Última actualización: octubre de 2021

Resumen de seguridad

HubSpot

Índice

Resumen de la seguridad en HubSpot

Nuestra empresa y nuestros productos

HubSpot es la plataforma líder en el mundo de inbound marketing, ventas inbound, asistencia, administración de contenido y operaciones. Desde 2006, HubSpot tiene la misión de hacer el mundo más inbound. Hoy en día, más de 100.000 personas y empresas en más de 120 países usan el software, los servicios y la asistencia de HubSpot para transformar la manera en que atraen a la clientela, interactúan con ella y la deleitan.

Los productos de HubSpot se ofrecen como soluciones de software como servicio (SaaS) y están disponibles mediante aplicaciones web específicas, interfaces de programación de aplicaciones (API) y plugins de correo electrónico.

Seguridad y riesgo en HubSpot

En materia de seguridad, HubSpot se centra principalmente en proteger los datos de su clientela. Por eso invertimos en los recursos y controles adecuados para proteger y brindar servicios a quienes nos eligen todos los días. Esa inversión incluye la implementación de equipos exclusivos de seguridad empresarial y seguridad de los productos, que son responsables del programa de seguridad integral de HubSpot y el proceso de control. Nos centramos en la definición de nuevos controles y el perfeccionamiento de los existentes, en la implementación y gestión del marco de seguridad de HubSpot y en el suministro de una estructura de soporte para facilitar una administración de riesgos efectiva. Nuestro director de seguridad de la información supervisa la implementación de medidas de protección en HubSpot y sus productos.

Nuestros objetivos de seguridad y gestión de riesgos

Desarrollamos un marco de seguridad adoptando buenas prácticas en la industria del SaaS y nuestros principales objetivos incluyen:

- Confianza y protección del cliente: ofrecer de manera consistente productos y servicios superiores a nuestra clientela mientras protegemos la privacidad y confidencialidad de su información.
- Disponibilidad y continuidad del servicio: garantizar la disponibilidad constante del servicio y los datos a todas las personas autorizadas, además de reducir de manera proactiva los riesgos de seguridad que amenacen la continuidad del servicio.
- Integridad del servicio y de la información: garantizar que la información del cliente nunca se corrompa ni altere de manera inapropiada.
- Cumplimiento normativo: diseñamos nuestro programa de seguridad corporativa en torno a las buenas prácticas de seguridad cibernética de la industria, que incluyen los controles de seguridad fundamentales del Center for Internet Security (CIS). Los controles que rigen la disponibilidad, confidencialidad y seguridad de los datos de la clientela también se diseñaron de conformidad con los Principios de servicios de confianza (TSP) que establece el Instituto Estadounidense de Contadores Públicos Certificados (AICPA).

Controles de seguridad de HubSpot

Con el objetivo de proteger los datos que se nos confían, aplicamos una estrategia de defensa exhaustiva para implementar capas de seguridad en toda nuestra organización. En las siguientes secciones, se describe un subconjunto de nuestras preguntas más frecuentes sobre controles.

Infraestructura del producto de HubSpot

Seguridad de la infraestructura en la nube

HubSpot no aloja los sistemas del producto en sus oficinas corporativas, sino que delega el alojamiento a Amazon Web Services (AWS), proveedor líder de infraestructura en la nube que garantiza una disponibilidad del servicio de entre un 99,95% y el 100% y redundancia a todos los servicios de energía, redes y climatización.

La infraestructura de producto de AWS se encuentra en la región este de EE.UU. o en Alemania. Este proveedor mantiene un programa de seguridad auditado, además de medidas de seguridad físicas, ambientales y de infraestructura. Los planes de recuperación ante desastres y continuidad del negocio se han validado como parte de sus certificaciones SOC 2 tipo 2 e ISO 27001.

La documentación de cumplimiento se encuentra disponible públicamente en la página de conformidad en la nube de AWS.

HubSpot también tiene un artículo en su base de conocimientos con preguntas frecuentes sobre nuestra infraestructura en la nube, que puedes leer aquí.

Seguridad de la red y protección del perímetro

La infraestructura de producto de HubSpot aplica varias capas de filtrado e inspección de todas las conexiones en la plataforma.

Se implementan listas de control de acceso a nivel de la red para evitar el acceso no autorizado a nuestra infraestructura de producto interna. También configuramos firewalls

para rechazar las conexiones de red que no estén autorizadas explícitamente por defecto y monitorizamos el tráfico para detectar cualquier actividad sospechosa.

Los cambios en la seguridad de la red se monitorizan activamente y se controlan mediante procesos de control de cambios estándar. Los conjuntos de reglas para los firewalls se revisan anualmente para ayudar a garantizar que solo se configuren las conexiones necesarias.

Gestión de la configuración

La automatización impulsa la capacidad de HubSpot de crecer con las necesidades de nuestra clientela. La infraestructura del producto es un entorno altamente automatizado que amplía la capacidad y la eficiencia en función de las necesidades. Las instancias de servidor se controlan minuciosamente, desde su aprovisionamiento hasta su desaprovisionamiento, garantizando así que toda la actividad que se desvíe de los parámetros de referencia establecidos se detecte y revierta con una frecuencia predefinida. Si un servidor de producción se desvía de la configuración de base, se sobrescribirá con la opción original en un plazo de 30 minutos.

Todas las configuraciones de tipo de servidor están incrustadas en imágenes y archivos de configuración. La gestión de la configuración a nivel del servidor se gestiona por medio de estas imágenes y scripts de configuración cuando se crea el servidor. Los cambios en la configuración y las imágenes estándar se gestionan a través de un proceso controlado de administración de cambios. Cada tipo de instancia incluye su propia configuración reforzada, según la implementación de la instancia.

La administración de parches se gestiona usando herramientas de administración de la configuración automatizada o eliminando las instancias de servidor que ya no cumplen con los valores de referencia previstos y aprovisionando una instancia nueva en su lugar. La gestión de la configuración rigurosa y automatizada ya está incorporada a nuestros procesos de infraestructura cotidianos.

Alertas y monitorización

En HubSpot, no solo automatizamos completamente los procedimientos de creación, sino que también nos involucramos profundamente en las características automatizadas de

respuesta, monitorización y alertas para abordar constantemente los problemas potenciales. La infraestructura del producto de HubSpot está diseñada para alertar a los ingenieros y administradores cuando se producen anomalías. Especialmente, las tasas de error, las situaciones de uso indebido, los ataques de aplicaciones y otras anomalías generan respuestas automáticas y alertas para que los equipos correspondientes investiguen y tomen las medidas pertinentes. Cuando ocurren actividades inesperadas o malintencionadas, los sistemas automatizados se aseguran de involucrar a las personas adecuadas para que el problema se solucione rápidamente.

Muchos de los desencadenantes automatizados también se diseñaron dentro del sistema para poder responder de inmediato ante situaciones imprevistas. Bloqueo de tráfico, cuarentenas, finalización de procesos y otras funciones similares se activan al llegar a umbrales predefinidos para garantizar que la plataforma de HubSpot pueda protegerse a sí misma frente a una amplia variedad de situaciones indeseables.

Protección de las aplicaciones

Medidas de protección de las aplicaciones web

Todo el contenido de la clientela alojado en la plataforma está protegido con un firewall de aplicaciones web (WAF). El WAF está configurado con una combinación de reglas estándar de la industria y personalizadas, capaces de activar y desactivar automáticamente los controles correspondientes para proteger mejor a nuestros clientes. Estas herramientas monitorizan activamente el tráfico en tiempo real en la capa de aplicación y tienen la capacidad de alertar sobre un comportamiento malintencionado o rechazarlo según su tipo y clasificación.

Las reglas que se usan para detectar y bloquear tráfico malintencionado respetan las pautas de buenas prácticas documentadas por Open Web Application Security Project (OWASP) en las 10 recomendaciones principales de OWASP y otras recomendaciones similares. También se incorporan medidas de seguridad contra los ataques de denegación de servicio distribuido (DDoS). Estas medidas ayudan a garantizar que los sitios de la clientela y otras partes de los productos de HubSpot estén siempre disponibles.

Gestión del desarrollo y los lanzamientos

Una de las principales ventajas de HubSpot es un conjunto de características de progreso rápido. Mejoramos nuestros productos constantemente a través de un moderno enfoque con respecto al desarrollo de software.

Muchas veces al día se proponen, aprueban, fusionan e implementan códigos nuevos. Antes de la implementación, se llevan a cabo revisiones de código, pruebas (cuando corresponda) y aprobación de fusiones. El control de la aprobación está a cargo de propietarios de repositorios designados. Una vez que se aprueba, el código se envía automáticamente al entorno de integración continua de HubSpot, donde se realizan las tareas de compilación, embalaje y pruebas de unidades.

Con todas las implementaciones de códigos, se crean archivos de códigos de producción existentes en caso de que un punto de entrada posterior a la implementación detecte errores. El equipo de implementación gestiona las notificaciones relacionadas con el estado de sus aplicaciones. Si se produce un error, inmediatamente se lleva a cabo una reversión.

Usamos en gran medida el «gating» de software y la administración de tráfico para controlar características basadas en las preferencias de la clientela (beta privado, beta público o lanzamiento completo). HubSpot garantiza actualizaciones sin problemas y, al ser una aplicación SaaS, no tendrás períodos de inactividad asociados a los lanzamientos. Los principales cambios en las características se comunican con mensajes en la aplicación o en publicaciones de actualización de productos.

Apenas se desarrolla el código, se lo implementa en el entorno de control de calidad exclusivo e independiente de HubSpot para la última fase de prueba antes de pasar a producción. La segmentación a nivel de la red evita el acceso no autorizado y no deseado entre los entornos de aseguramiento de la calidad y producción.

Análisis de vulnerabilidad, pruebas de penetración y programas de recompensas por detección de errores

El equipo de seguridad de HubSpot administra un enfoque de múltiples niveles para el análisis de vulnerabilidad, en el que hace uso de una variedad de herramientas reconocidas

en el sector para garantizar la cobertura completa de todos nuestros productos tecnológicos.

Los análisis de vulnerabilidad se configuran para buscar vulnerabilidades explotables a diario. Los análisis constantes, las listas de inclusión de análisis adaptables y las actualizaciones continuas de las firmas de detección de ataques ayudan a HubSpot a mantenerse un paso adelante ante muchas amenazas de seguridad.

También contratamos a otras empresas reconocidas en el sector para que realicen pruebas de penetración anuales. El objetivo de estos programas es identificar de manera iterativa los errores que supongan un riesgo para la seguridad y abordar con rapidez cualquier problema. Las pruebas de penetración se realizan en las capas de la aplicación y las capas de la red del sistema tecnológico de HubSpot.

Además del análisis de vulnerabilidad interno y las pruebas de penetración independientes, HubSpot dispone de un programa de recompensas por detección de errores donde invitamos a investigadores de seguridad independientes a participar en la identificación de fallas en los productos de HubSpot. Los miembros de la comunidad y los clientes y clientas de HubSpot pueden realizar pruebas de seguridad en los portales de prueba. En https://bugcrowd.com/hubspot, encontrarás información acerca de nuestro programa de recompensas por detección de errores.

Protección de datos de la clientela

Separación lógica de instancias

HubSpot ofrece una solución de SaaS multiinquilino altamente escalable. La interfaz de usuario y las API de HubSpot limitan el acceso exclusivamente al contenido autorizado. HubSpot segmenta lógicamente los datos mediante un ID de portal y asocia ese ID único con todos los datos y objetos pertenecientes a una o un cliente específico. La información está disponible por medio de la interfaz de usuario o API para un portal específico de HubSpot, sin riesgo de acceso entre portales o contaminación de datos.

Las reglas de autorización se incorporan a la arquitectura del diseño y se validan de manera continua. Además, registramos la autentificación de aplicaciones y los cambios asociados, la disponibilidad de las aplicaciones y las vistas de páginas de los usuarios.

Información confidencial

Los productos de HubSpot constituyen una experiencia integrada de marketing, ventas, servicios, gestión de contenido y operaciones. La información recopilada en nuestros productos se obtiene a través de la interacción con leads o la clientela, los directorios públicos y proveedores externos con buena reputación.

Las herramientas de HubSpot permiten a la clientela definir el tipo de información que se recopilará y almacenará en su nombre. De acuerdo con los Términos de servicio y la Política de uso aceptable de HubSpot, nuestros clientes y clientas son responsables de recopilar solo la información adecuada para respaldar sus procesos de marketing, ventas, servicios, gestión de contenido y operaciones. Los productos de HubSpot no se deben utilizar para recopilar o captar información confidencial, como números de tarjetas de crédito o débito, información de cuentas financieras personales, números del seguro social, pasaportes y licencias de conducir, ni tampoco información laboral, financiera o de salud.

Puedes ver más información sobre la clasificación de datos que se usan y son compatibles con el sistema de HubSpot en la tabla de clasificación de datos de nuestro informe de SOC 2.

Cifrado en tránsito y en reposo

Todas las interacciones confidenciales con los productos de HubSpot (p. ej., llamadas de API, sesiones autentificadas, etc.) se cifran en tránsito con TLS versión 1.2 o 1.3 y claves de 2048 bits o superiores. La seguridad de la capa de transporte (TLS) también está disponible por defecto para los clientes y las clientas que alojen sus sitios web en la plataforma de HubSpot.

Consulta nuestra guía de configuración de sitios web y nuestro artículo de la base de conocimientos sobre SSL y seguridad de dominio para ver más información sobre cómo configurar TLS.

HubSpot utiliza varias tecnologías para garantizar que los datos guardados se cifren en reposo. Los datos de la plataforma se almacenan usando cifrado AES-256. Las contraseñas de los usuarios se cifran en reposo con hash siguiendo las buenas prácticas de la industria. Determinadas características de correo electrónico funcionan al cifrar datos de mensajes tanto en reposo como en tránsito.

Gestión de claves

La plataforma de HubSpot administra de manera segura las claves de cifrado para el cifrado en reposo y en tránsito. Las claves privadas de TLS para el cifrado en tránsito se administran mediante nuestro partner de entrega de contenido. Las claves de cifrado a nivel de campo y de volumen para el cifrado en reposo se almacenan en un sistema de administración de claves (KMS) reforzado. Las claves se rotan a una frecuencia que depende del nivel de confidencialidad de los datos que se están cifrando. En general, los certificados TLS se renuevan anualmente.

En este momento, HubSpot no puede usar claves de cifrado suministradas por la clientela.

Respaldo de datos y recuperación ante desastres

Fiabilidad y recuperación del sistema

Nos esforzaremos en la medida de lo comercialmente razonable para garantizar un tiempo de actividad del sistema del 99,95% para nuestro servicio de suscripción en un mes natural determinado. Consulta la sección 7 de los Términos específicos de los productos para más información.

Además, proporcionamos actualizaciones en tiempo real y datos históricos sobre el estado del sistema y la seguridad por medio de la página de estado de HubSpot.

Todos los servicios y productos de HubSpot se crean con total redundancia. La infraestructura del servidor se distribuye estratégicamente entre diversas zonas de disponibilidad y redes de nube privada virtuales bien diferenciadas dentro de nuestros proveedores de infraestructura, y todos los componentes web, de aplicaciones y de base

de datos se implementan con un mínimo de n+1 instancias de servidor o contenedores compatibles.

Recuperación ante desastres

HubSpot cuenta con un plan de recuperación ante desastres que se prueba anualmente como parte de nuestros controles de SOC 2. Consulta el informe de SOC 2 (que puedes descargar en hubspot.es/security) para más información.

Estrategia de respaldo

COPIAS DE SEGURIDAD DEL SISTEMA

Se crean copias de seguridad de los sistemas regularmente según frecuencias y cronogramas establecidos. La copia de seguridad de una base de datos incluye los últimos siete días; de esta manera, la restauración se puede realizar fácilmente. Las copias se monitorizan para garantizar que se ejecuten correctamente y se generan alertas en caso de excepciones. Las alertas de fallas se derivan, investigan y resuelven.

Los datos se respaldan a diario en su región y se copian periódicamente en una región de AWS distinta por si se produce una interrupción regional primaria del servicio. Hay alertas y controles para detectar y clasificar fallas de replicación.

Todos los conjuntos de datos se guardan en una instalación de almacenamiento de archivos de alta disponibilidad, como S3 de Amazon.

ALMACENAMIENTO FÍSICO DE COPIAS DE RESPALDO

Como usamos servicios de nube pública para el alojamiento, el respaldo y la recuperación, HubSpot no implementa infraestructura física ni medios de almacenamiento físicos dentro de sus productos. Además, no solemos producir ni utilizar otros medios impresos (p. ej., papel, cinta, etcétera) como una alternativa para poner nuestros productos a disposición de la clientela.

PROTECCIONES DE LAS COPIAS DE RESPALDO

Por defecto, todas las copias de respaldo se protegen con restricciones de control de acceso en las redes de infraestructura del producto de HubSpot y listas de control de acceso en los sistemas de archivos que guardan los archivos de respaldo.

OPCIONES DE RESPALDO DE LA CLIENTELA

Para los clientes que además quieran respaldar sus datos, la plataforma de HubSpot brinda muchas maneras para que te asegures de tener lo que necesitas. Muchas de las características que hay en tu portal contienen funciones de exportación y la biblioteca de API públicas de HubSpot puede usarse para sincronizar tu información con otros sistemas. Si quieres más información para respaldar tus datos, consulta nuestro artículo de la base de conocimientos sobre cómo exportar contenido.

Identidad y control de acceso

Gestión de usuarios de los productos

Los productos de HubSpot admiten reglas de autorización detalladas. Los clientes pueden crear y administrar usuarios de sus portales y asignar los privilegios apropiados para sus cuentas, además de limitar el acceso a sus características de datos.

Si quieres más información sobre las funciones de los usuarios, consulta la Guía de permisos y funciones de los usuarios de HubSpot.

Medidas de protección del inicio de sesión de los productos

Los productos de HubSpot permiten a los usuarios ingresar a sus cuentas mediante el inicio de sesión incorporado con la cuenta de Google o SSO. El inicio de sesión incorporado refuerza una política de contraseñas uniforme que requiere un mínimo de 8 caracteres con una combinación de letras minúsculas y mayúsculas, caracteres especiales, espacios en blanco y números. Quienes usan el inicio de sesión incorporado de HubSpot no pueden cambiar la política de contraseñas predeterminada.

El inicio de sesión con la cuenta de Google está disponible para toda la clientela de HubSpot. Las opciones más avanzadas de SSO basado en SAML integradas en cualquier IDP basado en SAML están disponibles para el nivel Enterprise.

Quienes usan un proveedor de SSO pueden ofrecer esta opción a sus usuarios. Las instrucciones para configurar el SSO están disponibles en este artículo de la base de conocimientos y en HubSpot Academy. Aquellos que opten por SSO o inicio de sesión con

Google pueden configurar una política de contraseñas en sus cuentas correspondientes de SSO o Google.

También se recomienda que quienes usan el inicio de sesión incorporado de HubSpot configuren la autentificación de dos factores para sus cuentas; además, las y los administradores de portal pueden configurar sus portales de HubSpot para garantizar que todas las personas tengan habilitado este tipo de autentificación.

Autorización de API de productos

El acceso a la interfaz de programación de aplicaciones (API) se habilita mediante la autorización de la clave de API u OAuth (versión 2). Las y los clientes tienen la capacidad de generar claves de API para sus portales. Las claves están diseñadas para crear prototipos de integraciones personalizadas con rapidez. La implementación de OAuth por parte de HubSpot es una estrategia más orientada a la autentificación y autorización de las solicitudes de API. Además, el uso de OAuth es obligatorio para todas las integraciones destacadas. La autorización de las solicitudes habilitadas con OAuth se establece mediante alcances definidos. Para más información sobre el uso de API, consulta el portal de desarrolladores en HubSpot.com.

Acceso a la infraestructura de producción

El acceso a los sistemas de HubSpot se controla rigurosamente y sigue el principio de menor privilegio. El personal de HubSpot recibe acceso por medio de un modelo de control de acceso por función.

El acceso cotidiano se limita solo a las personas con empleos que lo requieren. Para el acceso de emergencia (p. ej., alertas, respuestas/resolución de problemas) y el acceso a las funciones administrativas, el sistema de HubSpot utiliza un modelo de acceso de tipo Just-In-Time Access (JITA), mediante el cual los usuarios pueden solicitar acceso a funciones privilegiadas por tiempo limitado. Se registra cada JITA y se monitorizan los registros continuamente para detectar solicitudes anómalas. Cuando se acaba el tiempo, el acceso a la cuenta se termina y el permiso se revoca automáticamente.

Además, las conexiones de red directas a los dispositivos de la infraestructura de producto mediante protocolos SSH o similares están prohibidas y los ingenieros deben autentificarse

primero por medio de un servidor o host bastión o «jump box» para poder acceder a entornos de aseguramiento de la calidad o producción. La autentificación a nivel del servidor implementa claves SSH únicas para los usuarios y autentificación de doble factor basada en fichas.

El acceso del personal a los recursos corporativos y de producción está sujeto a una revisión automatizada diaria y, como mínimo, a una recertificación manual semestral.

Acceso del personal de HubSpot a los portales de clientes

El personal de asistencia y servicios y otro personal de primera línea puede solicitar acceso JITA a los portales de clientes con una duración limitada. Las solicitudes de acceso se limitan a las responsabilidades de trabajo asociadas con la asistencia y el aprovisionamiento de servicios para nuestra clientela, y quedan restringidas al portal de un cliente específico durante un período máximo de 24 horas. Se registran todas las solicitudes de acceso, los inicios de sesión, las consultas, las visitas a páginas y otra información similar.

Autentificación y autorización corporativa

El acceso a la red corporativa, tanto de manera remota como presencial, requiere autentificación multifactorial (MFA) y todas las aplicaciones de SaaS que HubSpot utilice requieren SSO con MFA para facilitar el control de acceso centralizado.

Las políticas de contraseñas siguen las buenas prácticas de la industria en lo que respecta a la longitud, complejidad y frecuencia de rotación.

Creamos un extenso conjunto de sistemas de soporte para optimizar y automatizar nuestras actividades de cumplimiento y gestión de la seguridad. Además de muchas otras funciones, el sistema recorre nuestra infraestructura de producto y corporativa varias veces al día para garantizar que los permisos que se otorgan son adecuados, gestionar eventos de personal, revocar cuentas y acceso cuando sea necesario y recopilar evidencia de cumplimiento para cada uno de nuestros controles de seguridad tecnológica. Estos sistemas internos recorren la infraestructura y validan que cumpla con las configuraciones aprobadas las 24 horas del día.

Seguridad organizacional y corporativa

Verificación de antecedentes e incorporación

Todo el personal de HubSpot se somete a una extensa verificación de antecedentes por parte de un tercero antes de recibir una oferta formal de empleo. En particular, se revisan el empleo, la educación y los antecedentes penales. Fuera de Estados Unidos, se realizan verificaciones de empleo. La verificación de referencias se realiza a discreción del personal de gerencia que hace la contratación.

Al ser contratado, todo el personal debe leer y aceptar la Política de uso aceptable corporativa de HubSpot (AUP) y el Código de buen juicio, que ayudan a definir las responsabilidades del personal en materia de seguridad a la hora de proteger los activos y datos de la empresa, lo que incluye, entre otras cosas, la protección de dispositivos móviles y del equipo corporativo.

Gestión de políticas

Para lograr que todo el personal esté en sintonía con respecto a la protección de nuestros datos, documentamos y mantenemos por escrito diversas políticas y procedimientos. Contamos con una política fundamental de seguridad de la información escrita que abarca requisitos para el manejo de los datos, consideraciones de privacidad y respuestas a infracciones, entre muchos otros temas.

Las políticas se revisan y aprueban una vez al año como mínimo y se almacenan en el wiki de la empresa. Aquellas que requieren el reconocimiento del personal se incorporan de manera obligatoria a la capacitación anual.

Capacitación para crear conciencia sobre la importancia de la seguridad

El personal es nuestra primera línea de defensa y nos aseguramos de que tenga toda la preparación necesaria para ejercer sus funciones. Se ofrece capacitación para crear conciencia sobre la importancia de la seguridad, que abarca buenas prácticas de seguridad generales, a todo el personal nuevo de HubSpot al momento de la contratación y en forma anual. Además de esto, HubSpot mantiene actualizados a sus empleados y empleadas en

torno a las últimas noticias en materia de seguridad y a las iniciativas más recientes con artículos internos.

Tras la capacitación inicial, hay contenido más específico disponible según la función de un empleado y el acceso resultante. Por ejemplo, HubSpot cuenta con un programa de promoción de la seguridad donde los equipos de desarrollo tienen oportunidades para continuar capacitándose sobre desarrollo de la seguridad, riesgos comunes, amenazas y problemas.

Gestión del riesgo

HubSpot tiene un programa de gestión del riesgo empresarial que incluye una política documentada, evaluaciones de riesgo continuas y un registro formal de riesgos. Las actividades de disminución de riesgos y corrección se monitorizan por medio de un sistema de creación de tickets y se revisan a una frecuencia determinada.

En el informe de SOC 2 que puedes descargar en hubspot.es/security, podrás encontrar más información sobre el programa de evaluación y gestión de riesgos.

Gestión de proveedores

Recurrimos a empresas proveedoras de servicios que mejoran la capacidad de los productos de HubSpot para satisfacer tus necesidades de marketing, ventas, servicios, gestión de contenido y operaciones. Contamos con un programa de gestión de proveedores para garantizar que existan controles apropiados de seguridad y privacidad. El programa incluye la creación de inventarios, la monitorización y la revisión de los programas de seguridad de los proveedores que ofrecen compatibilidad con HubSpot.

Se evalúan las medidas de seguridad apropiadas para el servicio proporcionado y el tipo de información que se intercambia. El cumplimiento continuo de las medidas de protección previstas se gestiona como parte de nuestra relación contractual con ellos. Nuestros equipos de seguridad, asesoramiento legal y cumplimiento trabajan en coordinación con nuestras partes interesadas en el proceso de revisión de la gestión de proveedores.

También encontrarás una lista de subprocesadores de HubSpot dentro del Acuerdo para el procesamiento de datos (DPA).

Seguridad física corporativa

Las oficinas de HubSpot cuentan con muchas medidas de seguridad. En todas las sedes globales hay guardias de seguridad que ayudan a crear un entorno seguro para el personal. El acceso se controla con fichas RFID individuales, que se desactivan automáticamente si se pierden o ya no son necesarias (p. ej., ante un despido, por el uso poco frecuente, etc.). También contamos con videovigilancia y otras medidas de seguridad.

Medidas de seguridad de la red corporativa

Se implementan firewalls de aplicación administrados en forma centralizada para garantizar la disponibilidad en las oficinas de HubSpot. Nuestras redes de invitados están separadas de nuestra red corporativa y cuentan con firewalls diferentes. También configuramos firewalls para filtrar tráfico entrante no autorizado proveniente de internet y para rechazar las conexiones de red entrantes que no estén autorizadas explícitamente por defecto.

HubSpot realiza controles de cumplimiento en el sistema antes de autorizar la conexión de un dispositivo a la red corporativa. Los dispositivos no autorizados se desconectan de inmediato o se mueven a VLAN de contención.

Seguridad en puntos de terminación y protección antivirus y contra malware

HubSpot aprovecha las funciones de detección y respuesta de puntos de terminación (EDR) para proteger sus sistemas. Con esto, tenemos gran visibilidad de los comportamientos anómalos del sistema y podemos investigar y tomar medidas rápidamente, ya sea a través de desencadenantes de eventos automatizados como de la contención manual de un sistema. Nuestra plataforma de EDR se integra con otras herramientas de seguridad para crear un entorno optimizado y así proteger nuestro negocio.

Gestión de incidentes

Respuesta ante incidentes

El centro de operaciones de seguridad de HubSpot proporciona cobertura las 24 horas del día, los 365 días del año para responder rápidamente a todos los eventos de seguridad y privacidad. El programa de respuesta rápida ante incidentes de HubSpot es adaptable y repetible. Se crean tipos de incidentes predefinidos y basados en tendencias históricas para facilitar el seguimiento de incidentes, la asignación de tareas, la derivación y la comunicación oportunos. Muchos procesos automatizados alimentan el proceso de respuesta ante incidentes, incluidas las alertas de actividad malintencionada o anomalías, alertas de proveedores, solicitudes de clientes y eventos de privacidad, entre otros.

En respuesta a un incidente cualquiera, primero determinamos el nivel de exposición de la información y definimos el origen del problema de seguridad si es posible. Proporcionamos actualizaciones periódicas según sea necesario para garantizar la resolución apropiada del incidente.

El personal directivo de seguridad revisa todos los incidentes relacionados con la seguridad, presuntos o confirmados, y coordinamos con los clientes afectados utilizando los medios más adecuados, según la naturaleza del incidente.

Además de nuestro centro de operaciones, también contamos con un equipo de detección de amenazas internas que trabaja para descubrir vulnerabilidades de manera sistemática y garantizar que se implementen las buenas prácticas para proteger nuestro producto.

Cumplimiento

Sarbanes-Oxley (SOX)

Como corresponde a una empresa que cotiza en bolsa, los controles de TI clave de HubSpot se auditan periódicamente como parte del cumplimiento de la ley Sarbanes Oxley (SOX).

La información pública sobre dicho cumplimiento se encuentra disponible en nuestros archivos de la Comisión de Bolsa y Valores (SEC). Puedes ver más información en nuestra página de relaciones con inversores (https://ir.hubspot.com/).

Controles del sistema y la organización (SOC 2)

HubSpot lleva a cabo auditorías estrictas de SOC 2 tipo 2 y SOC 3 anualmente para avalar los controles que rigen la seguridad, disponibilidad y confidencialidad de los datos de la clientela, ya que cumple con los Principios de servicios de confianza (Trust Service Principles, TSP) que establece el AICPA (Instituto Estadounidense de Contadores Públicos Certificados). El nivel de excelencia de nuestros controles nos llena de orgullo, por eso te invitamos a contactar con tu representante de HubSpot para obtener una copia de nuestro informe de SOC 2 tipo 2. El informe de SOC 3 se encuentra disponible públicamente para descarga desde la página de seguridad de HubSpot (hubspot.es/security).

Procesamiento y almacenamiento de datos confidenciales

Consulta nuestros Términos de servicio (legal.hubspot.com/es/terms-of-service) para ver más información sobre los tipos de datos prohibidos. Los productos de HubSpot no se deben utilizar para recopilar o captar información confidencial, como números de tarjetas de crédito o débito, información de cuentas financieras personales, números del seguro social, pasaportes y licencias de conducir o identificadores similares, ni tampoco información laboral, financiera o de salud.

Muchos clientes del ámbito médico utilizan HubSpot para sus equipos de atención al público sin incorporar información confidencial de salud. Sin embargo, no debe considerarse una solución para procesar o almacenar información médica protegida electrónicamente ya que no cuenta con la certificación de HITRUST ni cumple con la Ley de transferencia y responsabilidad de seguro médico (HIPAA).

Asimismo, cuando los clientes y clientas de HubSpot pagan por el servicio con tarjeta de crédito, no almacenamos, procesamos ni recopilamos información de las tarjetas de crédito que recibimos de nuestros clientes y no cumplimos con la normativa PCI-DSS. En cambio, recurrimos a procesadores de tarjetas de crédito confiables que cumplan con dicha normativa para garantizar el manejo seguro de nuestras propias transacciones de pago.

Privacidad

La privacidad de la información de nuestra clientela es una de las principales consideraciones de HubSpot. Tal como se describe en nuestra Política de privacidad, no venderemos tu información personal a ningún tercero. Las medidas de protección que se describen en este documento y otras medidas que hemos implementado se diseñaron para garantizar la privacidad y la integridad de tu información. Los productos de HubSpot se diseñan y construyen teniendo en cuenta las necesidades de la clientela y las consideraciones de privacidad. Nuestro programa de privacidad incorpora las buenas prácticas, las necesidades de la clientela y sus contactos y los requisitos normativos.

Retención y eliminación de datos

Los datos de la clientela se conservarán en tanto esta continúe activa. La plataforma de HubSpot brinda a su clientela activa las herramientas para eliminar su información (consulta la sección «Eliminación o devolución de datos personales» en nuestro DPA) o exportarla (consulta el artículo de la base de conocimientos sobre cómo exportar tu contenido y tus datos).

Los datos de antiguos clientes y clientas se eliminan de las bases de datos en tiempo real previa solicitud por escrito de la parte interesada o después de un plazo establecido a la terminación de todos los contratos. Los datos de quienes tienen la versión gratuita se depuran cuando el portal deja de estar activo y los datos de antiguos clientes de pago, 90 días después de que se termina la relación.

La información almacenada en copias, instantáneas y respaldos no se depura constantemente, sino que, de manera natural, se vuelve obsoleta en los depósitos a medida que transcurre el ciclo de vida de la información. HubSpot conserva cierta información, como registros y metadatos relacionados, para cumplir con normas de seguridad, cumplimiento o estatutarias.

Actualmente, no ofrece a su clientela la posibilidad de definir políticas personalizadas para la retención de datos.

Gestión del programa de privacidad

Los equipos jurídicos, de seguridad y de otra índole de HubSpot colaboran para garantizar una implementación eficaz y constante del programa de privacidad. Encontrarás información sobre nuestro compromiso con la privacidad de tu información en los siguientes documentos:

- Política de privacidad
- Política de privacidad de productos
- Acuerdo para el procesamiento de datos

Respuesta ante filtraciones de datos

Puedes ver nuestras políticas de informes, procesos y obligaciones en relación con la filtración de datos en nuestro informe de SOC, dentro de la sección «Respuesta ante incidentes».

También detallamos nuestras obligaciones con respecto a las violaciones de datos personales en el DPA.

RGPD

La plataforma de HubSpot contiene características que permiten a nuestra clientela cumplir con los requisitos del Reglamento General de Protección de Datos (RGPD), que incluyen la capacidad de realizar una eliminación según el RGPD en respuesta a solicitudes de acceso de partes interesadas. Consulta este artículo de la base de conocimientos y nuestra página de cumplimiento del RGPD aquí.

Alcance y uso del documento

HubSpot valora la transparencia en las maneras en que brindamos soluciones a nuestra clientela. Este documento se diseñó teniendo en cuenta esta cualidad. Mejoramos constantemente las medidas de protección que hemos implementado y, por esta razón, la

información y los datos que aparecen en este documento (incluidas las comunicaciones relacionadas) no pretenden crear un vínculo o una obligación contractual entre HubSpot y otras partes, ni enmendar, alterar o revisar los acuerdos existentes entre las partes.