de productos de Certiport.
- El logotipo de CATC debe colocarse en un lugar que sea visible para los candidatos a la prueba antes de ingresar a las instalaciones.
- El CATC debe saludar a los candidatos a la prueba de manera profesional y proporcionar políticas y procedimientos de prueba antes del comienzo del examen.

Adaptación de discapacidades

Como proveedor mundial de exámenes de certificación, Certiport se compromete a garantizar que aquellas personas que deseen certificar su competencia en el uso de computadoras tengan la oportunidad de hacerlo. Certiport, en consecuencia, adopta la Ley de Estadounidenses con Discapacidades (ADA), así como otras adaptaciones globales para discapacidades diseñadas para promover esos objetivos.

Condiciones de las máquinas:

Los Centros de Formación deben cumplir con las siguientes características de las máquinas para realizar las certificaciones:

Requerimientos técnicos Mac

Encontrará todos los requisitos de hardware, software, entorno, conectividad y permisos que se deben cumplir para garantizar la entrega de exámenes compatibles y consistentes. Los exámenes Live-in-the-Application (LITA) tienen requisitos de programa individuales que van más allá de los del software o la solución de entrega del examen; consulte cada programa individual para obtener información detallada.

Nota: Si no se encuentra en los requisitos a continuación, debe considerarse "No compatible".

Artículo	Obligatorio / Mínimo	Recomendado
Sistema operativo	Mac OS X Ventura 13.x Mac OS X Monterey 12.x Mac OS X Big Sur 11.x Mac OS X Catalina 10.15 (compatible solo con Adobe 2020)	
Importante: El idioma de Mac OS, el idioma del software instalado localmente (solo para los exámenes LITA), el idioma de Compass y el idioma del examen deben coincidir. Consulte las preguntas frecuentes para obtener información detallada.		
Derechos de administrador	Se requieren derechos de administrador local de Mac para instalar Compass, pero no para entregar exámenes.)	
Procesador	Pentium 4 o equivalente 1,3 GHz o superior	Core i5 o equivalente 2,6 GHz o superior
Para el procesador Apple Silicon (M1):		
Nota: Los exámenes de Adobe 2020 no son compatibles con el M1 porque solo las versiones 12.x y 11.x de Mac OSX son compatibles en computadoras con el procesador M1, y los exámenes de Adobe 2020 solo son compatibles en Mac OSX versión 10.15.		
RAM (exámenes LITA)	4GB	8GB
RAM (exámenes no LITA)	2GB	4GB
Disco duro	5GB	+1 GB por minuto por programa de examen instalado
Resolución de video	1280 x 800 (Pantalla panorámica 16:9) 1024 x 768 (Estándar 4:3)	1920 x 1080 (Pantalla panorámica 16:9) 1280 x 1024 (Estándar 4:3)
Audio	El examen CSB English for IT requiere sonido a través de parlantes o auriculares/audífonos. Si no está administrando este examen, no se requiere sonido. (Se recomienda el uso de auriculares en un salón de clases o en persona). Nota: El equipo de soporte técnico de Certiport no podrá solucionar ningún problema relacionado con la reproducción de audio o los dispositivos.	
Protocolo de seguridad	TLS 1.1 o superior	
Velocidad de conexión a Internet	256 kbps o DSL	Conexión a internet de alta velocidad
Navegadores de Internet compatibles	Safari o cromo	
Teclado y Mouses	Sí	
Configuración del navegador	Las Cookies deben estar habilitadas	
cortafuegos	Los cortafuegos corporativos (incluidas las VPN) a menudo hacen que este método de entrega falle. Realice su examen en un entorno sin un firewall corporativo o asegúrese de que los puertos y las direcciones IP estén en la lista blanca Requerido: El dominio certiport.com debe ser accesible. Además, debe tener acceso completo a través de los puertos 80 (HTTP), 443 (HTTPS) y se permiten redireccionamientos HTTP.	
Puertos de comunicación y direcciones IP	Obligatorio: incluir en la lista blanca el dominio "*.certiport.com".	

Nota: Como consecuencia del traslado de Certiport a Azure Cloud, será imposible proporcionar una lista de direcciones IP que deben ser accesibles para una experiencia de examen ininterrumpida. Por lo tanto,



ahora requerimos que *.certiport.com se incluya en la lista blanca.

Mínimo: Las siguientes direcciones IP deben ser accesibles:

159.182.30.18 | www.certiport.es
159.182.31.253 | nuget.certiport.com
93.191.169.139 | IP de seguridad adicional
159.182.30.17 | descargas.certiport.com
159.182.30.17 | verificar.certiport.com
64.27.100.27
64.27.64.232
64.106.193.0/24
64.106.220.0/24
206.188.17.0/24
159.182.0.0/16
13.107.246.0/24
13.107.253.0/24
147.243.0.0/16
191.232.166.33 | azuresouthamerica.starttest.com
51.140.142.254 | azureeurope.starttest.com
104.211.154.51 | azureindia.starttest.com
40.122.173.143 | azureuscentral.starttest.com
168.63.220.86 | azurehongkong.starttest.com

Nota: Si se accede a Internet a través de un servidor proxy de autenticación y el sistema no está configurado para pasarle credenciales automáticamente, experimentará problemas durante la prueba.

Artículos prohibidos

Nota: Si no se encuentra en los requisitos a continuación o en la lista de Requisitos avanzados, debe considerarse "No compatible".

Artículo	La entrega del examen debe cumplir con las siguientes restricciones
Dispositivos informáticos portátiles	Las computadoras portátiles, tabletas y teléfonos inteligentes con pantalla táctil están estrictamente prohibidos. Nota: Los ejemplos de dispositivos informáticos portátiles prohibidos incluyen, entre otros: Surface Pro, Chromebooks, teléfonos y tabletas con Android e iOS.
Procesador	Los dispositivos que ejecutan procesadores Ultra Mobile están estrictamente prohibidos. Esto incluye, entre otros, Intel Atom, líneas de CPU AMD NEO y CPU ARM (excluyendo el procesador Apple M1 ARM para exámenes compatibles).
RAM	Menos que la memoria RAM mínima especificada del sistema operativo de su estación de trabajo de examen
Sistemas operativos	Los sistemas operativos de servidor están estrictamente prohibidos en las estaciones de trabajo de entrega de exámenes. Los entornos virtuales están estrictamente prohibidos para la entrega de exámenes. Todos los sistemas operativos basados en Linux/Unix están estrictamente prohibidos.
Mostrar	Los monitores de pantalla táctil están estrictamente prohibidos para la entrega del examen. La resolución de pantalla inferior a 1024 x 768 en color de 16 bits está estrictamente prohibida.
Conexión de red	Pearson recomienda enfáticamente evitar configuraciones de redes que involucren servidores proxy, configuraciones avanzadas de seguridad de firewall y otras medidas de seguridad de la red, como, entre otras, el filtrado de paquetes o la inspección de paquetes. Se desaconsejan encarecidamente las conexiones VPN, ya que provocarán interrupciones en la entrega del examen.
Conexión a Internet	Las VPN SSL están estrictamente prohibidas (p. ej., Hotspot Shield). Las conexiones de acceso telefónico a Internet no son compatibles.
Navegadores de Internet	Los navegadores que no se encuentran en la lista de navegadores de Internet admitidos en este documento no se pueden usar para realizar el examen

Requerimientos técnicos Windows

Encontrará todos los requisitos de hardware, software, entorno, conectividad y permisos que se deben cumplir para garantizar la entrega de exámenes compatibles y consistentes. Los exámenes Live-in-the-Application (LITA) tienen requisitos de programa individuales que van más allá de los del software o la solución de entrega del examen; consulte cada programa individual para obtener información detallada. Esta página también enumera qué exámenes están disponibles en qué sistema de entrega.

Artículo	Obligatorio / Mínimo	Recomendado
Sistema operativo	Windows 11 Enterprise, Professional, Home o Education (las aplicaciones de Adobe y Autodesk instaladas localmente necesarias para la entrega Live-in-the-App con Compass no son compatibles con Windows 11)	
	Windows 10 Enterprise, Professional, Home o Education Ver. 1607 compilación 14393.2515 o posterior (32 bits y 64 bits)	
	Windows 8.1 Enterprise o Professional (32 bits y 64 bits)	
Nota: Algunos exámenes Live-in-the-Application solo admiten sistemas operativos de 64 bits.		
Importante: El idioma de Windows, el idioma del software instalado localmente (solo para exámenes LITA), el idioma de Compass y el idioma del examen deben coincidir.		
Derechos de administrador	Se requieren derechos de administrador local de Windows para instalar Compass, configurar los ajustes y administrar exámenes locales.	
Procesador	Pentium 4 o equivalente 1,3 GHz o superior	Core i5 o equivalente 2,6 GHz o superior
Nota: Algunos exámenes Live-in-the-Application solo admiten procesadores de 64 bits. No admitimos procesadores ARM.		
RAM (exámenes LITA)	4GB	8GB
RAM (exámenes no LITA)	2GB	4GB
Disco duro	5GB	+1 GB por minuto por programa de examen instalado
Resolución de video	1280 x 800 (Pantalla panorámica 16:9) 1024 x 768 (Estándar 4:3)	1920 x 1080 (Pantalla panorámica 16:9) 1280 x 1024 (Estándar 4:3)
Audio	El examen CSB English for IT requiere sonido a través de parlantes o auriculares/audífonos. Si no está administrando este examen, no se requiere sonido. (Se recomienda el uso de auriculares en un salón de clases o en persona). Nota: El equipo de soporte técnico de Certiport no podrá solucionar ningún problema relacionado con la reproducción de audio o los dispositivos.	
Protocolo de seguridad	TLS 1.1 o superior	
Velocidad de conexión a Internet	256 kbps o DSL	Conexión a internet de alta velocidad
Navegadores de Internet compatibles	Microsoft Internet Explorer 11 (solo versión de 32 bits) Últimas versiones de Microsoft Edge, Chrome o Firefox	
Teclado y Mouses	Mouse con rueda de 2 botones Teclado	
Configuración del navegador	Las Cookies deben estar habilitadas	
Software adicional	Debe estar instalado .NET 4.6.2 o posterior (solo Windows)	
cortafuegos	Los cortafuegos corporativos (incluidas las VPN) a menudo hacen que este método de entrega falle. Realice su examen en un entorno sin un firewall corporativo o asegúrese de que los puertos y las direcciones IP estén en la lista blanca Requerido: El dominio certiport.com debe ser accesible. Además, debe tener acceso completo a través de los puertos 80 (HTTP), 443 (HTTPS), 56774 (TCP) y se permiten redireccionamientos HTTP.	
Puertos de comunicación y direcciones IP	Obligatorio: incluir en la lista blanca el dominio "*.certiport.com".	

Nota: Como consecuencia del traslado de Certiport a Azure Cloud, será imposible proporcionar una lista de direcciones IP que deben ser accesibles para una experiencia de examen ininterrumpida. Por lo tanto, ahora requerimos que *.certiport.com se incluya en la lista blanca.

Mínimo: Las siguientes direcciones IP deben ser accesibles:

159.182.30.18 | www.certiport.es
159.182.31.253 | nuget.certiport.com
93.191.169.139 | IP de seguridad adicional
159.182.30.17 | descargas.certiport.com
159.182.30.17 | verificar.certiport.com
64.27.100.27
64.27.64.232
64.106.193.0/24
64.106.220.0/24
206.188.17.0/24
159.182.0.0/16
13.107.246.0/24
13.107.253.0/24
147.243.0.0/16
191.232.166.33 | azuresouthamerica.starttest.com
51.140.142.254 | azureeurope.starttest.com
104.211.154.51 | azureindia.starttest.com
40.122.173.143 | azureuscentral.starttest.com
168.63.220.86 | azurehongkong.starttest.com

Nota: Si se accede a Internet a través de un servidor proxy de autenticación y el sistema no está configurado para pasarle credenciales automáticamente, experimentará problemas durante la prueba.

Artículos prohibidos

Nota: Si no se encuentra en los requisitos a continuación o en la lista de Requisitos avanzados, debe considerarse "No compatible".

Artículo	La entrega del examen debe cumplir con las siguientes restricciones
Dispositivos informáticos portátiles	Las computadoras portátiles, tabletas y teléfonos inteligentes con pantalla táctil están estrictamente prohibidos. Nota: Los ejemplos de dispositivos informáticos portátiles prohibidos incluyen, entre otros: Surface Pro, Chromebooks, teléfonos y tabletas con Android e iOS.
Procesador	Los dispositivos que ejecutan procesadores Ultra Mobile están estrictamente prohibidos. Esto incluye, entre otros, Intel Atom, líneas de CPU AMD NEO y CPU ARM.
RAM	Menos que la memoria RAM mínima especificada del sistema operativo de su estación de trabajo de examen Windows XP y Vista están estrictamente prohibidos
Sistemas operativos	Sistema operativo Windows Server estrictamente prohibido en las estaciones de trabajo de entrega de exámenes Los entornos virtuales están estrictamente prohibidos para la entrega de exámenes. Todos los sistemas operativos basados en Linux/Unix están estrictamente prohibidos.
Mostrar	Los monitores de pantalla táctil están estrictamente prohibidos para la entrega del examen. La resolución de pantalla inferior a 1024 x 768 en color de 16 bits está estrictamente prohibida.
Conexión de red	Pearson recomienda enfáticamente evitar configuraciones de redes que involucren servidores proxy, configuraciones avanzadas de seguridad de firewall y otras medidas de seguridad de la red, como, entre otras, el filtrado de paquetes o la inspección de paquetes. Se desaconsejan encarecidamente las conexiones VPN, ya que provocarán interrupciones en la entrega del examen.
Conexión a Internet	Las VPN SSL están estrictamente prohibidas (p. ej., Hotspot Shield). Las conexiones de acceso telefónico a Internet no son compatibles.
Navegadores de Internet	Los navegadores que no se encuentran en la lista de navegadores de Internet admitidos en este documento no se pueden usar para realizar el examen.

Vouchers: Adobe Certified Professional es la certificación reconocida por la industria que demuestra el dominio del software Adobe Creative Cloud y el conocimiento imprescindible para las carreras de medios digitales. Cada examen está integrado con una aplicación de Adobe y diseñado por expertos, lo que permite una evaluación auténtica de las habilidades de preparación para el trabajo.

INFRAESTRUCTURA DE SEGURIDAD DE LA PLATAFORMA CERTIPOINT

Certiport es comprometido con la seguridad de los usuarios. La presente declaración de seguridad y privacidad describe las normas sobre la recopilación de datos y las prácticas de uso del sitio Certiport.com (en adelante el “Sitio”) que Certiport, a Pearson VUE Business hospeda a favor de Microsoft. No se aplica a ningún otro sitio, producto o servicio de Certiport, a Pearson VUE Business en línea o fuera de línea. Al acceder el Sitio, usted expresa su consentimiento a la recopilación de información y a las prácticas de uso descritas en esta declaración de privacidad.

Recopilación de información personal

Cuando usted se registra, Certiport le solicita información personal incluido su nombre, dirección postal, dirección electrónica, país y número de teléfono. Además, es posible que Certiport le solicite otra información tales como una descripción de su educación académica, sexo, empleo, fecha de nacimiento y otros datos demográficos similares. Esta información se almacena en su perfil personal y usted la puede ver en Certiport.com.

Transferencia de información al patrocinador del programa

Si el Programa de certificación es patrocinado por una empresa tercera, esta información también se pondrá a disposición del patrocinador del programa. Para obtener más información acerca del uso que dará el patrocinador a su información personal, póngase en contacto con el patrocinador.

Recopilación de información anónima

El Sitio puede recopilar cierta información anónima sobre su visita, tal como el nombre del proveedor de servicios Internet y la dirección de Protocolo de Internet (IP) mediante los cuales tiene acceso a Internet, la fecha y la hora en que acceda al Sitio, las páginas que abra mientras visita el Sitio y la dirección de Internet del sitio Web desde el cual se conectó directamente con el sitio. Esta información se utiliza para facilitar la mejora del Sitio, para analizar las tendencias y administrar el Sitio.

programa de protección de datos "safe harbor"

Hemos seguido las pautas de protección de datos "Safe Harbor" del Departamento de Comercio de Estados Unidos sobre la información personal recopilada en la conexión de entrega de certificaciones. Además, nos hemos comprometido a llevar a cabo las medidas propuestas por las autoridades de protección de datos de la Unión Europea acerca de la recopilación y manejo de la información personal.

acceso y control de su información personal

Si desea revisar o actualizar su perfil, simplemente visite el sitio Certiport.com y haga clic en Mi perfil para modificar su información personal. Allí podrá:



- Ver y editar su información personal.
- Indicar a Certiport que no desea recibir información sobre comercialización.
- Comunicar a Certiport si desea que su información personal sea compartida con sus socios de manera que usted pueda recibir información sobre comercialización relacionado con sus productos y servicios ya sea por correo electrónico o por correo postal.
- Aprovechar de los servicios del creador de carreras profesionales personales “Mi Certiport”.
- Distinguirse de los demás al compartir su transcripción digital con empleadores potenciales.
- Solicitar unidades de educación académica o avance profesional.
- Recibir boletines personalizados por correo electrónico que contengan las noticias más recientes relacionadas con su certificación y campo.
- Asistir a eventos locales de apreciación para los clientes.
- Adquirir y registrar productos de Certiport.

Uso de la información personal

Certiport utilizará esta información para personalizar su experiencia, facilitar el uso del Sitio y proveer un servicio al cliente más eficiente. Certiport puede utilizar su información personal para proporcionarle información importante sobre los productos o servicios que está utilizando, incluidos, pero sin limitarse a, actualizaciones y avisos importantes, ampliaciones para las herramientas y servicios Web para acceder y utilizar los resultados de sus exámenes, proporcionar soluciones personalizadas cuando estén disponibles, y permitirle aprovechar sus logros con otras empresas. Con su permiso, Certiport puede enviarle información sobre otros productos y servicios Certiport.

Almacenamiento y proceso

La información personal recopilada en el sitio puede ser almacenada y procesada en Estados Unidos de Norteamérica o en cualquier otro país donde Certiport o sus afiliados, subsidiarios o agentes mantengan facilidades. Además, al utilizar el Sitio, usted nos autoriza a dicha transferencia de información fuera del país.

De forma predeterminada, Certiport tiene autorización para almacenar de manera segura los resultados de sus exámenes, certificados digitales e información relacionada. Esta información se utilizará solamente para los fines específicos del programa de certificación y para su beneficio personal.

Divulgación a terceros

La información personal que recopila Certiport puede ser transmitida a proveedores de servicios de terceros fiables a fin de informarle a Usted sobre productos y servicios que ofrece Certiport, tales como el hospedaje del sitio, servicios de embalaje y postales, servicio al cliente, e iniciativas de comercialización. A los socios de Certiport se les exige que mantengan la privacidad de la información y tienen prohibido utilizar la información para cualquier otro fin.

Certiport puede revelar información personal si así lo requiere la ley o en buena fe de que tal acción es necesaria para:

Cumplir con mandatos de ley o para cumplir con procesos legales servidos en Certiport o el Sitio.
Proteger y defender los derechos o propiedad de Certiport.

Actuar en circunstancias urgentes para proteger la seguridad personal de los usuarios de los productos Certiport, nuestro sitio Web o al público en general.

Seguridad de su información personal

Certiport protege estrictamente la seguridad de su información personal y respeta su preferencia para el uso de la misma. Certiport protegerá cuidadosamente sus datos para que evite pérdidas, uso inapropiado, acceso o divulgación sin autorización o destrucción de los mismos. Salvo como se explicó anteriormente, no se compartirá su información personal con ninguna otra empresa sin su permiso. Dentro de la empresa, los datos se almacenan en servidores controlados por contraseñas con acceso limitado.

Además, usted puede desempeñar un papel importante en la protección de su información. Ninguna persona no autorizada puede ver o editar su información personal sin conocer los datos para conectarse a Mi Certiport (nombre de usuario y contraseña), por tanto le rogamos que no comparta estos datos con otras personas.

Al registrarse a través de Certiport, está dando su consentimiento para que su información confidencial se transmita o se utilice en el modo indicado en esta normativa.

Privacidad de los menores de edad

Certiport se compromete a proteger las necesidades de privacidad de los menores. Certiport recomienda a los padres y apoderados a jugar un papel activo en las actividades e intereses en línea de sus hijos.

Uso de cookies

Certiport.com utiliza cookies no persistentes en conexión al uso de Mi Certiport. La autenticación de Mi Certiport asigna un número de identificación personal y lo envía a su PC en forma de un pequeño archivo de texto, denominado “cookie”. El uso de esta cookie permite que interactúe con varias partes de Certiport.com. La cookie es válida solamente durante su sesión autenticada en Certiport.com y no se almacena en su PC tras cancelarse la sesión autenticada.

Modificaciones en esta declaración de privacidad

A medida que el Sitio expande, mejora y actualiza las ofertas y servicios de Certiport, Certiport se reserva el derecho de modificar o corregir la norma en cualquier momento y por cualquier motivo. Cuando esto suceda, Certiport revisará la fecha de la “última actualización” que se encuentra al principio de este documento.

Para modificaciones drásticas en este documento, Certiport le avisará ya sea al colocar un aviso notorio en la página inicial de su sitio web o al enviarle un aviso al respecto. Certiport le invita a que revise periódicamente esta declaración de privacidad para mantenerse informado sobre lo que la organización está haciendo para proteger la información personal recopilada. Su uso ininterrumpido del servicio constituye su aceptación a lo establecido en esta declaración de privacidad y las actualizaciones a este documento.

Tenga en cuenta que esta declaración de privacidad y cualquier otra opción que seleccione en el Sitio no se aplica necesariamente a la información personal que haya proporcionado a Microsoft en el contexto de otros productos o servicios de Certiport, a Pearson VUE Business, en el contexto de otros servicios o productos que sean operados independientemente.

Información de contacto

Certiport, a Pearson VUE Business le invita a que nos envíe sus comentarios relacionados con esta declaración de seguridad y privacidad. Si cree que Certiport, a Pearson VUE Business no ha cumplido con esta declaración de seguridad y privacidad, comuníquese con nosotros mediante correo electrónico al PrivacyOfficer@certiport.com, o por correo regular a la dirección incluida a continuación. Certiport se esforzará sinceramente para determinar y solucionar el problema a la brevedad posible.

3. Mesa de ayuda de soporte técnico (Plataforma GLPI)

LA INFRAESTRUCTURA TECNOLÓGICA DE LA PLATAFORMA GLPI

La plataforma GLPI es un aplicativo del servidor OVH

Los servidor OVH

OVHCloud es una plataforma que proporciona servicios web gestionados y servidores dedicados. Muchos usuarios confían en ellos, pero lo fantástico de ellos es que se han convertido en el proveedor de servicios de alojamiento más destacado de toda Europa. Al mismo tiempo, también es el tercer proveedor de servicios más grande del mundo.

Proporcionar servicios de alojamiento web, servidor y nube excepcionalmente buenos hace que los clientes estén satisfechos debido a su fantástico rendimiento. Curiosamente, OVHCloud gestiona su red de fibra óptica en todo el mundo para mejorar aún más su rendimiento.

El uso de los servicios de OVHCloud puede traer consigo muchas funciones. Aquí discutiremos algunas de las características principales que obtiene con los servicios de OVHCloud.

Varios servicios de alojamiento disponibles

A veces, un tipo de servicio de alojamiento no es suficiente para satisfacer los requisitos de todos los clientes. Como solución a esto, OVHCloud ofrece muchos tipos diferentes de servicios de alojamiento. Algunos de ellos son:

- Alojamiento compartido
- Alojamiento para revendedores
- Alojamiento VPS
- Alojamiento dedicado
- Servicios de colocation
- Con esta amplia gama de servicios disponibles, es sencillo para diferentes tipos de clientes optar por el mejor según sus necesidades.

Integración del panel de control

Administrar el sitio web de alojamiento no es una tarea fácil a menos que obtenga las herramientas eficientes a su disposición. Para que el proceso de gestión sea muy sencillo y fácil para los usuarios, los servicios de alojamiento de OVHCloud integran paneles de control de código abierto. No solo facilita la administración, sino que los usuarios también pueden usar todas las funciones con facilidad.

Gestión de archivos

Una de las mejores cosas de los servicios de alojamiento de OVHCloud es que los usuarios pueden hacer su gestión de archivos. Con la ayuda de cosas como FTO o Shell, los usuarios pueden acceder a sus archivos y administrarlos.

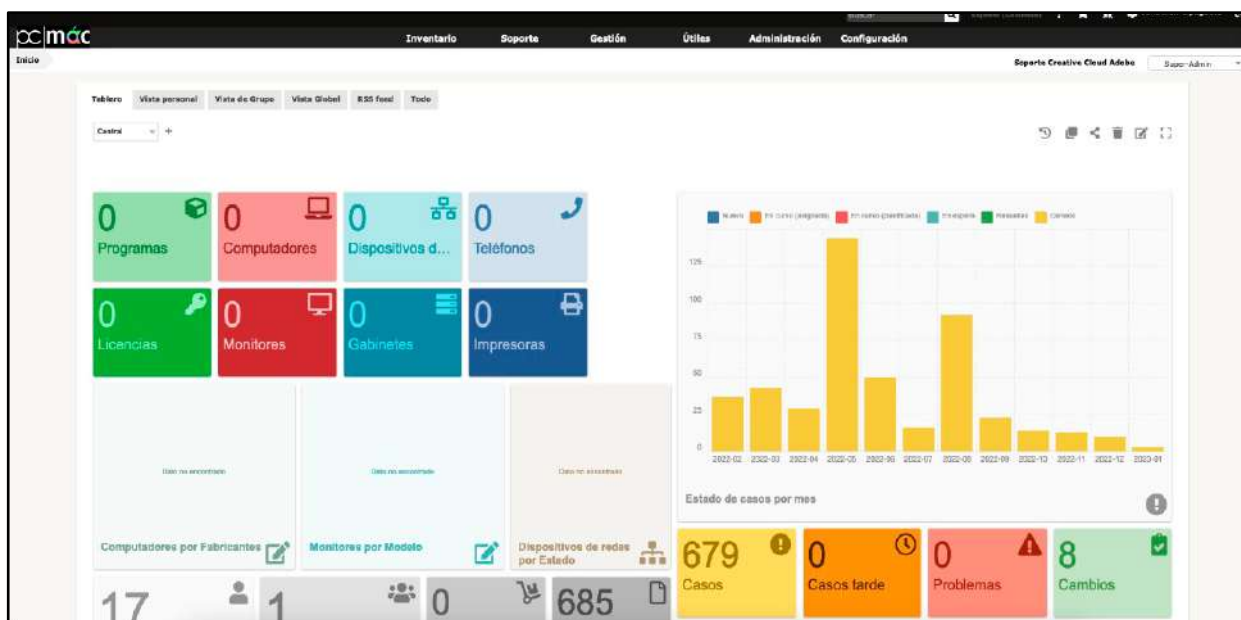
La seguridad recibe mucha atención

Cuando se trata de la seguridad de los usuarios, OVHCloud no deja nada de qué preocuparse. Han trabajado mucho en diferentes cosas, y lo siguiente hace que su plataforma sea muy segura para muchos usuarios.

- Detección de spam.
- Firewalls.
- Herramientas de detección de malware.

La plataforma GLPI

Esta es una plataforma de gestión de los casos de soporte que se encuentra implementada en un servidor en nube del canal y mediante la cual el personal de soporte solucionara los registros y la atención de los casos.



En este aplicativo podemos administrar incidentes / solicitudes para solucionar problemas, crear directorio de contactos y empresas, base del conocimiento, entre otras funcionalidades.

Link de ingreso: <https://ayuda.pcmac.co/front/central.php>

Usuario: arincon (Asignada a Adriana Rincón del área de Formación Profesional)

Contraseña: MesaAyuda2022



En este caso sena.edu.co al ser de Microsoft tiene 5.000 destinatarios diarios, 500 por mensaje y 1.000 destinatarios diarios sin relación, para crear usuarios de roles nombrados a continuación son ilimitados.

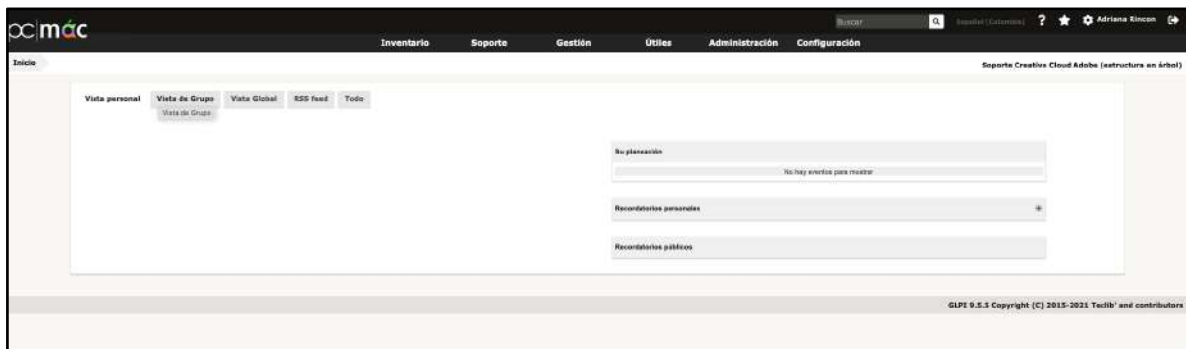
Roles:

En la plataforma encontramos los siguientes perfiles que son asignados a cada usuario y permite el acceso a distintas características de la plataforma:

- **Admin:** este perfil administra los permisos sobre la totalidad del software GLPI. Sin embargo, no tiene acceso a todas las características en la configuración de las reglas, entidades y otros temas sensibles que puedan degradar las acciones de GLPI.
- **Hotliner:** este perfil permite introducir incidencias y tener acceso a su seguimiento. En cambio, este perfil no permite hacerse cargo de ellas.
- **Observador:** este perfil solo accede en modo lectura a la información sobre el inventario y su gestión. En cuanto a las incidencias, este perfil puede declararlas o atribuirles.
- **Read-only:** este perfil define el acceso de solo lectura. Se utiliza cuando los objetos están bloqueados. También se puede utilizar para dar a los usuarios derechos para desbloquear objetos.
- **Self-Service:** este perfil está dedicado a la presentación de solicitudes de asistencia. Se define en la instalación de GLPI como el perfil predeterminado. Así, GLPI atribuye este perfil a cualquier nuevo usuario que se conecte. Descubriremos en este capítulo cómo es posible asignar permisos a un usuario (aplicación de un perfil en una o varias entidades).
- **Super-Admin:** este perfil posee todos los permisos y por ello la configuración y ajuste de la aplicación. El número de usuarios con este perfil debe ser restringido.

- **Supervisor:** este perfil toma los elementos del perfil Técnico añadiendo elementos que permiten la gestión de un equipo y su organización (atribución de tickets ...).
- **Technician:** este perfil corresponde al utilizado para un técnico de mantenimiento. Tiene acceso al inventario de lectura y al servicio de asistencia para procesar tickets.

Página Principal: Donde encontraran un resumen de los casos de acuerdo el estado en que se encuentren.



La plataforma cuenta con una barra de herramienta que permite navegar entre las distintas características que ofrece.

Inventario:



Permite llevar control de los activos adquiridos por el SENA que apliquen para la ejecución de este contrato y son registrados por los usuarios con el rol Super-Admin.

Soporte:



Se accede a todos los casos de soporte creados, permite ver o filtrar los casos según su estado, crear los cambios que sean necesarios en el proyecto o ver estadísticas que permiten llevar seguimiento de manera grafica en la atención de los casos.

Gestión:



Se realiza un seguimiento de sus gastos, contratos y proveedores, cree nuevos objetos de inventario, gestione la base de datos de usuarios y realice informes.

Útiles:



Es el espacio donde se acceden a los artículos de conocimiento creados. También permiten crear proyectos en los cuales se crean tareas, se asignan responsables, se crea un cronograma y permite llevar control de cada una de las actividades.

Administración



Se encuentra toda la administración realizada en la plataforma relacionadas a usuarios con acceso, grupo de soporte creados y definición de roles.

Configuración



Se encuentran las configuraciones administrativas y técnicas aplicada la plataforma entre las cuales se encuentran árbol de categorías, correo de recepción de casos, tiempo de respuesta, definición de frecuencia de backup de la base de datos, Plantillas de respuesta, entre otros.

Gestión del soporte:

Para la gestión del soporte se encuentra con las siguientes características e implementaciones.

Tickets

GLPI permite a los usuarios con acceso seleccionar entre Incidente o Solicitud al crear el ticket. Cada categoría podría asignarse a un grupo específico de usuarios / perfiles o responsable.

Problemas

La función Problema en GLPI permite informar, asignar y planificar, etc., acciones o decisiones y se puede distinguir por sus conceptos: reclamantes, observadores, asignación, estado, urgencia, impacto, prioridad, categoría.

Cambios (RFC)

La característica de «Cambio» es el establecimiento de la resolución de un problema (en el sentido GLPI o no) o el establecimiento de un nuevo elemento o proceso material / humano de su SI. El cambio le permite informar, asignar, planificar, presupuestar, etc.

Planificación

La función de planificación en GLPI le permite realizar un seguimiento de las tareas de los agentes de TI, verificar el estado de los proyectos y tener una visión general de la actividad de la empresa.

Estadísticas

Con Estadísticas en GLPI puede visualizar estadísticas sobre los tickets, encuestas de satisfacción, tiempo medio, duración media real del tratamiento, sobre los componentes de las computadoras, número de tickets asignados a cada artículo, etc.

Tickets recurrentes

Es posible programar la apertura de tickets de forma recurrente. Por ejemplo: abra un ticket todos los viernes por la mañana para hacer una copia de seguridad en cinta esa misma noche.

Formularios

Cree formularios personalizados y de fácil acceso para los usuarios cuando quieran crear uno o más tickets o cambios.

Categorización de casos:

Para llevar una gestión más eficaz de los casos creados, se implementó un árbol de categorías que contiene de manera detallada los posibles escenarios que se pueden presentar en el soporte brindado. Las categorías implementadas son:

Administración de Usuarios

Administración de Usuarios > Actualización Datos

Administración de Usuarios > Asignación datos

Administración de Usuarios > Creación

Administración de Usuarios > Suspensión datos

Administración de Usuarios > Validación Datos

Adobe Stock

Adobe Stock > Aplicación Web

Adobe Stock > Aplicación Web > Ajustes a la Aplicación

Adobe Stock > Aplicación Web > Bloqueo

Adobe Stock > Aplicación Web > Configuración

Adobe Stock > Aplicación Web > Gestión de la Demanda

Adobe Stock > Aplicación Web > Lentitud

Adobe Stock > Aplicación Web > Mensaje de error

Adobe Stock > Aplicación Web > No Ingresa

Adobe Stock > Aplicación Web > Sincronización de Datos

Comunicaciones

Comunicaciones > Notificaciones

Comunicaciones > Notificaciones > General
Correo electrónico
Correo electrónico > Publicidad
Correo electrónico > Spam
Creative Cloud
Creative Cloud > Aplicación Escritorio
Creative Cloud > Aplicación Escritorio > Actualización
Creative Cloud > Aplicación Escritorio > Adicion
Creative Cloud > Aplicación Escritorio > Ajustes a la Aplicación
Creative Cloud > Aplicación Escritorio > Bloqueo
Creative Cloud > Aplicación Escritorio > Caída
Creative Cloud > Aplicación Escritorio > Configuración
Creative Cloud > Aplicación Escritorio > Desinstalación
Creative Cloud > Aplicación Escritorio > Error Funcional
Creative Cloud > Aplicación Escritorio > Error Licencia
Creative Cloud > Aplicación Escritorio > Información Incorrecta
Creative Cloud > Aplicación Escritorio > Instalación
Creative Cloud > Aplicación Escritorio > Lentitud
Creative Cloud > Aplicación Escritorio > Mensaje de error
Creative Cloud > Aplicación Escritorio > No Ingresa
Creative Cloud > Aplicación Escritorio > Sincronización de Datos
Creative Cloud > Aplicación Escritorio > Usabilidad
Creative Cloud > Aplicación Web
Creative Cloud > Aplicación Web > Ajustes a la Aplicación
Creative Cloud > Aplicación Web > Bloqueo
Creative Cloud > Aplicación Web > Caída
Creative Cloud > Aplicación Web > Configuración
Creative Cloud > Aplicación Web > Error Funcional
Creative Cloud > Aplicación Web > Error Licencia
Creative Cloud > Aplicación Web > Información Incorrecta
Creative Cloud > Aplicación Web > Lentitud
Creative Cloud > Aplicación Web > Mensaje de error
Creative Cloud > Aplicación Web > No Ingresa
Creative Cloud > Aplicación Web > Sincronización de Datos
Horas experto
Licenciamiento
Licenciamiento > Preguntas relacionadas al uso
Media Pro
Vouchers
Vouchers > Asignación
Vouchers > Caída
Vouchers > Error Funcional
Vouchers > Generación de Informes
Vouchers > Información Incorrecta
Vouchers > Mensaje de Error
Mesa de ayuda
Mesa de ayuda > Cambios
Mesa de ayuda > Pruebas

Backup Base de datos y código aplicación:

La plataforma se encuentra implementada en un servidor en nube de propiedad del canal. El servidor cuenta con un script el cual se ejecuta tanto manual como cada 24 horas el cual genera un archivo; en este archivo se encontrará la base de datos de la mesa de ayuda así como los archivos fuentes hasta la fecha de realizado el respectivo backup.

El jefe de Soporte Técnico será el encargado de realizar estas copias de seguridad en un ubicación externa al servidor de manera periódica.

Plantillas de Respuesta y Solución:

Una de las funcionabilidades de la plataforma que nos permite ser más efectivos y dar el sello de calidad es la posibilidad de crear estándares de respuesta a la atención de casos mediante plantillas; esto nos permite poder contestar más rápido los casos y dar una sola respuesta en soluciones a problemas frecuentes mejorando la calidad de información.

Nuevo elemento - Seguimiento

Formatos ▾ **B** *I* A ▾ A ▾         

Buen día

Mi nombre es X y le ayudaré en la resolución del caso.

Revisando la base de datos encuentro que ya cuenta con la licencia Adobe Creative Cloud asignada al correo X. En este caso debe seguir los siguientes pasos:

1. Ingrese al siguiente link https://ims-na1.adobelogin.com/ims/authorize?client_id=oc_welcome&response_type=token&redirect_uri=https://www.adobe.com&prompt=login
2. La página le pedirá que inicie sesión. Ingrese con el correo electrónico X.
3. Si es la primera vez que ingresa con esa cuenta, tendrá que configurar una contraseña nueva para tener acceso a la licencia. Si no es así, se le pedirá que ingrese la contraseña para iniciar sesión.
4. Una vez halla ingresado correctamente, continúe de acuerdo a los pasos indicados en los manuales de instalación.

Windows: <https://acortar.link/cerScV>

Mac: <https://acortar.link/IOeNR3>

Tenga en cuenta que para los aprendices la licencia se asigna a los correos de dominio misena.edu.co y para instructores y funcionarios a los correos de dominio sena.edu.co.

Tiempo de atención

Hace referencia al tiempo que dispone el equipo de soporte para dar una primera respuesta formal con un diagnóstico y definir el tiempo de entrega de la solución al problema.

Niveles de Soporte y Mantenimiento:

Nivel 1

Son todas aquellas actividades de contacto inicial entre el administrador y la Consola de Administración, en este nivel el usuario administrador trata de evidenciar el problema e identifica si es problema de la herramienta o es un tema relacionado a la capacitación en el uso. Este nivel corresponde la mesa de ayuda por parte de Pc Mac S.A.

Hay disponibles tres (3) técnicos dedicados a este nivel para resolver casos básicos.

Michael Orejuela
Soporte técnico

Estephania Morales
Soporte técnico

Jairo Chaparro
Soporte técnico

Nivel 2

Son todos aquellos requerimientos relacionados directamente con la configuración, instalación o acceso a las opciones del sistema.

Se encuentra disponible dos (2) técnicos administrativos dedicados a este nivel para resolver casos

Para la atención de este nivel contamos con la mesa de ayuda y en dado caso que la solución no sea efectiva se realizará el procedimiento de subir a un nivel 3, se debe notificar a Customer Success Manager para supervisión y seguimiento del caso.

Jonathan Mauricio Cipagauta
Jefe de Soporte Técnico

Lina Alvarez
Directa de Proyecto

Nivel 3

Son todos aquellos incidentes que requieren un nivel de experticia tanto en las herramientas como posiblemente en llegar a realizar una intervención de código, presentación, temas de rendimiento, accesos denegados, entre otros.

Para la atención de Nivel 3 la mesa de servicio, al tener los accesos a la Consola de Administración subirá el caso al fabricante, del cual realizará las actualizaciones de avance que se tenga. Adobe Corroborará para que el soporte sea oportuno y eficaz.

Se encuentra disponible dos (2) técnicos administrativos por parte del canal dedicados a este nivel para resolver casos, si el caso es mayor se hará la solicitud directamente a fabricante.

Jonathan Mauricio Cipagauta
Jefe de Soporte Técnico

Lina Alvarez
Directa de Proyecto

Ubicación y Medios de Contacto Pc Mac S.A.

Cuenta con una mesa de apoyo en la ciudad de Bogotá y puede ser contactado a través de los siguientes canales de comunicación:

- Mesa de soporte: notificacionesadobe@sena.edu.co
- Línea Celular WhatsApp - 3182075324
- Cel. (57) (1) 611 1911 - 604 8282
- Horarios: Lunes a Viernes de 8:30 a.m a 5:30 p.m

Niveles de prioridad de la mesa de ayuda

Prioridad	Prioridad Herramienta de Gestión
Alta	1
Media	2
Baja	3

Definición de Prioridades:

Alta: El problema se traduce en interrupciones extremadamente graves de un sistema de producción.

Mediana: El problema provoca graves interrupciones en las operaciones normales y puede tener un impacto negativo en la instalación de toda la entidad o en plazos urgentes.

Baja: El problema provoca interrupciones en las operaciones normales.

Estado de los Tickets

Una vez que la Mesa de Ayuda realiza el registro de un requerimiento o incidencia esta puede pasar por los siguientes estados:

- **Nuevo:** Estado inicial de apertura de un Ticket del servicio El ticket debe permanecer en este estado hasta ser tomado por el Agente Resolutor, quien deberá, como primera acción actualizarlo para indicar su nueva condición (Cancelled, In Progress o Postponed). Este estado da inicio a la medición de los SLA comprometidos.

- **En curso Asignado:** Estado que se utiliza cuando el responsable de dar soporte (Agente Resolutor), inicia la fase de diagnóstico o solución del ticket. Cuando se transita por primera vez a este estado, se finaliza el cálculo del SLA denominado Tiempo de Atención (TDA).

- En curso planificado:

Estado que se utiliza para indicar que la atención del ticket se suspende indefinidamente (sin indicar hasta cuándo, así como en el caso del estado En espera).

En este estado se detienen los cálculos de los SLA denominados Tiempo de Atención (TDA) y Tiempo de Solución (TDS).

Al salir de este estado se retoman los cálculos de los SLA comprometidos.

Situaciones en donde utilizar este estado:

Garantías: cuando se está tramitando la garantía con un fabricante

Transito: el elemento/partes se encuentra en transporte hacia el destino

Aprobación: cuando el servicio se encuentra pendiente de una probación del cliente para compra de elementos y/o instalación de sw

- En espera: Estado que se utiliza cuando el responsable de dar soporte (Agente Resolutor), en común acuerdo con el usuario, coordinan retomar la entrega del servicio en una fecha/hora posterior. En este estado se detienen los cálculos de los SLA denominados Tiempo de Atención (TDA) y Tiempo de Solución (TDS). Al salir de este estado se retoman los cálculos de los SLA comprometidos.

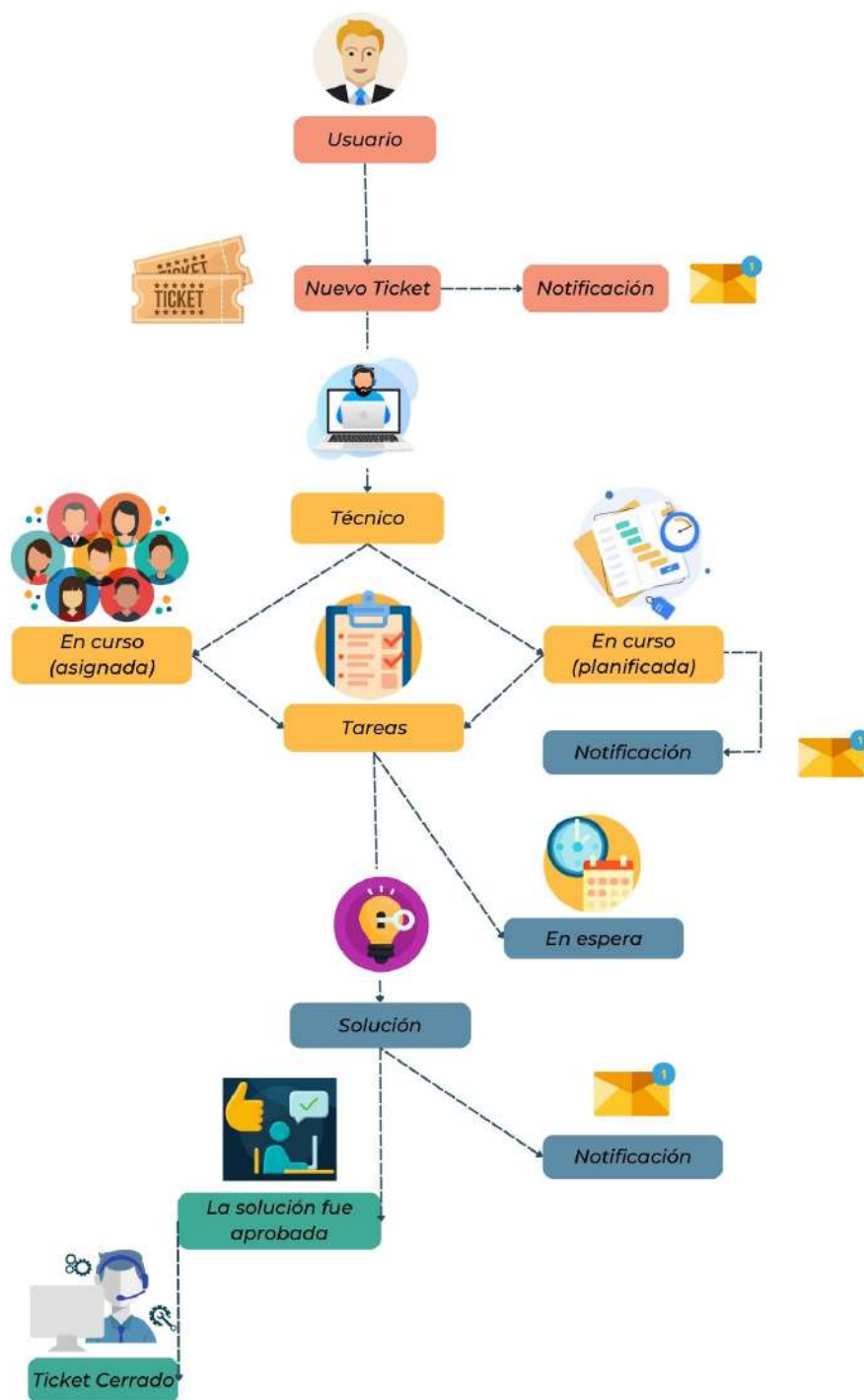
- Resuelto: Pre-Cierre, Estado utilizado cuando el responsable de dar el soporte soluciona de forma definitiva el ticket dando continuidad operativa al servicio. Cuando se transita a este estado sin pasar por el estado Parcialmente-Resuelto, se finaliza el cálculo del SLA denominado Tiempo de Solución (TDS). En este estado se permite reabrir el ticket.

- Re-abierto: Estado utilizado por el usuario para re abrir un Ticket antes de 48 horas. Su tratamiento es similar al estado Open, salvo que desde este estado no se permite transitar al estado cancelado.

- Cerrado: Estado utilizado para finalizar el ticket. En este estado no se permite reabrir el ticket.

- Cancelado: Estado que se utiliza para cancelar o anular un ticket generado por error o por duplicidad.

Flujo de trabajo



Calendario de Servicio de la mesa de ayuda para soporte

Calendarios Requerimiento		
Calendario	Descripción	Detalle
1	Horario Regular	9 horas x 5 días – Español Lunes a Viernes

Calendarios Incidentes		
Calendario	Descripción	Detalle
1	Horario Regular	24 horas x 7 días - 365 días al año – inglés

Contingencias del Servicio y Tiempos de Recuperación

Tiempos de Respuesta:

Clasificación de la Actividad	Concepto de Impacto	Cantidad de Horas para dar Respuesta	Cantidad de Horas estimadas para solucionar
Actividad Crítica.	Interrumpe el acceso al aplicativo.	30 minutos	12 hasta 24 horas.
Actividad Urgente	El problema provoca graves interrupciones en las operaciones normales y puede tener un impacto negativo en la instalación de toda la entidad o en plazos urgentes	Una hora	24 hasta 96 horas.
Actividad Importante	El problema provoca interrupciones en las operaciones normales.	Cuatro horas	96 hasta 128 horas.
Actividad Menor	El problema da lugar a interrupciones mínimas o nulas a las operaciones normales.	Un día hábil	96 hasta 128 horas.
Requerimiento Aprendiz	Consultas solicitudes de soporte o de acompañamiento realizadas por un aprendiz	3 día hábiles	96 hasta 128 horas.

ANS Comprometidos para Solicitudes de Servicio

Solicitudes de Servicio	Tiempo de Respuesta (Horas)
Dudas frente a la aplicación	9 horas
Capacitación	48 horas
Reportes de gestión	18 horas

INFRAESTRUCTURA DE SEGURIDAD DE LA PLATAFORMA GLPI

La plataforma GLPI es un aplicativo del servidor OVH

Seguridad de las infraestructuras de OVH

Seguridad de las infraestructuras: OVH se compromete a mantener una seguridad óptima de sus infraestructuras. Ente otras medidas, ha puesto en marcha una política de seguridad de sus sistemas de información y responde a las exigencias de múltiples normas y certificaciones (certificación PCI-DSS, certificación ISO/IEC 27001, certificaciones SOC 1 tipo II y SOC 2 tipo II...). OVHcloud también ofrece la autorización de alojamiento de datos de salud (HDS) para su solución Healthcare.

1. Sistema de gestión de la seguridad

Compromisos de OVH como proveedor de alojamiento

OVH aplica una política de seguridad de los sistemas de información (PSSI) que describe todos nuestros dispositivos en este ámbito. Nuestra PSSI se actualiza al menos una vez al año o en caso de que se produzcan cambios importantes que afecten a su contenido. La seguridad de nuestras soluciones, a su vez, se rige por sistemas de gestión de la seguridad de la información formales.

Existen diferentes funciones que coordinan nuestras acciones en lo que respecta a la seguridad perimetral:

- El responsable de la seguridad de los sistemas de información (RSSI).
- El responsable de seguridad, que se encarga de los procesos y proyectos relacionados con la seguridad perimetral.
- El delegado de protección de datos (DPO), que vela por la preservación de los datos personales.
- El gestor de riesgos, que coordina la gestión de los riesgos de seguridad y los planes de acción apropiados.
- El responsable de las medidas de seguridad, que implementa y aplica las disposiciones relativas a los riesgos identificados.

2. Conformidad y certificación

Compromisos de OVH como proveedor de alojamiento

Para garantizar el mantenimiento de la conformidad y evaluar la eficacia de nuestros sistemas, se realizan periódicamente auditorías de seguridad. Estas pueden ser de cinco tipos:

- Auditorías externas (certificaciones, clientes);
- Auditorías internas, llevadas a cabo por auditores internos o externos;
- Auditorías técnicas (pruebas de intrusión, escaneos de vulnerabilidad, revisiones de código), llevadas a cabo por auditores internos o externos;
- Auditorías de las actividades de terceros, realizadas por el responsable de la gestión de terceros;

- Auditorías de los datacenters, llevadas a cabo por auditores internos. La naturaleza y la frecuencia de las auditorías realizadas dependen de la solución y el perímetro. Cuando se identifica una situación no conforme, se añade la correspondiente medida correctiva a los planes de acción. Todas estas medidas están sujetas a un seguimiento formal, del que se guarda un registro, así como a una revisión periódica donde se vuelve a examinar su efectividad.

3. Auditorías del cliente

Recomendaciones destinadas al cliente responsable del tratamiento

El cliente puede realizar por su cuenta auditorías técnicas (pruebas de intrusión) en los servicios alojados, así como en los componentes de gestión del servicio. Las condiciones de realización de las auditorías están estipuladas en los contratos o se gestionan ad hoc a petición del cliente.

Compromisos de OVH como proveedor de alojamiento

Las condiciones de realización de las auditorías están estipuladas en los contratos o se gestionan ad hoc a petición del cliente.

4. Gestión de riesgos

Recomendaciones destinadas al cliente responsable del tratamiento

El cliente debe asegurarse de que las medidas de seguridad implementadas por OVH sean suficientes con respecto a los riesgos derivados del uso que haga de la infraestructura.

Compromisos de OVH como proveedor de alojamiento

OVH aplica una metodología formal de gestión de riesgos, que se revisa al menos una vez al año o en caso de cambios importantes y que también afecta a los datos personales y datos sensibles (salud, pagos, etc.).

Esta metodología formaliza los análisis realizados: identificación de activos, procesos críticos, amenazas y vulnerabilidades.

Se basa en la norma ISO 27005. Al finalizar cada análisis se elabora un plan para hacer frente a los riesgos identificados. Este se pone en marcha en un plazo máximo de 12 meses. El plan documenta el análisis detalladamente y prioriza las acciones a realizar. Cada medida correctiva se añade a los planes de acción y se le hace un seguimiento formal, del que se guarda un registro, y una revisión periódica en la que se vuelve a examinar su efectividad.

4. Gestión del cambio

Recomendaciones destinadas al cliente responsable del tratamiento

El cliente debe asegurarse de que sus datos de contacto son correctos para que OVH pueda notificarle los cambios que puedan afectar a sus soluciones. En caso necesario, corresponde al cliente llevar a cabo las acciones necesarias en la configuración de sus servicios para adaptarse a dichos cambios.

Compromisos de OVH como proveedor de alojamiento

OVH dispone de un procedimiento formal de gestión del cambio:

- Las funciones y responsabilidades están claramente definidas.
- Se han especificado criterios de clasificación para identificar los pasos a seguir para implementar el cambio.
- Se gestionan las prioridades. Se lleva a cabo un análisis de los riesgos asociados a los cambios (si se identifica un riesgo, el responsable de seguridad y el gestor de riesgos participan en la validación del cambio).
- Se realizan pruebas de intrusión (si es aplicable). El cambio se planifica y se programa con los clientes (si es aplicable).
- El despliegue es progresivo (1/10/100/1000) y, en caso de riesgo, se prevé un procedimiento de reversión de los cambios.
- Se lleva a cabo una revisión a posteriori de los diferentes activos afectados por el cambio.
- Se documentan los pasos en la herramienta de gestión del cambio.

6. Política de desarrollo de sistemas y aplicaciones

Compromisos de OVH como proveedor de alojamiento

OVH implementa y documenta los procesos que deben seguir sus desarrolladores. Estos procesos contienen los principios para desarrollar de forma segura, las medidas de protección de datos desde el diseño y una política de revisión del código (detección de vulnerabilidades, tratamiento de errores, gestión de los accesos y entradas, seguridad del almacenamiento y las comunicaciones).

- También se realizan revisiones de código periódicamente.
- validación de las nuevas funcionalidades antes del lanzamiento, pruebas en el entorno de validación (si es aplicable) y despliegue progresivo (1/10/100/1000);
- separación de funciones y responsabilidades entre los desarrolladores y las personas encargadas de la puesta en producción.

7. Monitorización de los servicios y las infraestructuras

Compromisos de OVH como proveedor de alojamiento

Todos los servicios de OVH cuentan con una infraestructura de monitorización. Sus objetivos son múltiples:

- Detectar incidencias de producción y seguridad;
- Vigilar las funciones críticas, enviando una alerta al sistema de supervisión;
- Avisar a los responsables y activar los procedimientos adecuados;
- Asegurar la continuidad del servicio en la realización de las tareas automatizadas;
- Asegurar la integridad de los recursos monitorizados.

8. Gestión de incidencias

Recomendaciones destinadas al cliente responsable del tratamiento

El cliente debe asegurarse de que sus datos de contacto son correctos para que OVH pueda notificarle posibles incidencias. También debe establecer procedimientos de gestión de las incidencias que afecten a su sistema de información, incluyendo a OVH como posible fuente de alerta.

Compromisos de OVH como proveedor de alojamiento

Existe un procedimiento de gestión de incidencias que permite prevenir, detectar y resolver estas contingencias en las infraestructuras de gestión del servicio y en el propio servicio. Dicho procedimiento incluye:

- Una guía de calificación de los eventos de seguridad.
- Tratamiento de los eventos de seguridad.
- Ejercicios de simulación para la célula de crisis.
- Pruebas del plan de respuesta a incidencias.
- Comunicación con el cliente en el marco de una célula de crisis.

Estos procedimientos están integrados en un proceso de mejora continua para la vigilancia, evaluación y gestión global de las incidencias y de sus acciones correctivas.

9. Gestión de vulnerabilidades

Recomendaciones destinadas al cliente responsable del tratamiento

El cliente debe asegurarse de que sus datos de contacto son correctos para que OVH pueda notificarle posibles vulnerabilidades detectadas en su sistema de información.

Compromisos de OVH como proveedor de alojamiento

El responsable de seguridad y su equipo efectúan un seguimiento de las nuevas vulnerabilidades, identificándolas a través de:

- Sitios web públicos de información.
- Alertas de los fabricantes y editores de las soluciones desplegadas.
- Incidencias y observaciones comunicadas por nuestros equipos de operaciones, terceros o clientes.
- Escaneos de vulnerabilidades internos y externos realizados periódicamente.
- Auditorías técnicas, así como revisiones de código y de configuración.

Si se detecta una vulnerabilidad, un equipo específico realiza un análisis para determinar su impacto potencial en los sistemas y escenarios operativos.

Si es necesario, se ponen en marcha acciones de mitigación y se define un plan correctivo.

Las medidas adoptadas se añaden a los planes de acción y se les hace un seguimiento formal, del que se guarda un registro. Asimismo, cada medida es sometida a una revisión periódica en la que se vuelve a examinar su efectividad.

10. Gestión de la continuidad del negocio

Recomendaciones destinadas al cliente responsable del tratamiento

La continuidad del sistema de información es responsabilidad del cliente. Este último debe asegurarse de que los dispositivos estándar implementados por OVH, las opciones contratadas y los mecanismos complementarios que él implemente le permitirán alcanzar sus objetivos.

Compromisos de OVH como proveedor de alojamiento

La continuidad de la actividad de las infraestructuras (disponibilidad de los dispositivos, las aplicaciones y los procesos operativos) se asegura mediante diferentes mecanismos:

- Continuidad de la refrigeración líquida y por aire.
- Continuidad y redundancia del suministro de electricidad.
- Gestión de la capacidad de los dispositivos que se encuentran bajo la responsabilidad de OVH;
- Asistencia técnica del servicio.
- Redundancia de los dispositivos y servidores utilizados en la administración de los sistemas.

Además, existen otros mecanismos que aseguran la reanudación del servicio en caso de incidencia, tales como la copia de seguridad de la configuración de los dispositivos de red.

En función del servicio, OVH puede ofrecer funcionalidades de backup y de restauración, incluidas de manera estándar o como opción de pago, que el cliente podrá utilizar.

11. Riesgos naturales y medioambientales

Compromisos de OVH como proveedor de alojamiento

OVH aplica medidas destinadas a prevenir los riesgos naturales y medioambientales:

- Instalación de pararrayos para reducir la onda electromagnética concomitante.
- Ubicación de las instalaciones de OVH en zonas no inundables y sin riesgos sísmicos.
- Presencia de sistemas de alimentación ininterrumpida (SAI) con capacidad suficiente y de transformadores de emergencia con conmutación automática de la carga.
- Activación automática de los grupos electrógenos con una autonomía mínima de 24 horas.
- Instalación de un sistema de refrigeración líquida de los servidores (el 98% de las salas de alojamiento no tienen climatización).
- Despliegue de unidades de calefacción, ventilación y aire acondicionado (HVAC) que mantienen la temperatura y la humedad a un nivel constante.
- Gestión de un sistema de detección de incendios (en los datacenters se realizan simulacros de incendio cada 6 meses).

12. Medidas generales de seguridad de las instalaciones

Compromisos de OVH como proveedor de alojamiento

El acceso físico a las instalaciones de OVH está basado en una política de seguridad perimetral restrictiva, efectiva desde el área de entrada. Cada local se clasifica en las siguientes categorías:

- Zonas de circulación privadas.
- Oficinas accesibles para todos los trabajadores y visitantes registrados.
- Oficinas confidenciales, restringidas a determinadas personas.
- Zonas que albergan el equipamiento de los datacenters.
- Zonas confidenciales de los datacenters.
- Zonas de los datacenters que albergan servicios críticos.

13. Medidas generales de seguridad de las instalaciones

Compromisos de OVH como proveedor de alojamiento

Existen medidas de seguridad para controlar el acceso a las instalaciones de OVH:

- Política de derechos de acceso.
- Paredes (o mecanismos equivalentes) entre cada zona.
- Cámaras situadas en las entradas y salidas de las instalaciones, así como en las salas de servidores.
- Acceso seguro controlado por lectores de acreditaciones.
- Barreras láser en los aparcamientos.
- Sistema de detección de movimiento.
- Mecanismos de prevención de accesos forzados en las entradas y salidas de los datacenters;
- Mecanismos de detección de intrusos (seguridad las 24 horas y videovigilancia).
- Centro de vigilancia permanente, que controla las aperturas de las puertas de entrada y salida.

14. Acceso a las instalaciones de OVH

Compromisos de OVH como proveedor de alojamiento

Los controles de acceso físico se basan en un sistema de acreditaciones. Cada acreditación está asociada a una cuenta de OVH, asociada a su vez a una persona. Este mecanismo permite identificar a cualquier persona en las instalaciones y autenticar los mecanismos de control:

- Cada persona que acceda a las instalaciones de OVH debe tener una acreditación personal vinculada a su identidad.
- La identidad se verifica antes de entregar cualquier acreditación.
- En las instalaciones es necesario llevar la acreditación en un lugar visible.
- Las acreditaciones no deben mencionar el nombre del titular o de la empresa.
- Las acreditaciones deben permitir identificar de inmediato las categorías de las personas presentes (trabajadores, terceros, acceso temporal o visitantes).

- La acreditación se desactiva en cuanto su titular deja de estar autorizado para acceder a las instalaciones.
- La acreditación de los trabajadores de OVH se activa durante la vigencia de su contrato de trabajo (para las demás categorías, se desactiva automáticamente al cabo de un período de tiempo determinado).
- Cuando una acreditación no se utiliza durante tres semanas, esta se desactiva automáticamente.

15. Gestión de los accesos a las zonas

Compromisos de OVH como proveedor de alojamiento

Acceso en las puertas mediante acreditación

Este es el control de acceso estándar en las instalaciones de OVH:

La puerta está conectada al sistema centralizado de gestión de los derechos de acceso.

La persona debe pasar su acreditación por el lector para desbloquear la puerta.

Los accesos se verifican en el momento de la lectura para asegurarse de que las personas tengan los derechos de entrada adecuados.

En caso de avería del sistema centralizado de gestión de los derechos de acceso, los derechos configurados en el momento de la incidencia son válidos hasta que esta se resuelva.

Las cerraduras de las puertas están protegidas frente a cortes de electricidad y permanecen cerradas en esos casos.

Acceso en las puertas mediante acreditación

Algunas áreas o dispositivos se cierran mediante cerraduras de llave:

En cada una de las instalaciones, las llaves se guardan en un lugar centralizado y restringido, con un listado de todas las llaves.

Cada llave se identifica mediante una etiqueta. Existe un inventario de las llaves.

Cualquier uso de las llaves se puede rastrear a través de un mecanismo de entrega o un libro de registro en papel.

El listado de las llaves se coteja diariamente con el inventario.

Acceso a los datacenters por esclusas unipersonales

El acceso a nuestros centros de datos se efectúa exclusivamente a través de esclusas unipersonales:

Cada esclusa tiene dos puertas y un compartimento intermedio, con el fin de asegurarse de que solo pase una persona a la vez.

Solo es posible abrir una puerta si la otra está cerrada (mantrap).

Las esclusas utilizan el mismo sistema de acreditaciones que las otras puertas, y se aplican las mismas reglas.

Unos mecanismos de detención comprueban que solo haya una persona en la esclusa (anti-piggybacking).

El sistema está configurado para impedir que la acreditación pueda utilizarse más de una vez en el mismo sentido (anti-passback).

Una cámara colocada alrededor de la esclusa permite vigilar las entradas.

Acceso a las esclusas de mercancías

- Las entradas de mercancías a los datacenters se realizan exclusivamente a través de pasarelas específicas:
- El vestíbulo de entrega está configurado de la misma forma que una esclusa unipersonal, pero con un espacio mayor, sin control sobre el volumen y el peso, y con lectores de acreditaciones solo en el exterior.
- Por el vestíbulo solo pasa el artículo entregado (las personas deben acceder a través de las esclusas unipersonales).
- En el vestíbulo hay una cámara sin ángulos muertos.

16. Gestión de accesos físicos de terceros

Recomendaciones destinadas al cliente responsable del tratamiento

OVH nunca interviene en las instalaciones de sus clientes. Estos últimos son responsables de la seguridad de sus instalaciones.

Compromisos de OVH como proveedor de alojamiento

La circulación de visitantes y proveedores de servicios ocasionales está estrictamente regulada. Estas personas se registran en cuanto llegan a las instalaciones y se les proporciona una acreditación de visitante o proveedor de servicios:

- Cada visita debe notificarse con antelación.
- Estas personas externas están bajo la responsabilidad de un empleado y siempre van acompañadas.
- Siempre se verifica la identidad antes de permitir el acceso a las instalaciones.
- Cada persona externa tiene una acreditación personal asignada para ese día, que debe devolver antes de abandonar las instalaciones.
- Las acreditaciones siempre deben llevarse en un lugar visible.
- Las acreditaciones se desactivan automáticamente al final de la visita.

17. Sensibilización y formación del personal

Compromisos de OVH como proveedor de alojamiento

El personal de OVH conoce las normas de seguridad y las reglas de conformidad del tratamiento de datos personales:

- Anualmente se imparten sesiones de formación sobre estos temas para los equipos implicados.
- Anualmente se imparten sesiones de formación sobre la realización de las auditorías para los equipos implicados.
- Anualmente se imparten sesiones de formación sobre los servicios técnicos para los equipos implicados.

- Cuando se incorporan nuevos empleados se les sensibiliza sobre la seguridad del sistema de información (SI).
- Periódicamente se envían a todo el personal comunicaciones relativas a la seguridad.
- Se organizan campañas de prueba para garantizar que adquieran los hábitos adecuados en caso de amenaza.

18. Gestión de accesos lógicos al sistema de información de OVH

Compromisos de OVH como proveedor de alojamiento

OVH aplica una estricta política de gestión de los accesos lógicos para los empleados:

- Los permisos son concedidos y supervisados por los responsables directos según los principios de mínimo privilegio y de adquisición gradual de la confianza.
- En la medida de lo posible, todos los permisos se basan en funciones y no en derechos unitarios.
- La gestión de los derechos de acceso y los permisos asignados a un usuario o sistema se basan en un procedimiento de registro, modificación y cancelación que involucra a los responsables, al departamento interno de informática y a recursos humanos.
- Todos los empleados usan cuentas de usuario nominativas.
- Las sesiones de conexión siempre tienen un tiempo de expiración que depende de cada aplicación.
- La identidad de los usuarios se verifica antes de cualquier cambio en los medios de autenticación.
- En caso de olvidar la contraseña, solo el responsable del trabajador y el responsable de seguridad están autorizados para restablecerla.
- Las cuentas de usuario se desactivan automáticamente si la contraseña no se renueva cada 90 días.
- Está prohibido el uso de cuentas predeterminadas, genéricas y anónimas.
- Se aplica una política de contraseñas estricta.
- El usuario no elige su contraseña, sino que esta se genera automáticamente.
- La longitud mínima de una contraseña es de 10 caracteres alfanuméricos.
- La frecuencia de renovación de la contraseña es de 3 meses.
- Está prohibido almacenar contraseñas en archivos no encriptados, en papel o en navegadores web.
- Es obligatorio utilizar un programa de gestión de contraseñas local validado por los equipos de seguridad.
- El acceso remoto al sistema de información (SI) de OVH siempre se realiza a través de una VPN, que requiere una contraseña conocida solo por el usuario y un secreto compartido configurado en el equipo de trabajo.

19. Gestión de accesos de administración a las plataformas de producción

Compromisos de OVH como proveedor de alojamiento

OVH aplica una política de gestión de los accesos de administración de las plataformas:

- Todos los accesos de administración a un sistema en producción se realizan a través de un bastión.
- Los administradores se conectan a los bastiones por SSH, utilizando parejas de claves públicas y privadas individuales y nominativas.
- La conexión al sistema de destino se realiza, o bien mediante una cuenta de departamento compartida, o bien mediante una cuenta nominativa a través de los bastiones. Está prohibido utilizar cuentas predeterminadas en los sistemas y dispositivos.
- La autenticación de doble factor es obligatoria para el acceso remoto tanto de los administradores como de los empleados con accesos a perímetros sensibles, y se guarda un registro completo para permitir la trazabilidad.
- Los administradores tienen una cuenta exclusivamente dedicada a las tareas de administración, además de su cuenta de usuario.
- Los permisos son concedidos y supervisados por los responsables directos según los principios de mínimo privilegio y de adquisición gradual de la confianza.
- Las claves SSH están protegidas con una contraseña que debe cumplir los requisitos de la política de contraseñas. Se realiza una revisión periódica de los derechos y accesos en colaboración con los departamentos pertinentes.

20. Control de los accesos al área de cliente

Recomendaciones destinadas al cliente responsable del tratamiento

El cliente es responsable de la gestión y la seguridad de sus medios de autenticación. Para proteger mejor el acceso a su cuenta, este tiene la posibilidad de: • activar la doble autenticación en el área de cliente de OVH; • restringir las conexiones a una lista de direcciones IP previamente declaradas.

Compromisos de OVH como proveedor de alojamiento

La gestión de los servicios de OVH por el cliente se realiza a través del área de cliente o la API. Por defecto, el acceso se realiza a través de una cuenta nominativa (ID de cliente) y una contraseña:

- El cliente elige la contraseña, que debe cumplir los criterios de complejidad impuestos por la interfaz.
- En los servidores de OVH solo se almacenan los hashes de las contraseñas.
- OVH ofrece la posibilidad de activar la doble autenticación desde el área de cliente, a través de un sistema de contraseñas de un solo uso (OTP) enviadas por SMS, el uso de una aplicación móvil o la utilización de una clave compatible con U2F.
- El cliente puede restringir el acceso a su área de cliente a direcciones IP determinadas.
- Los tokens de acceso a la API se pueden utilizar durante su período de validez sin volver a pasar controles específicos.
- Todas las actividades de los clientes en el área de cliente o en la API quedan registradas.
- El cliente puede separar las tareas técnicas y administrativas relacionadas con la gestión de los servicios.

21. Seguridad de los equipos de trabajo y los dispositivos móviles

Recomendaciones destinadas al cliente responsable del tratamiento

El cliente debe garantizar la seguridad de los equipos de trabajo y los dispositivos móviles que permitan administrar el servicio y los sistemas.

Compromisos de OVH como proveedor de alojamiento

Seguridad de los equipos de trabajo estándar

OVH aplica medidas para garantizar la seguridad de los equipos de trabajo estándar del personal:

- Gestión automática de actualizaciones;
- Instalación y actualización de antivirus, con escaneos regulares; • posibilidad de instalar únicamente aplicaciones de un catálogo validado;
- Cifrado sistemático de los discos duros;
- Ausencia de derechos de administración para los empleados en sus equipos de trabajo;
- Procedimiento de actualización sobre los equipos de trabajo potencialmente comprometidos;
- Estandarización de los equipos;
- Procedimiento de eliminación de las sesiones y restauración de los equipos cuando un empleado deja de trabajar en la empresa.

Seguridad de los terminales móviles

OVH aplica medidas para garantizar la seguridad de los dispositivos móviles personales o proporcionados por OVH:

- Registro obligatorio de los terminales en el sistema de gestión centralizado, antes de acceder a los recursos internos (wifi, correo electrónico, calendarios, directorio, etc.);
- Verificación de la política de seguridad implementada en el terminal (código de desbloqueo, temporización de bloqueo automático, cifrado del almacenamiento);
- Procedimiento de borrado remoto de los terminales en caso de pérdida o robo.

22. Seguridad de la red

Recomendaciones destinadas al cliente responsable del tratamiento

El cliente es el único responsable de la encriptación del contenido comunicado a través de la red de OVH.

Compromisos de OVH como proveedor de alojamiento

OVH gestiona una red privada de fibra óptica de alta velocidad, interconectada con numerosos operadores de internet y de tránsito. OVH gestiona su propio backbone, que distribuye la conectividad a las redes locales de cada datacenter y los interconecta.

Todo este equipamiento está protegido por las siguientes medidas:

- Mantenimiento de un inventario dentro de una base de gestión de las configuraciones.
- Establecimiento de un proceso de hardening, con manuales que describen los parámetros que deben modificarse para garantizar que la configuración sea segura.

- Los accesos a las funciones de administración de los dispositivos están restringidos mediante listas de control.
- Todos los dispositivos se gestionan a través de un bastión, aplicando el principio de mínimo privilegio.
- Se realizan copias de seguridad de todas las configuraciones de los dispositivos de red.
- El equipo de operaciones de red recopila, centraliza y monitoriza los logs permanentemente.
- El despliegue de configuraciones está automatizado y se basa en plantillas validadas.

23. Gestión de la continuidad del negocio

Compromisos de OVH como proveedor de alojamiento

OVH aplica una política de backup en los servidores y dispositivos que utiliza para prestar sus servicios:

- Se realiza copia de seguridad de todos los sistemas y datos necesarios para la continuidad de los servicios, la reconstrucción del sistema de información o el análisis posterior a las incidencias (archivos de las bases de datos técnicas y administrativas, historiales de actividad, código fuente de las aplicaciones desarrolladas internamente, configuración de los servidores, aplicaciones y dispositivos, etc.).
- Las frecuencias, tiempos de retención y métodos de almacenamiento de las copias de seguridad se establecen de acuerdo con las necesidades de cada activo. Se monitoriza la realización de las copias de seguridad, y se gestionan las alertas y errores.

24. Historización

Recomendaciones destinadas al cliente responsable del tratamiento

El cliente es el único responsable de la política de historización de sus propios sistemas y aplicaciones.

Compromisos de OVH como proveedor de alojamiento

OVH aplica una política de conservación de registros en los servidores y dispositivos que utiliza para prestar sus servicios:

- Backup y conservación centralizada de los logs.
- Consulta y análisis de los logs por un número limitado de actores autorizados, con arreglo a la política de permisos y de gestión de los accesos.
- Separación de tareas entre los equipos responsables del funcionamiento de la infraestructura de monitorización y los equipos responsables del funcionamiento del servicio. A continuación se detalla la lista de actividades de las que se conserva un registro.
- Logs de los servidores de almacenamiento que alojan los datos de los clientes.
- Logs de las máquinas que gestionan la infraestructura del cliente.
- Logs de las máquinas destinadas a la monitorización de la infraestructura.
- Logs de los antivirus instalados en todas las máquinas equipadas con ellos.
- Control de la integridad de los logs y los sistemas, cuando corresponda.
- Tareas y eventos realizados por el cliente en su infraestructura.
- Logs y alertas de detección de intrusos en la red, cuando corresponda.
- Logs de los dispositivos de red.
- Logs de la infraestructura de las cámaras de vigilancia.

- Logs de las máquinas de los administradores.
- Logs de los servidores de tiempo.
- Logs de los lectores de acreditaciones.
- Logs de los bastiones.

5. Plataforma de correos masivos (SendPulse)

LA INFRAESTRUCTURA TECNOLÓGICA DE LA PLATAFORMA SENDPULSE

Con el fin de garantizar la divulgación y promoción del uso del licenciamiento entre los usuarios, el envío de manuales, videos, instructivos, eventos de entrenamiento, capacitación, etc; Hacemos la entrega de un software de correos masivos de uso educativo, para que el Formación Profesional puedan difundir información de forma directa y exclusiva para sus objetivos de su distribución de contenido.

Contenido:

La plataforma tiene 125.000 destinatarios, los usuarios pueden agregar correos electrónicos y una salida ilimitada de correos electrónicos con un validador de correo electrónico para 100 correos electrónicos.

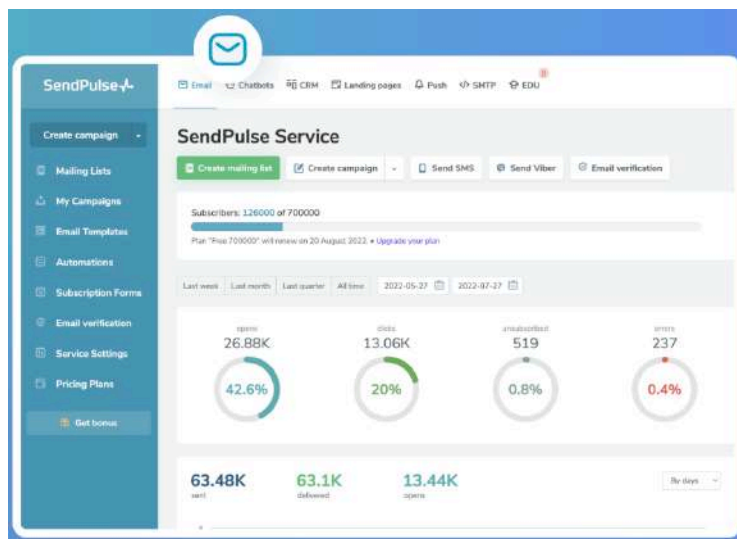
Alcance de la herramienta:

Con SendPulse enviar correos transaccionales es seguro, confiable y rápido no hay restricciones en el número de listas de correo electrónico que puedes agregar, no necesitas realizar muchas configuraciones y lo mejor de todo, los pagos mensuales no son obligatorios, puedes pagar a medida que envías los correos.

Esta confirmado por las siguientes características:

- * Correos electrónicos
- * Chatbots
- * Landing Pages
- * Creador de Cursos
- * CRM
- * Web Push
- * SMS
- * Viber
- * SMTP

- Servicio de Correo Electrónico



Cómodo editor de correo electrónico

El constructor de arrastrar y soltar permite crear rápidamente y fácilmente plantillas de correos electrónicos profesionales. No se necesita habilidades técnicas o conocimiento en HTML para crear una plantilla.

Formularios de suscripción

Para crear un formulario de suscripción único usando los colores y el estilos. Se coloca en el sitio web, selecciona suscriptores y envía a los correos electrónicos.

Más de 130 plantillas responsivas

Para diseñar y construir una plantilla de correo es más fácil y rápido. Navegar en las plantillas gratis de correo electrónico y se selecciona la que cumpla con los requisitos solicitados.

Automation 360

Con Automation 360 se puede configurar correos electrónicos, mensajes de chatbots, notificaciones web push, y flujos de SMS basados en variables, eventos y las acciones que los usuarios realizan.

Reenvía mensajes no abiertos

Para incrementar la tasa de apertura de las campaña reenviando un correo con una nueva línea de asunto a todos los destinatarios que no han abierto el correo electrónico anterior.

Personalización

Para aprovechar la información que tienes de los usuarios: los nombres, ubicación, fecha de nacimiento, etc. (Si se logra obtener), para incrementar la confianza, interacción y relevancia con cada correo electrónico que se envíen

Segmentación

Al envía diferentes correos electrónicos a los usuarios dependiendo el género, ubicación geográfica o intereses en particular.

Prueba A/B

Al tener diferentes versiones de correo electrónico usando diferentes líneas de asunto o contenido del mensaje. Después, se envía la versión que genera mejores resultados. Ese correo electrónico será el más efectivo.

Estadísticas

El servicio brinda estadísticas de apertura y clics para así poder monitorear los resultados y mejorar las campañas de correo electrónico.

Calificación del suscriptor

Para analiza la actividad de los usuarios, segmenta la lista de envío, y usa un acercamiento personal cuando trabajas en ellas.

Niveles de acceso de usuario

Para colaborar a los usuarios, dando acceso solo a ciertas secciones del servicio. Excluye acceso a áreas que contienen información confidencial.

Integración

Al integrar correos electrónicos al CRM o sistema CMS. Se puede enviar correos electrónicos directamente desde el propio proyectos, supervisar las campañas y ver estadísticas.

Aplicación móvil

Agrega nuevos usuarios a las listas de envío, Se puede enviar correos electrónicos, y consultar los resultados de las campañas en donde sea.

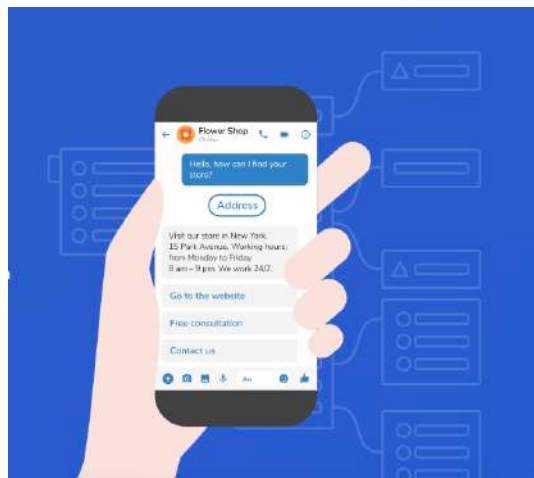
Correos AMP

Se puede enviar correos interactivos a los usuarios usando la tecnología AMP4Email la cual permite cambiar el contenido de correos electrónicos al instante.

Verificador de correo electrónico

Para verificar la lista de envío y limpiarla de direcciones de correo electrónico no existentes, spam, y direcciones con errores de tipografía.

- **Chatbots**



Crear multiples chatbots

Se puede agregar un chatbot a Facebook, Telegram o a WhatsApp y enviar a los usuarios mensajes en masa y personalizados.

Widgets de suscripción

Suscribir a los usuarios a las actualizaciones en Facebook Messenger, Telegram, y WhatsApp por medio de un widget en la página web.

Chatbot de Facebook

Crear flujos de auto-respuestas y entrega mensajes en grupo y personalizados en Facebook Messenger.

Editor de flujo de auto respuesta

Crear una serie de mensajes para ser enviados automáticamente a los usuarios basados en las acciones o palabras claves que utilizan en el chat.

Segmentación de suscriptores de chatbot

Según los datos de suscriptor que se maneje, se puede enviar campañas a sectores específicos de un público más amplio. Una campaña adecuadamente segmentada es más relevante para el grupo seleccionado de destinatarios.

Campañas y chatbots de WhatsApp

Enviar mensajes a través de un proveedor oficial de API WhatsApp Business. Configurando un chatbot para autorespuestas y enviar mensajes accionadores en WhatsApp.

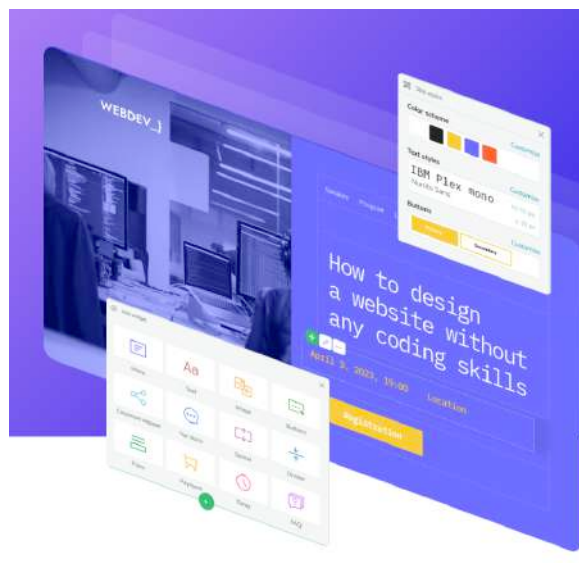
Aplicación de Chatbot

Instalar la aplicación para estar en contacto con los usuarios y enviar respuestas rápidas vía chatbots de Facebook, Telegram y WhatsApp.

API en WhatsApp para Negocios

Enviar campañas personalizadas de la solicitud y mensajes de chatbot en WhatsApp. Comunicarse con los usuarios en una sesión gratuita de 24 horas e integra WhatsApp con las herramientas de servicio de la entidad.

- **Landing Pages**



Landing Pages y tiendas en línea

Para crear páginas web sin codificar. Publícalas gratuitamente con un dominio ofrecido o conectarla al dominio único para incrementar la percepción de la marca y obtener más visitantes a la página web.

Plantillas Prediseñadas

Usar las plantillas para crear landing pages. Las herramientas ayudarán a editar las plantillas de acuerdo al estilo de la marca y las necesidades de la entidad. Se puede agregar contenido y contactos.

Enlace de página a la bio de redes sociales

Al colocar múltiples links de las redes sociales en la bio. Se comparte un enlace de página bio a los usuarios para que puedan conocer más de los productos y servicios, conectar el administrador dentro del canal que prefieras, por ejemplo, mensajería u otra red social.

Generador de arrastrar y soltar fácil de usar

Al crea una landing page sin contratar a un desarrollador ni escribir una línea de código.

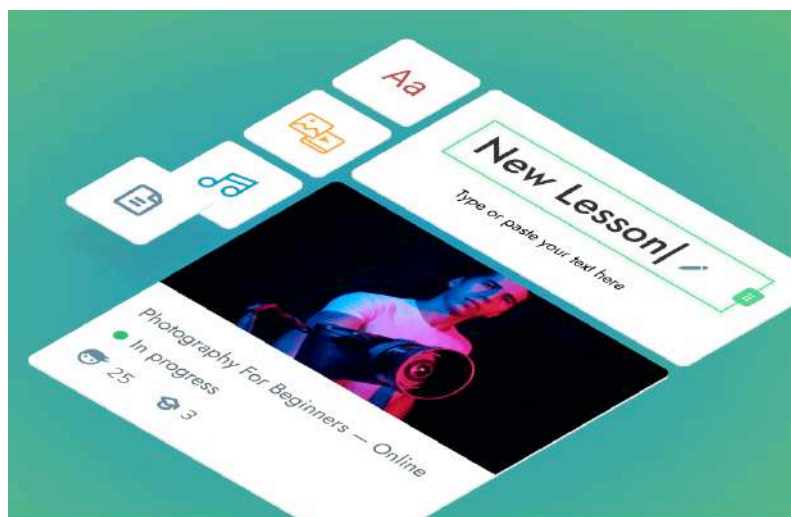
Herramientas e integraciones incorporadas

Para conectar el sistema de pago y pueda aceptar pagos de todo el mundo. Puede obtener la información de un visitante por medio de un formulario de suscripción y usar la información recolectada para enviar las ofertas relevantes.

SEO y analíticas

Para mejorar el puntaje en los buscadores usando herramientas de SEO basadas en información de Google Analytics.

- **Creador de Cursos Online**



Desarrollo de cursos en línea

Al crear cursos de capacitaciones originales sin tener experiencia técnica. Selecciona un el formato y el orden de la clase, el precio del curso, los criterios para la finalización y entrega certificados de finalización.

Monetización de conocimiento.

Para transforma todos los materiales del curso en productos digitales para comenzar a interactuar. Acepta pagos para el curso usando integraciones de métodos de pago populares.

Creador simple

Con el creador de cursos de arrastrar y soltar, pues crear la estructura del curso, añadiendo secciones, lecciones y exámenes. Usar instrucciones escritas, imágenes y audios y agregar clases pregrabadas para hacer las clases más atractivas y fáciles de entender.

Gestión completa

Crear pipelines, atrae nuevos participantes y permíteles registrarse a través de un formulario de suscripción. Administrar los contactos en CRM y usa otros servicios de SendPulse para mantener una comunicación efectiva con los usuarios.

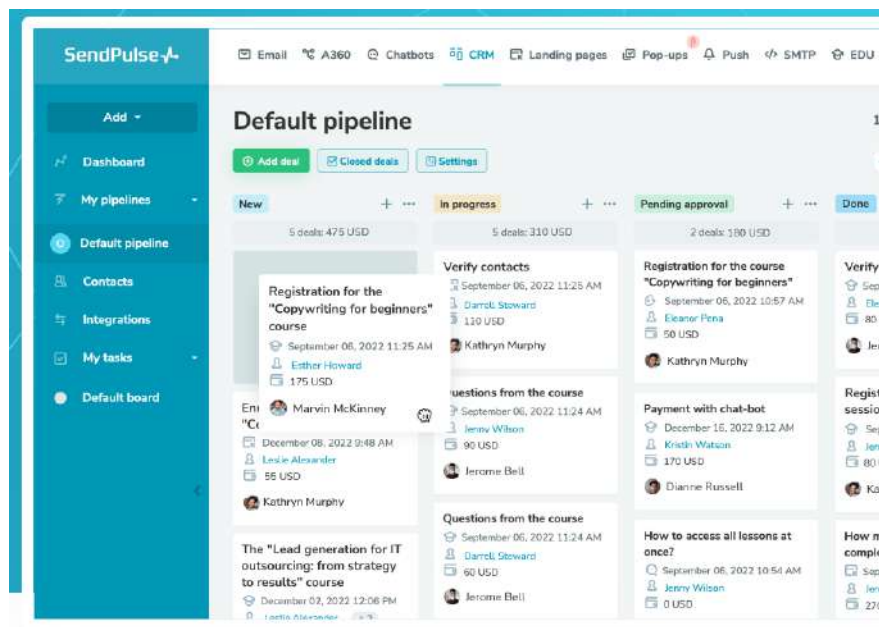
Comunicación por mensajes

Interactúa con los usuarios a través de distintos canales de comunicación como SMS y chatbots. Envía campañas de correo electrónico y notificaciones web push.

Formato conveniente de aprendizaje

Seguir el proceso de aprendizaje de los usuarios, apoyándolos en cada etapa del curso y respondiendo a sus preguntas.

- CRM



Canalizador de ventas

Manejar los flujos de trabajo en cada etapa de la canalización de ventas - crea tratos, agrega contactos y asigna miembros del equipo responsables.

Fácil comunicación con los clientes

Conecta con los usuarios directamente al abrir una tarjeta de contacto o trato. Envíarles un mensaje vía correo electrónico o Messenger.

Toda la información del cliente en un solo lugar

Crear tarjetas de contacto y actualizarla con nueva información. Agregar campos específicos a las tarjetas de contactos para poder llenarlas con notas y comentarios útiles para trabajar con los usuarios en un futuro.

Adición automática de tratos

Para configurar una adición automática de tratos cuando un contacto realiza una acción en específico en los flujos automáticos, chatbot, formulario de usuarios y otros canales.

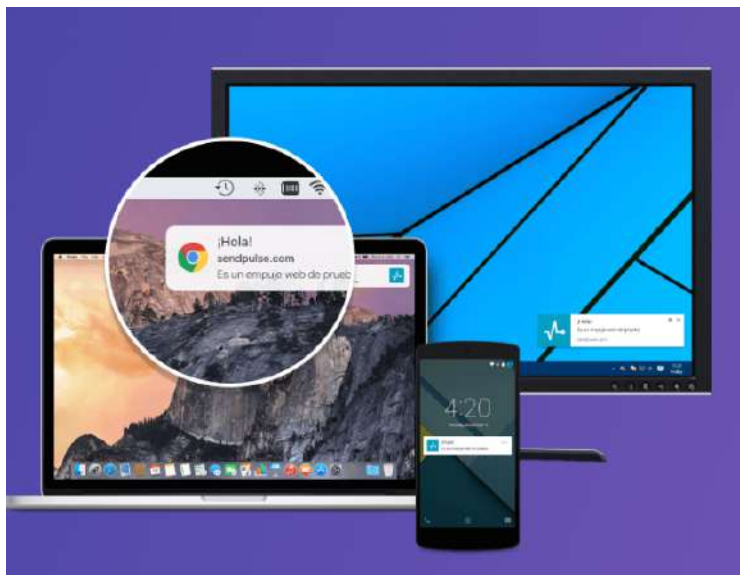
Trabajo en Equipo

Al ingresar a los usuarios al sistema de CRM para efectivamente colaborar en un proyecto juntos y distribuir la carga de trabajo entre diferentes miembros del equipo.

Integraciones

Vincular el CRM con otros servicios de SendPulse para unir las herramientas de marketing y ventas para poder cerrar los tratos con más efectividad.

- **Notificaciones Web Push**



Tasa alta de suscripción

Los visitantes visualizan las peticiones de los usuarios cuando están interesados en el sitio.

Flujos automatizados

Pueden configurar correos electrónicos, mensajes de chatbots, notificaciones web push y SMS basados en variables, eventos, y las acciones que los usuarios toman.

Personalización y segmentación

Añadir información personal de los destinatarios a las notificaciones push. Segmentar la lista acorde al lugar de residencia, fecha de suscripción, idioma, etc. para una comunicación más personal.

Notificaciones Offline

Los usuarios verán las notificaciones tan pronto estén en línea.

Mensajes accionadores y en grupo

Enviar notificaciones push a todos los usuarios o configurar mensajes automatizados cuando se encuentren condiciones específicas.

Desarrollador API

Usar el API SendPulse y enviar notificaciones web push, correos electrónicos y SMS por medio de una plataforma.

- **Servicio SMS**

The screenshot shows the 'New SMS Campaign' interface in the NEXSYS dashboard. The top navigation bar includes links for Email, Chatbots, CRM, Landing pages, Pop-ups, Push, SMTP, and EDU. The left sidebar contains various icons for campaign management. The main form area is titled 'New SMS Campaign' and includes the following fields: 'Sender' (set to 'HappyCoke'), 'Text SMS' (with a character count of 127/160), 'Recipients' (with an 'Add manually' dropdown), and a 'Send SMS' section with radio buttons for 'Immediately' (selected) and 'Start sending SMS at'. A green 'Send' button is at the bottom right. A 'PREVIEW' section on the right shows the message as it would appear on a mobile phone screen.

Alcance Global y entrega rápida

Enviar mensajes en cualquier elección a más de 1,000 operadoras móviles globalmente.

Nombre de Remitente

Para mejorar la percepción de la marca cuando envíes campañas SMS agregando un nombre de remitente para que los destinatarios puedan visualizar el nombre de la entidad en el campo de “SMS de”.

Automatización fácil de configurar

Los SMS en grupo pueden ser programados para enviarse en una hora y fecha en específico. También puedes configurar envío gradual de SMS en lapsos específicos de tiempo.

SMS Personalizados

Pueden agregar el nombre del destinatario y otra información personal a cada SMS: el nombre de la entidad, fecha de nacimiento, código de descuentos y otros.

Mensajes Accionadores y en grupo

Enviar campañas de SMS a todos los suscriptores o configura mensajes automatizados cuando se cumplan condiciones específicas.

Estadísticas

Evalúa los resultados de las campañas SMS al analizar las estadísticas de apertura y entrega de cada mensaje que envíes.

Integración API

Para usar el API para integrar envíos de SMS con la página web, aplicación, software o sistema CRM.

Auto respuestas de SMS

Llega a los consumidores en diferentes puntos de contacto implementando estrategias de marketing multicanal. Configura un flujo automatizado de mensajes con SMS, correos electrónicos, mensajes de chatbot y notificaciones web push.

Formularios de suscripción

Para crear formularios SMS de suscripción e intégralos a la página web. Puedes personalizar el tamaño, fondo, color de la letra, e incluso subir imágenes con el logo.

Links de Cancelar Suscripción

Incluye un link para cancelar la suscripción a los SMS y manteniendo una lista de contactos que no están interesados en las ofertas.

- **Mensajes de Viber**



Planificador

Para enviar mensajes al instante o posponlos para después usar el Planificador. El planificador mandará mensajes automáticamente sin necesidad de la intervención.

Duración de vida de Mensaje

El periodo de tiempo durante el cual el servicio intenta enviar un mensaje se llama “duración de vida de mensaje”. Pueden activar en caso de que el destinatario no haya estado disponible en la hora del envío.

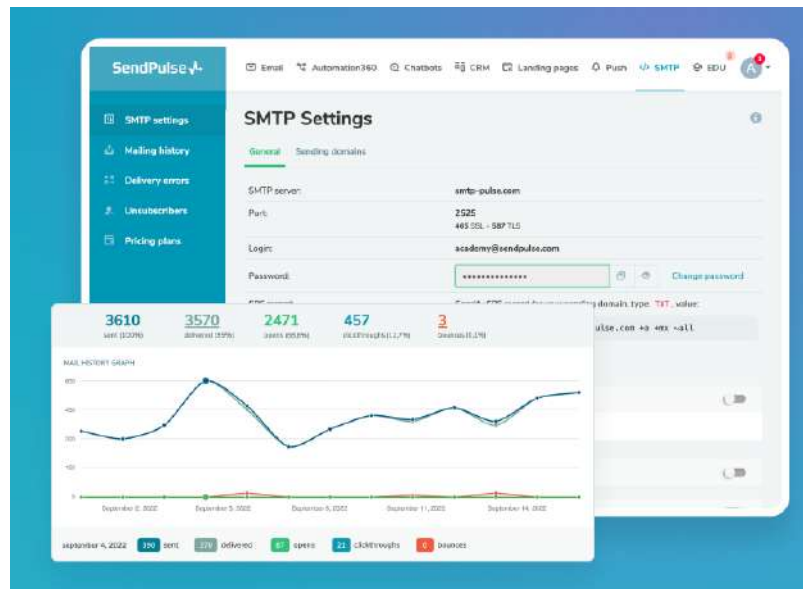
Reenvía mensajes no leídos por SMS

Si la duración de vida del mensaje enviado en Viber expira, el mensaje puede ser entregado vía SMS. Para hacer esto necesita activar la función “Reenviar mensajes no leídos por SMS”.

1,000 caracteres

De ahora en adelante no se limitará la longitud del texto. No se necesita pensar en cómo escribir un mensaje de 140 caracteres, como es en el caso de SMS.

- **Servicio SMTP**



Direcciones IP Dedicadas

Usar una dirección IP dedicada para incrementar la reputación del remitente y evitar una lista negra por acciones de alguien más.

Registros SPF y DKIM

Para demostrar que es la entidad y dominio propio al mandar mensajes, y minimiza la cantidad de mensajes que puedan ser marcados como spam al usar las firmas criptográficas especiales SPF y DKIM.

Alta velocidad de envío

No se necesita esperar mucho tiempo al enviar correos electrónicos. Usar el SMTP para enviar altos volúmenes de correos a las suscriptores en tiempo.

Estadísticas

Para cada lista de correo pueden descubrir el número de mensajes que se enviaron, el número de conversiones hechas y los enlaces abiertos, entre otros detalles.

Reportes

El servicio genera reportes de envío y reportes de falla de entrega, todos los reportes pueden ser descargados a la computadora.

Lista de no suscritos

Los correos electrónicos no podrán ser enviados a ninguna de las direcciones de la lista de destinatarios que han dejado de suscribirse, incluso si están en alguna lista de mensajería.

INFRAESTRUCTURA DE SEGURIDAD DE LA PLATAFORMA SENDPULSE

En SendPulse, valoramos mucho la confianza de los usuarios y nos esforzamos por proteger los datos confidenciales de la entidad con el mismo cuidado que los nuestros. El equipo trabaja constantemente para mejorar las funciones de protección para mantener los datos seguros frente a posibles amenazas en línea y hacer que sea seguro de que la información personal permanece bien protegida.

Los programa de seguridad es completamente de código abierto, por lo que puedes comprender cómo funciona y utilizar los productos y servicios de manera confiada.

Las principales prácticas de seguridad

Implementación de mecanismos actualizados de protección de cuentas

Autenticación de dos factores

La seguridad de la información personal depende de cuán vulnerable sea la cuenta a los ataques de piratas informáticos profesionales. Dado que las contraseñas a menudo pueden verse comprometidas, introdujimos la verificación de usuario en dos pasos. Además de ingresar el nombre y contraseña al acceder a la cuenta, también deberás ingresar un código único que puedes obtener por correo electrónico.

El método de autenticación de dos factores puede advertirte sobre un posible intento de robo de datos y recibir acceso no autorizado a la cuenta mediante el envío de un correo electrónico.

Restricciones de acceso a la dirección IPs

Esta característica protegerá la cuenta, especialmente si usas solo computadoras del trabajo o del hogar con direcciones IP estáticas. Después de cada autorización, recibirás un correo electrónico con la hora de inicio de sesión y los detalles de la dirección IP. Esto ayudará a proteger los datos en caso de que terceros intenten iniciar sesión en la cuenta sin acceso a la red local.

Límites de envío de correos electrónicos SMTP

El propósito principal de los servidores SMTP es enviar, recibir y retransmitir correos electrónicos. Con el servicio SMTP puedes enviar correos automatizados y transaccionales desde cualquier lugar.

Para evitar el envío de correos no autorizados en el nombre, en caso de pérdida o robo de la contraseña SMTP, se introduce limitaciones de dirección IP del remitente.

Mecanismos reCAPTCHA

Esencialmente, este es un método de protección contra bots que se utiliza para detectar el acceso automatizado a sitios web y prevenir ataques de bots.

Cada vez que las acciones de los usuarios parecen sospechosas, se les pide que realicen una prueba de reconocimiento de imágenes o ingresen una cierta combinación de letras y números que solo las personas pueden identificar.

Alertas de inicio de sesión sospechosas

Este procedimiento de seguridad ayudará a mejorar la seguridad general de la cuenta. El inicio de sesión se evitará automáticamente y se te notificará cada vez que se realice un intento de inicio de sesión desde un dispositivo o navegador sospechoso.

Gestión de vulnerabilidades

Trabajamos constantemente para garantizar la máxima seguridad y privacidad. Implementamos procesos de remediación automatizados y manuales para mitigar las posibles vulnerabilidades de la plataforma. Con este propósito, lanzamos el Open Bug Bounty, donde los usuarios que encontraron errores de seguridad en los servicios pueden recibir una recompensa económica.

Protección de datos de pago

SendPulse solo funciona con sistemas de pago certificados. No almacenamos los datos de la tarjeta de crédito del cliente. Todos los puntos de datos se envían directamente al sistema de pago seleccionado de conformidad con todas las medidas de seguridad según el protocolo de encriptación de datos SSL.

Disponibilidad del servicio

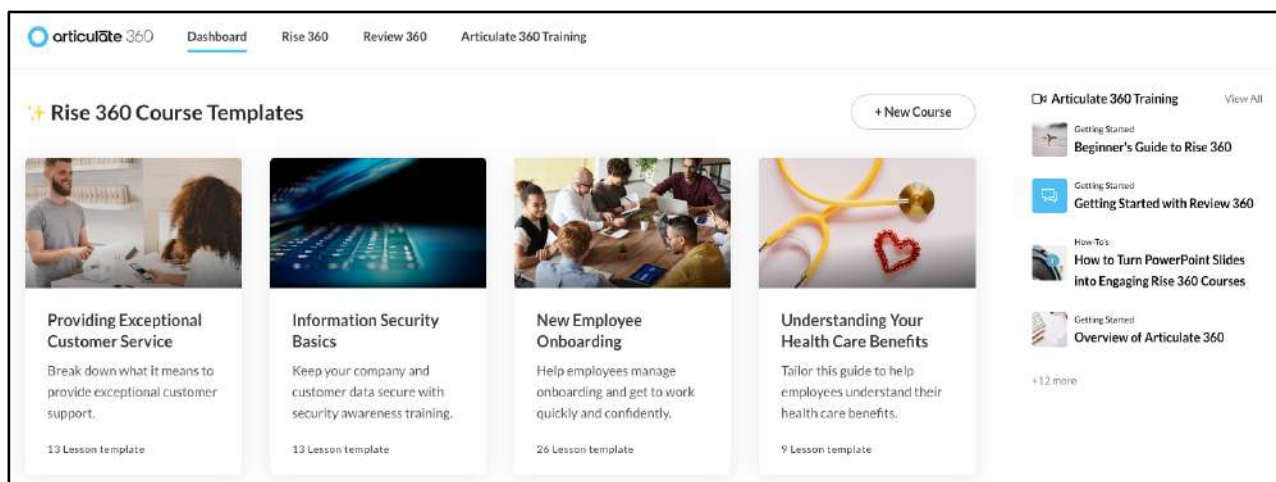
Los servidores de bases de datos operan diariamente con redundancia total de todos los recursos. Estas copias de seguridad se utilizan para evitar la pérdida de datos y recuperar la información del sistema rápidamente.

6. Software de creación de contenidos web (Articulate 360)

LA INFRAESTRUCTURA TECNOLÓGICA DEL SOFTWARE ARTICULATE 360

Es una herramienta de creación de contenidos web Articulate 360 para uso educativo, que permita elaborar, instructivos webs, material didáctico y en general, estructuras organizadas de contenido dispuestas para los usuarios.

Asimismo, que apoye el desarrollo de proyectos con interactividad básica, compartir enlaces con los revisores y obtener comentarios, perfeccionamiento de videos, usar imágenes y plantillas de la biblioteca de contenido, capacitación en diseño de instrucción y transformar presentaciones de PowerPoint en aprendizaje electrónico interactivo.



Es una anualidad que permite tener acceso a un usuario a todas las herramientas de autoría creadas por Articulate, teniendo la posibilidad de comprar y vincularlas con otras cuentas para crear un TEAMS (equipo de trabajo), las herramientas que incluye son: Storyline 360, Studio 360, Rise, Preso, Peek, Replay 360, Content Library, Articulate Review y Articulate Live.

*Articulate TEAMS también incluye espacio ilimitado en Articulate Review y capacidad de administrar las cuentas del TEAMS

Número de suscripción: 1145921

Número de usuarios: 3 usuarios adquiridos

Son contratadas 3 suscripciones profesionales para creación de contenido del software Articulate 360.

Requisito:

Es necesario que los usuarios que van a usar la suscripción generen un Articulate ID para que los puedas invitar a formar parte del equipo y se les habiliten las herramientas.

Articulate ID

Es un inicio de sesión único para todo lo relacionado con Articulate. Articulate ID permite acceder a Articulate 360, descargar software, participar en discusiones de E-Learning Heroes; este tipo de cuenta permite administrar los servicios automatizados, incluidas las suscripciones.

Para crear el ID de Articulate: [Ingresa a este enlace](#). Una vez se finalice el registro llegara una solicitud de autenticación en la dirección de correo electrónico

Servicio Articulate	ID Articulate
Articulate 360	✓
Descargas de software	✓
Héroes e-learning	✓
Tienda Articulate	Suscripciones a Articulate 360

**El Articulate ID es intransferible y no debe compartirse con nadie.*

Articulate 360 Teams: Roles y permisos

Descripción de los roles

Existen cuatro tipos de roles en una cuenta de equipos Articulate 360.

1. Propietario de la cuenta

El propietario de la cuenta es la persona que compró la suscripción y es el responsable de administrar la facturación. El propietario de la cuenta es el único que puede comprar más suscripciones para los usuarios.

El propietario de la cuenta también es un administrador de cuenta, por lo que puede administrar todos los usuarios, grupos y administradores.

Puede que el propietario de la cuenta no tenga una suscripción de forma predeterminada. Si el propietario de la cuenta necesita crear cursos en línea, se debe asignar a una suscripción para usar las aplicaciones de Articulate 360.

Este es un usuario con el rol de propietario de la cuenta.

SENA (SUB-1145921) ▾

Subscripción por equipo / Renueva Aug 26, 2024

Revendedor autorizado: mfernandez@taec.com.mx

Equipo

Administradores

Administrar, agregar o quitar administradores de tu suscripción de equipo.

#	Nombre	Estado	Grupo
1	LINA Alvarez (lina.alvarez@pcmac.co)	✓	Administrador de la cuenta

2. Administrador de la cuenta

El administrador de cuenta gestiona todos los usuarios, grupos y administradore, no puede tomar decisiones de compras, pero puede pedir al propietario de la cuenta que compre más suscripciones a medida que aumenta la demanda de usuarios.

Los administradores no utilizan suscripciones (de forma predeterminada), por lo que se pueden agregar los administradores que sean requeridos. Sin embargo, si los administradores necesitan gestionar el equipo y crear cursos de aprendizaje en línea, puede asignar suscripciones para que puedan utilizar las aplicaciones de Articulate 360.

Estos son los usuarios con el rol de administrador de la cuenta

SENA (SUB-1145921) ▾

Subscripción por equipo / Renueva Aug 26, 2024

Revendedor autorizado: mfernandez@taec.com.mx

Equipo

Administradores

Administrar, agregar o quitar administradores de tu suscripción de equipo.

Comprar más puestos

#	Nombre	Estado	Grupo
1	LINA Alvarez (lina.alvarez@pcmac.co)	✓	Administrador de la cuenta
2	Lina Alvarez (notificacionesadobe@sena.edu.co)	✓	Administrador de la cuenta
3	John Ricardo Calderón Quiroga (jrcalderon@sena.edu.co)	✓	Administrador de la cuenta

Administrador de grupo

Los administradores de grupo gestionan a los usuarios en los grupos de los que son responsables. No pueden ver ni administrar otros grupos o administradores en la consola de administración de cuenta.

Los administradores de grupo no pueden tomar decisiones de compras, pero puede pedir al propietario de la cuenta que compre más suscripciones a medida que aumenta la demanda de usuarios.

Los administradores no utilizan espacios de usuario (de forma predeterminada), por lo que se pueden agregar los administradores de grupo que sean requeridos. Si los administradores necesitan gestionar el equipo y crear cursos de aprendizaje en línea, puede asignar suscripciones para que puedan utilizar las aplicaciones de Articulate 360.

Usuario

Tienen acceso a las aplicaciones de Articulate 360, como Storyline 360 y Rise 360. Los usuarios crean cursos de aprendizaje en línea y colaboran en proyectos.

SENA (SUB-1145921) ▾

Subscripción por equipo / Renueva Aug 26, 2024

Revendedor autorizado: mfernandez@taec.com.mx

Equipo

Administradores

Q

Buscar miembros o grupos

Nuevo grupo

Tu equipo incluye 3 licencias. Asignaste 3 licencias.

¿Necesita invitar a muchos miembros del equipo? [Suba un archivo CSV](#) para agregarlos rápidamente.

¿Necesitas una copia con los detalles de tus licencias? [Descarga el CSV](#).

Sin grupo

#	Nombre	Estado
1	Carlos Ramirez (carlosj.ramirez@misena.edu.co)	✓
2	Edward Leonardo Pico Carba (edward.picoc@misena.edu.co)	✓
3	Zuleidy Maria Ruiz Torres (zmruiz@misena.edu.co)	✓

Las suscripciones estarán a la disposición del área de Formación Profesional para dar acceso a los usuarios que requieran hacer uso de las herramientas y funciones incluidas en Articulate 360.

Tarea	Propietario de la cuenta	Administrador de la cuenta	Administrador de grupo	Usuario
Utiliza las aplicaciones de Articulate 360 para crear cursos de aprendizaje en línea y colaborar en los proyectos.				✓
Agrega usuarios al equipo	✓	✓	✓	
Importa usuarios en forma masiva a través de un archivo CSV	✓	✓		
Eliminar usuarios	✓	✓	✓	
Crea grupos de espacios de usuario	✓	✓		
Cambia el nombre de los grupos	✓	✓		
Agrega espacios a los grupos	✓	✓		
Agrega usuarios a los grupos	✓	✓	✓	
Mueve espacios entre grupos	✓	✓	✓	
Quita usuarios del equipo	✓	✓	✓	
Elimina espacios de los grupos	✓	✓		
Elimina grupos	✓	✓		
Agrega administradores	✓	✓		
Edita los permisos del administrador	✓	✓		
Asigna grupos a los administradores	✓	✓		
Elimina administradores	✓	✓		
Elige un nombre para el equipo	✓			
Cambia el nombre del equipo	✓	✓		
Cambia de equipos	✓	✓	✓	
Posee o administra varios equipos	✓	✓	✓	
Toma decisiones de compras, como comprar más espacios de usuario para el equipo	✓			

Transferencia de la propiedad de la cuenta

Las suscripciones de Articulate 360 Teams pueden tener varios administradores, pero solo un propietario de la cuenta. El propietario es la única persona que tiene acceso a la administración de facturación.

No puedes transferir propiedad de la cuenta a otra persona en la consola de administración de la cuenta, pero podemos ayudarte con eso solicitando un soporte de nombre Priorizado.

REQUISITOS DEL SISTEMA

Estos son los requisitos mínimos del sistema para crear y ver los cursos de Articulate.

Hardware para la creación de cursos

CPU:	Procesador de 2 GHz o superior (32 o 64 bits)
Memoria:	2 GB como mínimo
Espacio en disco disponible:	1 GB como mínimo
Display:	Resolución de pantalla de 1280 x 800 o superior
Multimedia:	Tarjeta de sonido, micrófono y cámara web para grabar narraciones y video

Software para la creación de cursos

Sistema operativo:	Windows 11 (32 o 64 bits) Windows 10 (versiones estándar compatibles de 32 o 64 bits) Mac OS X (versión más reciente de los procesadores Intel) con Parallels Desktop (versión más reciente) o VMware Fusion (versión más reciente)
Tiempo de ejecución de .NET:	Microsoft .NET Framework 4.8 o posterior (se instala si no está presente)
Visual C++:	Microsoft Visual C++ 2019 Redistributable (versión más reciente, se instala si no está presente)

Compatibilidad e integraciones

Compatibilidad con versiones anteriores

Los proyectos de Storyline 2 se pueden actualizar a Storyline 3, pero los proyectos de Storyline 3 no se pueden abrir ni editar con Storyline 2.

Los proyectos de Storyline 3 y Storyline 360 se pueden abrir indistintamente, excepto cuando un archivo de proyecto de Storyline 360 tiene funciones que son exclusivas de Storyline 360. Detalles aquí.

Importación de contenido

Microsoft Office 365 (solo aplicaciones de escritorio) o la versión perpetua más reciente de Microsoft PowerPoint (32 o 64 bits)

Usuarios de Mac: las aplicaciones de Office deben estar instaladas en su entorno de Windows.

No hay requisitos para importar contenido de Presenter y Quizmaker.

Para importar las interacciones de Engage, Studio 360 debe estar instalado con una suscripción activa a Articulate 360.

Publicar en Word

Microsoft Office 365 (solo aplicaciones de escritorio) o la versión perpetua más reciente de Microsoft Word (32 o 64 bits)

Traducción

Microsoft Office 365 (solo aplicaciones de escritorio) o la versión perpetua más reciente de Microsoft Word (32 o 64 bits)

Navegadores y aplicaciones móviles para ver los cursos publicados

Windows

Microsoft Edge (última versión), Google Chrome (última versión), Firefox (última versión)

Mac

Safari (última versión), Google Chrome (última versión), Firefox (última versión)

Móvil

Safari en Apple iOS/iPadOS (última versión), Google Chrome (última versión) en Apple iOS/iPadOS (última versión), Google Chrome (última versión) en Android OS 6 o posterior

Configuración de navegador requerida para ver los cursos publicados

JavaScript

JavaScript debe estar activado para que los cursos publicados funcionen.

Descargas de fuentes

Las descargas de fuentes deben estar habilitadas para ver las fuentes y los personajes correctos.

Accesibilidad en los cursos publicados

La salida de Storyline 3 es compatible con los siguientes lectores de pantalla, además de las Pautas de accesibilidad al contenido web (WCAG) 2.1 de nivel AA y las normas revisadas de Consulte la [Plantilla voluntaria de accesibilidad de productos®](#) (VPAT®) para obtener más información.

SOPORTE TÉCNICO

Standard:

Por correo electrónico.

Gratuito en la compra de cualquier licencia o anualidad de Articulate. Sin garantía en el tiempo de respuesta.

Priorizado:

Por correo electrónico.

Incluido cuando se adquiere Articulate 360 TEAM. Se pueden adquirir paquetes de horas de soporte personalizado con un costo adicional.

Chats en vivo

Ofrecemos soporte técnico de chat en vivo las 24 horas del día de lunes a viernes (hora estándar del este), excepto festivos estadounidenses, para cualquier persona con una suscripción a Articulate 360 Teams.

El soporte técnico de chat en vivo se incluye con tu suscripción a Articulate 360 Teams. [Haz clic aquí para iniciar el chatear.](#)

Extra: Los suscriptores de Articulate 360 Teams obtienen tiempos de respuesta prioritarios.

Soporte técnico por correo electrónico 24 horas al día, 7 días a la semana

Obtén soporte técnico personal de nuestro equipo por correo electrónico las 24 horas al día, 7 días a la semana. Envía un caso y responderemos de inmediato. El soporte técnico por correo electrónico nos permite realizar un seguimiento de tu historial de caso y, con tu autorización, incluso podemos probar tus archivos de proyecto para resolver el problema con mayor rapidez. Guardamos tu información en privado y eliminamos los archivos que enviarás en cuanto terminemos de solucionar los problemas.

Correo electrónico: soporte@taec.com.mx

Extra: Los suscriptores de Articulate 360 Teams obtienen tiempos de respuesta prioritarios.

Servicios de soporte de Articulado 360

Términos y condiciones para Articulate 360 y Articulate 360 para equipos

Estamos aquí para ayudar. Y lo tenemos cubierto con servicios de soporte para Articulate 360 y Articulate 360 para Teams. (Los términos y condiciones que se describen a continuación se aplican a ambos planes de suscripción a menos que se indique lo contrario).

Es posible que actualicemos este documento de vez en cuando en la búsqueda para brindar un soporte superior.

1. Definiciones

El **software** se refiere a todos los productos de Articulate incluidos con su suscripción a Articulate 360.

El soporte de productos es nuestro centro de soporte en línea en <https://support.articulate.com> (o el sitio sucesor), que incluye artículos de la base de conocimientos, requisitos del sistema, notas de la versión, descargas de productos y la información de contacto.

El soporte de la comunidad es soporte de fuentes múltiples en <https://community.articulate.com> (o sitio sucesor). Los miembros de la comunidad de todo el mundo participan en los debates del foro y envían ejemplos y descargas. Nuestro personal publica regularmente artículos, tutoriales, guías de usuario de productos y libros electrónicos.

El soporte por correo electrónico es soporte técnico a través de comunicación por correo electrónico en support@articulate.com (o dirección sucesora).

El chat en vivo es una interacción en tiempo real basada en texto con nuestro útil personal de soporte a través de una interfaz de chat en línea.

El soporte de nivel 1 es soporte básico para ID de Articulate, problemas de inicio de sesión, activaciones de licencias y preguntas generales sobre la instalación de software.

El soporte de nivel 2 es un soporte profundo y amplio para todas las funciones de Articulate 360, así como escalaciones desde el soporte de nivel 1.

El soporte de nivel 3 es soporte especializado para desafíos técnicos únicos, entornos de instalación inusuales, errores poco comunes y escalaciones del soporte de nivel 2.

2. Versiones de software admitidas

Se admitimos la versión más reciente del software Articulate 360.

3. Elementos cubiertos por los servicios de soporte de Articulate 360

Se brinda el soporte de productos y soporte comunitario para problemas técnicos y de uso durante su período de prueba gratuito y durante la duración de su suscripción a Articulate 360.

Es posible que no brindemos soporte a ningún cliente que no cumpla con los Términos de servicio generales de Articulate 360 (u otro acuerdo que cubra Articulate 360).

4. Elementos no cubiertos por los servicios de soporte de Articulate 360

No se proporciona soporte de productos para los siguientes temas. Sin embargo, el apoyo de la comunidad puede brindar orientación.

- Curso o diseño instruccional
- Modificación de la salida publicada
- Modificación de los tiempos de ejecución de los jugadores
- Modificación o ingeniería inversa de los archivos del reproductor
- Modificación de HTML personalizado o integración con otro contenido web
- Integración personalizada del sistema de gestión de aprendizaje (LMS)
- Productos de terceros, como LMS, sistemas de administración de contenido de aprendizaje (LCMS) y aplicaciones móviles
- Kits de desarrollo de software (SDK)
- Desarrollo o modificación de Flash personalizado
- Compatibilidad con ActionScript para películas Flash

- Codificación JSON para declaraciones xAPI personalizadas
- Codificación JavaScript
- Paquetes de instalación personalizados
- Instalaciones no locales
- Hardware o sistemas incompatibles con las especificaciones técnicas

Los errores del usuario, problemas que no se puede reproducir y hardware/software de terceros no tiene alcance sobre el soporte brindado.

Articulate no tendrá ninguna obligación de proporcionar servicios de soporte con respecto a: (a) problemas de soporte que surjan o estén relacionados con el incumplimiento de los Términos de servicio de Articulate 360; (b) problemas de soporte que están fuera del control de Articulate; (c) solicitudes de mejoras; (d) cualquier problema de soporte que sea responsabilidad del cliente, como se establece en los Términos de servicio de Articulate 360; o (e) problemas de asistencia técnica que surjan de cualquier función, programa, dispositivo o datos no proporcionados por Articulate.

5. Obligaciones del Cliente

Para reproducir, diagnosticar y solucionar un problema, cuando se solicite soporte (es decir, se envíe un caso de soporte), se puede solicitar que incluya en la solicitud de soporte:

- El nombre de la organización y la información del contacto
- Identificación de Articulate
- El número de compilación de su software Articulate 360
- La plataforma en la que se ejecuta Articulate 360
- Una descripción razonablemente detallada del incidente o solicitud.
- Mensajes de error u otras notificaciones generadas por el sistema
- Registros y archivos de rastreo aplicables
- Un caso de prueba o instrucciones para demostrar el problema

El lenguaje abusivo o amenazante resultará en la denegación de los servicios de apoyo, sin ninguna obligación adicional para el cliente.

La obligación de Articulate de brindar servicios de soporte está condicionada a que el cliente: (a) pague todas las tarifas correspondientes a Articulate a su vencimiento; (b) tener acceso válido a los Servicios; (c) proporcionar a Articulate toda la asistencia razonable y proporcionar a Articulate datos, información y materiales que sean razonablemente necesarios; (d) adquirir, instalar y mantener todos los equipos, líneas telefónicas, interfaces de comunicación y otro hardware y software necesarios para acceder a los Servicios; y (e) proporcionar información de contacto adecuada para todos los contactos de soporte autorizados.

6. Métodos de contacto

Puede solicitar soporte utilizando cualquiera de estos métodos:

Formulario de envío de casos de soporte: <https://articulate.com/support/contact/case>

Foro Comunitario: <https://community.articulate.com/discuss>

Correo electrónico: support@articulate.com

Chat en vivo: El chat en vivo se proporciona con las suscripciones de Articulate 360 for Teams.

7. Disponibilidad de soporte

Estos son los horarios de soporte programados:

Soporte de nivel 1: 24 horas al día, 7 días a la semana, excepto festivos

Soporte de nivel 2: 10:00 p. m. del domingo a 10:00 p. m. del viernes, hora del este de EE. UU., excepto los feriados observados en EE. UU.

Soporte de nivel 3: De 9:00 a. m. a 5:00 p. m., hora del este de EE. UU., de lunes a viernes, excepto los feriados observados en EE. UU.

8. Tiempos de respuesta

La calificación de la gravedad de cada problema que informa y se establece los siguientes tiempos de respuesta:

Gravedad	Criterios	Tiempo de respuesta inicial objetivo
Crítico	Un problema se considera crítico cuando tiene un impacto comercial significativo en un sistema de producción, lo que provoca que todos los sistemas de producción estén inactivos o funcionen a una capacidad reducida.	1 hora
Alto	A un problema se le asigna una gravedad alta cuando tiene algún impacto comercial en un sistema de producción, lo que resulta en alguna pérdida de funcionalidad en los sistemas de producción. Articulate 360 generalmente se puede usar, pero no proporciona una función particular de la manera más conveniente o rápida.	24 horas
Medio	A un problema se le asigna una gravedad media cuando se trata de preguntas que no son de producción, como preguntas de uso general y solicitudes de funciones. No hay impacto en la calidad, el rendimiento o la funcionalidad de un sistema de producción.	48 horas

9. Matriz de escalamiento

Un caso de soporte critico se escala de esta manera:

Nivel de escalamiento	Socio de escalada	Activar escalamiento cuando está abierto
1er nivel	Líder del equipo de soporte en servicio	> 4 Horas
2do Nivel	Director de Soporte Técnico	> 1 Día
3er Nivel	Director Técnico	> 2 Días

10. Plazo y rescisión

El soporte está cubierto durante el periodo que se haya contratado Articulate 360 Teams

INFRAESTRUCTURA DE SEGURIDAD DEL SOFTWARE ARTICULATE 360

Cifrado

Se aplica la tecnología de cifrado más avanzada disponible públicamente para proteger los datos. Uso de TLS de 256 bits/ Cifrado SSL y cifrado RSA mínimo de 2048 bits, Articulate cifra los datos en reposo y el tráfico de red, incluso en las páginas de pago, dentro y fuera de Amazon Web Services (AWS).

Política de contratación

Se tiene un riguroso proceso de contratación, que requiere una verificación completa de antecedentes, para garantizar que cualquier persona que sea contratada pueda realizar su función laboral. Se realizan capacitaciones internas cuando es necesario. El personal trabaja en estrecha colaboración entre sí en cuadrillas y equipos, dejando a ningún empleado solo con conocimiento confidencial y crítico.

Hosting

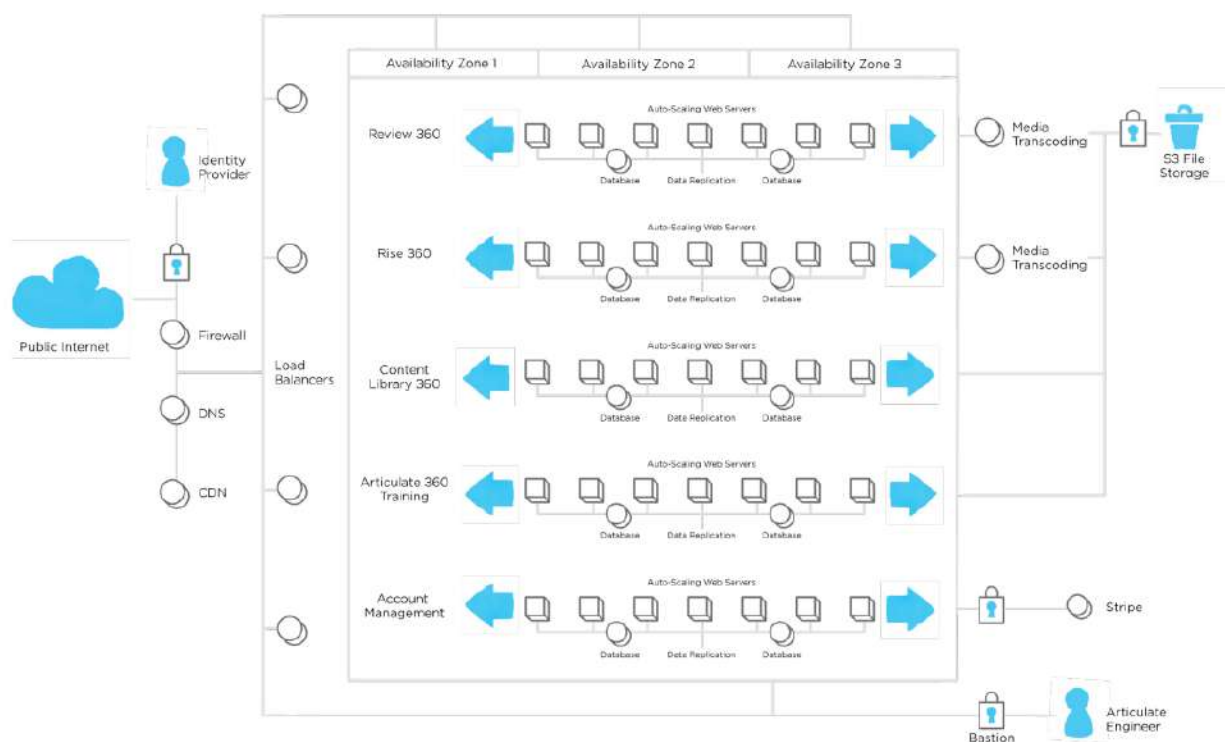
Los servicios de Articulate se encuentran alojados en servidores de AWS en la región us-east-1 ubicada en el norte de Virginia en el Estados Unidos. Los centros de datos de AWS son de última generación y utilizan arquitectura e ingeniería innovadoras. enfoques. Amazon tiene muchos años de experiencia en el diseño, construcción y operación a gran escala centros de datos. Esta experiencia se ha aplicado a la plataforma e infraestructura de AWS. Los centros de datos de AWS están alojados en instalaciones anodinas, y el acceso físico está estrictamente controlado tanto en el perímetro como en puntos de entrada de edificios por parte de personal de seguridad profesional que utiliza vigilancia por video, sistemas de detección de intrusos, y otros medios electrónicos. El personal autorizado debe pasar la autenticación de dos factores un mínimo de dos veces para acceder a los pisos del centro de datos. Se requiere que todos los visitantes y contratistas presenten una identificación y estén firmados y escoltados continuamente por personal autorizado.

AWS solo brinda acceso e información al centro de datos a empleados y contratistas que tienen un necesidad empresarial de tales privilegios. Cuando un empleado ya no tiene una necesidad comercial de estos privilegios, el acceso se revoca inmediatamente, incluso si esa persona continúa siendo un empleado de Amazon o AWS. Todo el acceso físico a los centros de datos por parte de los empleados de AWS se registra y audita de forma rutinaria.

Cuando un dispositivo de almacenamiento llega al final de su vida útil, los procedimientos de AWS incluyen una desactivación proceso que está diseñado para evitar que los datos del cliente estén expuestos a personas no autorizadas.

AWS utiliza las técnicas detalladas en DoD 5220.22-M ("Programa Nacional de Seguridad Industrial Manual de funcionamiento") o NIST 800-88 ("Pautas para la desinfección de medios") para destruir datos como parte del proceso de desmantelamiento. Todos los dispositivos de almacenamiento magnético fuera de servicio están desmagnetizados y físicamente destruido de acuerdo con las prácticas estándar de la industria.

Utiliza muchas soluciones proporcionadas por AWS, incluidas bases de datos relacionales, búsqueda de texto completo, colas, mensajería, gestión de identidad, cifrado y almacenamiento en caché. El objetivo es eliminar los puntos únicos de falla en la infraestructura y se tiene redundancia integrada en todos los servicios. Todos los servicios de Articulate son redundantes en tres (3) o más zonas de disponibilidad físicamente aisladas e independientes de los recursos en el norte de Virginia. Eso garantiza que varios centros de datos puedan desconectarse simultáneamente mientras se continúa brindando a los clientes una excelente experiencia. Así es como los servidores están estructurados dentro de la infraestructura de AWS:



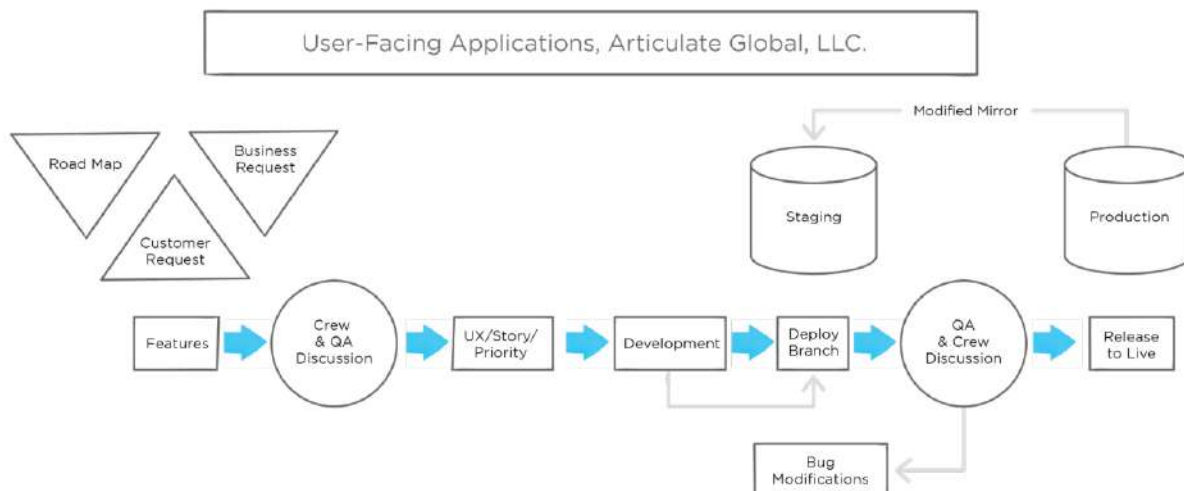
Se usa AWS CloudFront para servir contenido de manera eficiente a nivel mundial. CloudFront tiene numerosas ubicaciones alrededor el mundo, lo que permite acelerar el acceso de los usuarios al contenido, como los activos del curso (imágenes, videos, audio), logotipos, personajes y plantillas de curso.

NOTA: Para garantizar el acceso a los servicios esenciales de Articulate, asegúrese de incluir en la lista blanca los terminales necesarios, especialmente si se conecta a través de un proxy.

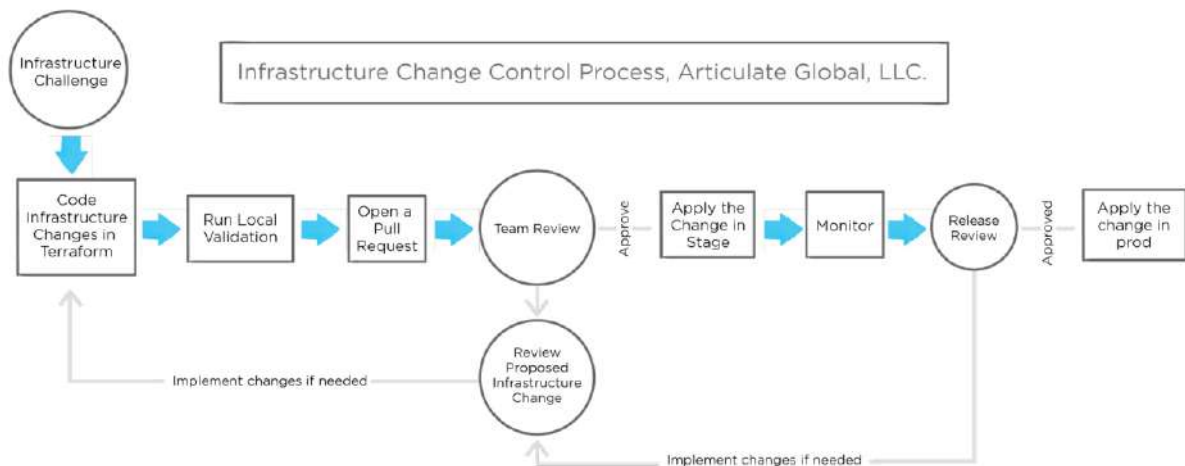
Ingeniería y Garantía de Calidad (QA)

El software es desarrollado internamente utilizando GitHub como repositorio de código fuente. El equipo desarrolla software y lleva a cabo revisiones de código en repositorios locales mediante solicitudes de incorporación de cambios. Los desarrolladores publican en las sucursales protegidas para control de calidad y partes interesadas del negocio para probar.

Proceso del ciclo de vida del desarrollo de software (SDLC):



El proceso formal en el que se actualiza los sistemas y software es el siguiente:



Autenticación de usuario

Se implementan las mejores prácticas para autenticar a los usuarios que inician sesión en los sitios y servicios. Cuando un usuario se registra para un ID de Articulate, proporcionan su dirección de correo electrónico o un administrador del equipo envía una invitación al usuario dirección de correo electrónico.

Articulate no almacena las credenciales de los usuarios. Confiamos en un servicio de terceros, Okta, como la autenticación proveedor. Okta implementa protocolos de identidad probados, comunes y populares que se utilizan tanto en entornos orientados al consumidor productos web e infraestructuras de identidad empresarial.

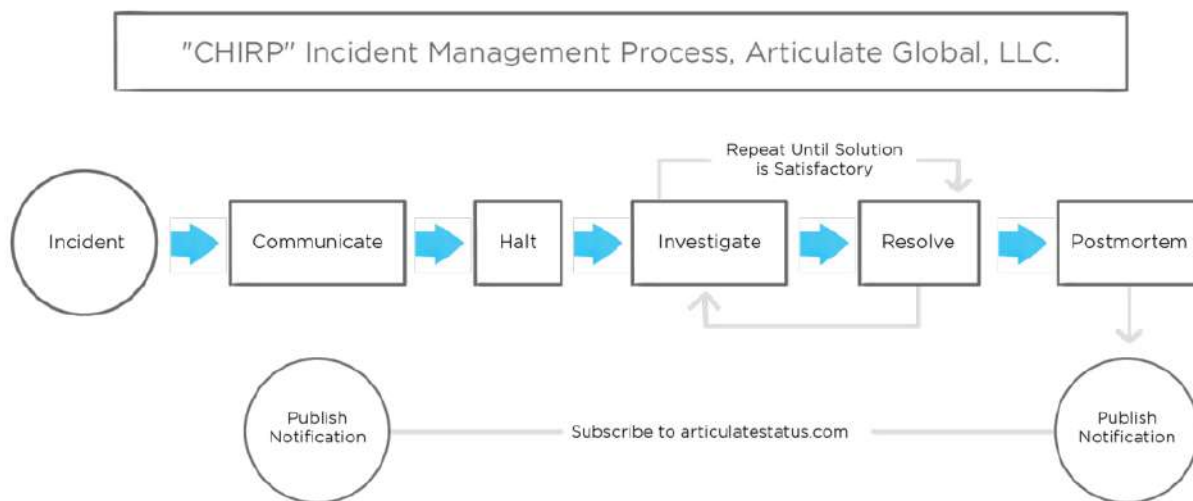
Las credenciales de Articulate ID se pasan a Okta para la autenticación y Okta regresa a JWT. El usuario crea un contraseña inicial y ese proceso requiere que el usuario tenga acceso a su cuenta de correo electrónico

El tráfico entre los clientes y la puerta de enlace API (Kong) y entre la puerta de enlace API y Okta es todo TLS 1.2 cifrado (estándar de la industria). Okta utiliza el cifrado AWS EBS en reposo (AES-256). Cuando usamos credenciales proporcionada por Okta para autorizar el acceso a las API de Articulate 360, las credenciales se verifican criptográficamente en la capa de puerta de enlace de la API antes de que las solicitudes pasen a las API de Articulate 360. En Okta, las contraseñas se codifican (y saltan) de forma segura mediante bcrypt.

Recuperación de Desastres y Gestión de Incidencias

El personal está preparado para responder a cualquier emergencia o interrupción. Se tiene un proceso simple para asegurar la comunicación con cualquier persona afectada y hacer todo lo posible para evitar que los incidentes vuelvan a ocurrir.

Este diagrama muestra el enfoque de respuesta con más detalle:



Protocolos de cumplimiento de la industria de tarjetas de pago (PCI).

Colaboración

El equipo de Articulate ofrecen funciones de colaboración y otras herramientas integradas que le permiten compartir su contenido a través del software Articulate. En función de la naturaleza colaborativa del software Articulate y en función de los permisos y la configuración que elija, el uso de dichas funciones permite compartir contenido con personas con las que quieran colaborar o con el público.

Atentamente,



Yesid Mauricio Castillo
Business Manager Adobe
ETLA Nexsys de Colombia



Lina Alvarez
Directora de Proyecto SENA
Pc Mac Servicios Y Ventas S.A

Acta 009 - Infraestructura Tecnologica

Informe de auditoría final

2023-03-16

Fecha de creación:	2023-03-15
Por:	lina alvarez (linalvarezh@gmail.com)
Estado:	Firmado
ID de transacción:	CBJCHBCAABAAFFKi-eR04CtfE5ccNhOeWzgsKf-HqnYU

Historial de “Acta 009 - Infraestructura Tecnologica”

-  lina alvarez (linalvarezh@gmail.com) ha creado el documento.
2023-03-15 - 23:54:52 GMT
-  El documento se ha enviado por correo electrónico a Mario Jaramillo (manager.etlaco@nexsysla.com) para su firma.
2023-03-15 - 23:55:48 GMT
-  El documento se ha enviado por correo electrónico a Lina Alvarez (lina.alvarez@pcmac.co) para su firma.
2023-03-15 - 23:55:48 GMT
-  Lina Alvarez (lina.alvarez@pcmac.co) ha visualizado el correo electrónico.
2023-03-15 - 23:55:56 GMT
-  Lina Alvarez (lina.alvarez@pcmac.co) ha firmado electrónicamente el documento.
Fecha de firma: 2023-03-15 - 23:56:20 GMT. Origen de hora: servidor.
-  Mario Jaramillo (manager.etlaco@nexsysla.com) ha visualizado el correo electrónico.
2023-03-16 - 13:17:21 GMT
-  Mario Jaramillo (manager.etlaco@nexsysla.com) ha firmado electrónicamente el documento.
Fecha de firma: 2023-03-16 - 13:20:38 GMT. Origen de hora: servidor.
-  Documento completado.
2023-03-16 - 13:20:38 GMT

Los usuarios de Acrobat Sign introducen los nombres y las direcciones de correo electrónico en este servicio. A menos que se indique lo contrario, estos datos no están verificados.



Powered by
Adobe
Acrobat Sign