Seguridad y Administración de Riesgos

Resumen del Programa

Última actualización: Junio de 2018

Contenidos

Resumen de la seguridad en HubSpot

1 Nuestra empresa y nuestro producto

HubSpot es el líder mundial en software de inbound marketing y ventas inbound. Desde 2006, HubSpot la misión ha consistido en hacer el mundo más «inbound». Hoy en día, decenas de miles de clientes en más de 90 países usan el software, los servicios y la asistencia técnica de HubSpot para transformar la manera en que atraen, interactúan y deleitan a los clientes. El software de inbound marketing y ventas inbound de HubSpot, clasificado como número 1 por VentureBeat, GetApp, Capterra y G2Crowd, abarca la publicación y monitorización en redes sociales, publicación en blogs, SEO, gestión de contenidos de sitios web, email marketing e informes y analíticas; todo en un solo producto integrado. Sales Hub and HubSpot CRM, las reconocidas aplicaciones de ventas de HubSpot, permiten que los equipos de ventas y servicio tengan conversaciones más eficaces con las oportunidades de venta, los prospectos y los clientes.

Los productos de HubSpot se ofrecen como soluciones de software como un servicio (SaaS). Estas soluciones están disponibles para los clientes mediante aplicaciones creadas para la Web, interfaces de programación de aplicaciones (API) y plugins de correo electrónico.

2 Control de la seguridad y del riesgo en HubSpot

El enfoque principal de la seguridad en HubSpot consiste en proteger los datos de nuestros clientes y usuarios. Esta es la razón por la que HubSpot ha invertido en los recursos y controles adecuados para proteger y servir a nuestros clientes. Esta inversión incluye la implementación de un equipo de seguridad dedicado. El equipo de seguridad es responsable de la seguridad integral y del programa de administración de riesgos, así como del proceso de control. El equipo de seguridad se centra en la definición de los nuevos controles así como en el perfeccionamiento de los ya existentes, en la implementación y gestión del marco de seguridad de HubSpot, así como en el suministro de estructura de soporte para facilitar una administración de riesgos efectiva. Nuestro director de seguridad, que reporta al director de finanzas, dirige el equipo de seguridad.

3 Nuestros objetivos de gestión de la seguridad y del riesgo

Hemos desarrollado nuestra estructura de seguridad utilizando las buenas prácticas en la industria de SaaS. Entre nuestros principales objetivos, se incluyen los siguientes:

- Confianza y protección del cliente: ofrecer de manera consistente un producto y servicio superior para nuestros clientes mientras protegemos la privacidad y confidencialidad de su información.
- Disponibilidad y continuidad del servicio: garantizar la disponibilidad del servicio y los datos de todos los individuos autorizados; reducir de manera proactiva los riesgos de seguridad que amenazan la continuidad del servicio.
- Información e integridad del servicio: garantizar que la información del cliente nunca se corrompa ni altere de manera inapropiada.
- Cumplimiento de estándares: implementar procesos y controles para alinearse con los estándares internacionales vigentes y con las buenas prácticas de la industria. Hemos diseñado nuestro programa de seguridad en torno a las mejores normas para la seguridad en la nube. En especial, nos servimos de estándares como COBIT y Cloud Security Alliance CCM, y alineamos nuestras prácticas con las normas ISO 27001 y NIST SP 800-53.

4 CONTROLES DE SEGURIDAD DE HUBSPOT

Con el objetivo de garantizar la protección de los datos que se nos confían, hemos implementado un conjunto de controles de seguridad. Los controles de seguridad de HubSpot están diseñados para que los empleados puedan tener un alto nivel de eficiencia sin obstáculos artificiales, al mismo tiempo que reducen los riesgos. Las siguientes secciones describen un subconjunto de controles. Para obtener más información acerca del programa de seguridad de HubSpot, echa un vistazo a todos los detalles en https://www.hubspot.es/security.

4.1 INFRAESTRUCTURA DEL PRODUCTO DE HUBSPOT

4.1.1 SEGURIDAD DEL CENTRO DE DATOS

HubSpot externaliza el alojamiento de su infraestructura de producto a proveedores de infraestructura en la nube líderes de la industria. Principalmente, los productos de HubSpot utilizan Amazon Web Services (AWS) y Google Cloud Platform (GCP) para el alojamiento de su infraestructura. Estas soluciones proporcionan altos niveles de seguridad física y de red, además de diversidad de proveedores de alojamiento. Actualmente, las instancias del servidor en la nube AWS de HubSpot residen en los Estados Unidos; las instancias de nube GCP residen en Alemania. Ambos proveedores mantienen un programa de seguridad auditado, incluido el cumplimiento de SOC 2 e ISO 27001. HubSpot no aloja ningún sistema informático de producción en sus oficinas corporativas.

Estos proveedores de infraestructura de clase mundial utilizan la infraestructura de las instalaciones más avanzadas, como la energía, las redes y la seguridad. El tiempo de funcionamiento de las instalaciones está garantizado entre el 99.95% y el 100%. Las instalaciones garantizan un mínimo de redundancia de N+1 a todos los servicios de energía, redes y de aire acondicionado. El acceso a estos sitios de proveedores está altamente restringido para acceso físico y electrónico mediante redes públicas (Internet) y privadas (Intranet) para eliminar cualquier interrupción no deseada en nuestro servicio a los clientes.

Las protecciones de seguridad física, ambiental y de infraestructura, incluidos los planes de continuidad y recuperación, se han validado independientemente como parte de las certificaciones SOC 2 Tipo II e ISO 27001. Los certificados están disponibles en el sitio de cumplimiento de AWS y en el sitio de seguridad de Google Cloud Platform.

4.1.2 SEGURIDAD DE LA RED Y PROTECCIÓN DEL PERÍMETRO

La infraestructura del producto de HubSpot se diseñó teniendo en cuenta las medidas de seguridad de Internet. En particular, las medidas de seguridad de la red están diseñadas para prevenir el acceso de red no autorizado a la infraestructura interna del producto. Estos controles de seguridad incluyen el enrutamiento a nivel empresarial y las listas de control de acceso a la red (uso de firewalls).

Las listas de control de acceso a nivel de la red se implementan en grupos de seguridad de Virtual Private Cloud (VPC) de AWS, que aplica medidas de protección a nivel de los puertos y las direcciones a cada una de las instancias del servidor en la infraestructura. Esto permite controlar en detalle el tráfico de red procedente de una red pública, así como el tráfico entre instancias del servidor en el interior de la infraestructura. Dentro de la infraestructura, las restricciones de red internas permiten emplear múltiples niveles con el objetivo de garantizar que solo los tipos de dispositivos apropiados puedan comunicarse.

Los cambios en el modelo de seguridad de red se monitorizan activamente y se controlan mediante procesos de control de cambios estándar. Se evalúan los riesgos de seguridad de todos los cambios y las reglas existentes, y se registran de forma adecuada.

4.1.3 *Gestión de la configuración*

La automatización impulsa la capacidad de HubSpot de crecer con las necesidades de nuestros clientes. La infraestructura del producto es un entorno altamente automatizado que amplía de manera flexible la capacidad y la eficiencia en función de las necesidades. Las instancias del servidor son manipuladas íntegramente con Puppet, lo que significa que las configuraciones del servidor se controlan rigurosamente desde su creación hasta su desaprovisionamiento.

Todas las configuraciones de tipo del servidor están incrustadas en imágenes y archivos de configuración de Puppet. 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 y el control de la configuración suele gestionarse eliminando las instancias del 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.

4.1.4 *Alertas y monitorización*

En HubSpot, no solo automatizamos completamente los procedimientos de creación, sino que también nos involucramos profundamente en las tecnologías automatizadas de respuesta, monitoreo 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 a los equipos correspondientes para que estos investiguen y efectúen las acciones pertinentes. Cuando ocurren actividades inesperadas o malintencionadas, los sistemas contactan con las personas adecuadas para garantizar que el problema se resuelva rápidamente.

Muchos de los desencadenantes automatizados también han sido diseñados dentro del sistema para poder responder de inmediato ante situaciones imprevistas. El bloqueo de tráfico, las cuarentenas, la 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 no deseadas.

El poder detrás de la capacidad de HubSpot para detectar y reaccionar ante anomalías radica en nuestro programa de monitoreo las 24 horas del día, los 365 días del año, así como en nuestro registro exhaustivo. Nuestros sistemas captan y almacenan registros que incluyen todas las tecnologías que abarcan nuestros productos. En la capa de la aplicación, también se registran todos los inicios de sesión, las vistas de página, las modificaciones y otros accesos a los portales de HubSpot. En el back-end de la infraestructura, registramos intentos de autentificación, cambios de permisos horizontales y verticales, el estado de la infraestructura y las solicitudes llevadas a cabo, entre muchos otros comandos y transacciones. Los registros y eventos se monitorean en tiempo real, y los eventos se transfieren de inmediato y a cualquier hora del día a los desarrolladores, a los profesionales de la seguridad y a los ingenieros para que tomen las medidas necesarias.

4.1.5 *Acceso a la infraestructura*

Categorías enteras de eventos de seguridad potenciales se evitan con un modelo de control de acceso bien diseñado, exigente y coherente. Por esta razón, se controla rigurosamente el acceso interno a los sistemas de HubSpot. Los empleados de HubSpot obtienen acceso a servicios corporativos, portales de ventas y marketing e infraestructura de producto según sus empleos usando un modelo de control de acceso basado en funciones. En la Sección 4.3, se incluye más información sobre el modelo RBAC de HubSpot en la empresa.

El acceso a herramientas de infraestructura, servidores y servicios similares se limita solo a las personas cuyos empleos lo requieren. Para el acceso de emergencia y 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.

Los usuarios tienen el privilegio de hacer solicitudes JITA por unidad empresarial y equipo. Cuando se requiere un acceso de emergencia, no estándar, como el acceso a sudo en un servidor Linux, el usuario solicita un JITA. Se registra el JITA y se monitorizan los registros continuamente para detectar solicitudes anómalas. Se otorga acceso a la función privilegiada, y la persona puede realizar su trabajo.

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.

4.2 Protección de las aplicaciones

4.2.1 Medidas de protección de las aplicaciones web

Como parte de su compromiso con la protección de los datos de los clientes y los sitios web, HubSpot ha implementado un firewall de aplicación web (WAF) reconocido en el sector. El WAF identifica ataques dirigidos a los productos de HubSpot o a los sitios de los clientes alojados en la plataforma. Las reglas que se usan para detectar y bloquear tráfico malintencionado cumplen con 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 los clientes y otras partes de los productos de HubSpot estén siempre disponibles.

El WAF está configurado con una combinación de las reglas estándares de la industria y de los clientes, pueden activar y desactivar automáticamente los controles adecuados para proteger mejor a nuestros clientes. Estas herramientas monitorizan el tráfico en tiempo real al nivel de la aplicación con la capacidad de alertar o negar un comportamiento malintencionado según el tipo de comportamiento y la tasa.

4.2.2 Gestión del desarrollo y lanzamientos

Una de las principales ventajas de HubSpot es un conjunto de características de rápido progreso. Mejoramos nuestros productos constantemente a través de un moderno enfoque respecto al desarrollo de software. Cientos de veces al día, se proponen, aprueban, fusionan e implementan códigos nuevos.

Equipos de ingenieros especializados con profundos conocimientos de la plataforma de HubSpot revisan los códigos y realizan controles de calidad a medida que la plataforma se desarrolla. El control de la aprobación está a cargo de propietarios de repositorios designados. Una vez aprobado, el código se envía automáticamente al entorno de integración continua de HubSpot, donde se realizan las tareas de compilación, embalaje y pruebas de unidades. Si se superan satisfactoriamente todas las pruebas, el nuevo código se implementa automáticamente en toda la capa de aplicación.

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.

Como parte del modelo de implementación continua, usamos principalmente software gating y de gestión del tráfico para controlar las características en función de las preferencias de los clientes (beta privado, beta público, lanzamiento completo). Los principales cambios en las características se comunican mediante mensajes dentro de la aplicación o publicaciones de actualización de producto. Los clientes y usuarios pueden registrarse para recibir actualizaciones en cuanto se publiquen o con la frecuencia que elijan.

4.2.3 *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 nuestra suite de productos tecnológicos. Llevamos a cabo diversas actividades de análisis de vulnerabilidad y pruebas de penetración contra nuestros sistemas de manera continua. Realizamos análisis de vulnerabilidad continuamente contra nuestras redes internas, aplicaciones e infraestructura corporativa. Los análisis de vulnerabilidad basados en la red y a nivel de las aplicaciones se realizan, como mínimo, una vez al día para asegurarnos de detectar las vulnerabilidades más recientes y actuar ante ellas. El análisis de código estático revisa automáticamente el código más reciente para detectar posibles errores de seguridad al comienzo del ciclo de vida de desarrollo.

Los análisis constantes, las listas de inclusión de análisis adaptables y las actualizaciones continuas de las firmas de ataques ayudan a HubSpot a mantenerse un paso más adelante ante muchas amenazas de seguridad. Para obtener una segunda opinión con respecto a nuestra capacidad de identificar y responder ante los riesgos de seguridad, contratamos a otras empresas reconocidas en el sector para que realicen cuatro pruebas de penetración al año. El objetivo de estos programas es identificar de manera iterativa los fallos que presenten riesgo para la seguridad y subsanar 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, y los evaluadores de penetración obtienen acceso interno a las redes empresariales o de productos de HubSpot para maximizar los tipos de vectores potenciales que se deben evaluar.

Además del análisis de vulnerabilidad interno y las pruebas de penetración independientes, HubSpot dirige un programa de recompensas por detección de errores. Se invita a los investigadores

independientes a participar en la identificación de fallos en los productos de HubSpot y se los premia por sus contribuciones. Los miembros de la comunidad y los clientes de HubSpot pueden realizar pruebas de seguridad en los portales de prueba. En https://bugcrowd.com/hubspot, encontrarás información acerca del programa de recompensas por detección de errores de HubSpot.

4.3 PROTECCIÓN DE DATOS DE LOS CLIENTES

4.3.1 INFORMACIÓN CONFIDENCIAL EN LOS PRODUCTOS DE HUBSPOT

Los productos de HubSpot representan una experiencia integrada de marketing y ventas. La información recopilada en nuestros productos está compuesta por información de marketing y ventas recopilada a través de la interacción con las oportunidades de venta, los directorios públicos o las fuentes de terceros con buena reputación. Las herramientas de captación de datos en línea de HubSpot permiten que los clientes definan el tipo de información que se almacenará en su nombre. De acuerdo con los Términos de Servicio y la Política de Uso Aceptable de HubSpot, nuestros clientes se aseguran de capturar solo la información adecuada para respaldar sus procesos de marketing y ventas. Los productos de HubSpot no se utilizan para recopilar o captar información confidencial, como números de tarjetas de crédito o débito, información de cuentas financieras personales, números del seguro social, números de pasaportes, números de licencias de conducir o identificadores similares, ni tampoco información laboral, financiera o de salud.

4.3.2 PROTECCIÓN DE LA INFORMACIÓN DE TARJETAS DE CRÉDITO

Muchos de los clientes de HubSpot pagan el servicio con tarjeta de crédito. HubSpot no almacena, procesa ni recopila información de las tarjetas de crédito que recibimos de nuestros clientes. Utilizamos las formas de pago confiables y compatibles con PCI de los proveedores para asegurar que la información de las tarjetas de crédito de los clientes se procesa de forma segura y de conformidad con las reglamentaciones pertinentes.

4.3.3 CIFRADO EN TRÁNSITO Y EN REPOSO

Todas las interacciones confidenciales con los productos de HubSpot (por ejemplo, llamadas de API, inicio de sesión, sesiones autentificadas en el portal del cliente, etc.) se cifran en tránsito con TLS 1.0, 1.1 o 1.2 y claves de 2.048 bits o superiores. Los clientes que alojan sus sitios en HubSpot pueden configurar los sitios para que también utilicen TLS. Consulta nuestra guía de configuración de sitio web para obtener más información sobre cómo configurar TLS. Los clientes que deseen limitar los protocolos de cifrado que se utilizan para las conexiones HTTPS pueden comenzar el proceso poniéndose en contacto con Asistencia Técnica a clientes o con el mánager del éxito del cliente.

HubSpot utiliza varias tecnologías para garantizar que los datos guardados se cifren en reposo. Los discos duros físicos y virtualizados utilizados por las instancias de servidor de productos de HubSpot, además de las soluciones de almacenamiento a largo plazo usan el cifrado AES-256. Además, algunos datos a nivel de campo o bases de datos se cifran en reposo, según la confidencialidad de la información. Por ejemplo, a las contraseñas de usuario se les aplica un algoritmo hash, y determinadas características de correo electrónico funcionan al cifrar datos de mensajes en reposo.

4.3.4 AUTENTIFICACIÓN Y AUTORIZACIÓN DE USUARIO

Los productos de HubSpot aplican una política de contraseña uniforme. La política de contraseñas requiere un mínimo de 8 caracteres que incluyen una combinación de letras minúsculas y mayúsculas, caracteres especiales, espacios en blanco y números. El requisito mínimo no se puede modificar según el portal. Los usuarios también pueden configurar la verificación en dos pasos usando el Autenticador de Google o un SMS para proporcionar un segundo factor al iniciar sesión.

Los clientes pueden asignar permisos detallados a los usuarios en sus portales y limitar el acceso al contenido y a las características del portal. Para obtener más información acerca de las funciones de los usuarios, consulta la Guía de Permisos y Funciones de los Usuarios de HubSpot.

El acceso a la interfaz de programación de aplicaciones (API) se habilita mediante la autentificación y la autorización de la clave de API u OAuth (versión 2). 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 autenticación y autorización de las solicitudes de la API. Además el uso de OAuth es obligatorio para todas las integraciones recomendadas. La autorización de las solicitudes para habilitar OAuth se establece mediante alcances definidos. Para más información sobre el uso de la API, consulta el Portal de desarrolladores en HubSpot.com.

4.3.5 Acceso de los empleados de HubSpot

HubSpot controla el acceso individual a la información dentro de su producción y ambiente corporativo. Un grupo reducido de empleados de HubSpot tiene acceso autorizado a la información de producción según su función en la empresa a través de controles de acceso por función (RBAC por sus siglas en inglés) o según las necesidades, lo que se conoce como JITA (just in time access/acceso justo al momento).

Los ingenieros y miembros del equipo de operaciones pueden tener acceso autorizado a varios sistemas de producción, como una función de su puesto. El acceso común necesita incluir respuestas de alerta y resolución de problemas, así como el análisis de información para las decisiones de inversión del producto y soporte de productos. El acceso a la infraestructura del producto está limitada por el acceso a la red, a la autenticación del usuario y a los controles de autorización. El acceso a las funciones de red se limita estrictamente a las personas cuyas funciones requieren ese acceso, y este se revisa continuamente.

El personal de asistencia al cliente, servicios y demás personal de interacción con el cliente que necesite información puede solicitar acceso just-in-time (JITA) a los portales del cliente con una duración limitada. Las solicitudes de acceso se limitan a las responsabilidades de trabajo asociadas con la asistencia técnica y el aprovisionamiento de servicios para nuestros clientes. Las solicitudes están limitadas a accesos Just-In-Time al portal de un cliente en particular durante un período de 24 horas. Se registran todas las solicitudes de acceso, los inicios de sesión, las consultas, las visitas a la página e información similar.

El acceso de los empleados a los recursos corporativos y de producción está sujeto a una revisión automatizada diaria y, como mínimo, a una recertificación manual semianual, para garantizar que la autorización que se otorgó es apropiada para la función y las necesidades laborales del empleado en cuestión.

4.4 PRIVACIDAD

La privacidad de la información de nuestros clientes 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 estado implementando, 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 del cliente y las consideraciones de privacidad. Nuestro programa de privacidad incorpora las buenas prácticas, las necesidades de los clientes y sus contactos, y los requisitos reglamentarios.

Por esta razón, HubSpot cuenta con la certificación de los Escudos de Privacidad (Privacy Shield) UE-EE. UU. y Suiza-EE. UU. Para obtener más información acerca de nuestra certificación, consulta el sitio del Escudo de Privacidad (Privacy Shield). Además, HubSpot cuenta con la certificación de TRUSTe de privacidad empresarial.

4.4.1 POLÍTICA DE RETENCIÓN DE DATOS

Los datos del cliente se conservarán en tanto que continúes siendo cliente y, mientras resulte práctico, tu información permanecerá en el sistema de HubSpot por tiempo indefinido. Los datos clave de ex clientes se eliminan de las bases de datos en tiempo real previa solicitud por escrito del cliente o después de un plazo establecido a la terminación de todos los contratos con el cliente. En general, los datos de los ex clientes se depuran 90 días después de terminar toda relación con dicho cliente. La información almacenada en copias, instantáneas y respaldos no se depura constantemente, sino que, de manera natural, envejece en los depósitos a medida que transcurre el ciclo de vida de la información. HubSpot se reserva el derecho de modificar el período de poda de datos y del proceso a su discreción, a fin de abordar las necesidades técnicas, de cumplimiento o legales.

4.4.2 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. En nuestra Política de Privacidad y nuestro Acuerdo para el procesamiento de datos, hallarás información detallada sobre nuestro compromiso con la privacidad de tu información.

4.5 CONTINUIDAD DEL NEGOCIO Y RECUPERACIÓN ANTE DESASTRES

HubSpot cuenta con planes de continuidad empresarial y recuperación de desastres que se enfocan en evitar las interrupciones mediante la redundancia de las telecomunicaciones, los sistemas y las operaciones empresariales, y las estrategias de recuperación rápida en casos de problemas de disponibilidad o rendimiento. Cuando ocurren situaciones que afectan al cliente, el objetivo de HubSpot es aislar y abordar el problema de manera rápida y transparente. Los problemas identificados se publican en el sitio de estado de HubSpot y se actualizan posteriormente hasta que se resuelve el problema.

4.5.1 RESISTENCIA Y RECUPERACIÓN DEL SISTEMA

La prueba de continuidad empresarial forma parte del procesamiento normal de HubSpot. Los procesos de recuperación de HubSpot se validan de manera continua a través de procedimientos normales de

mantenimiento y asistencia técnica. Seguimos los principios de implementación continua y creamos o destruimos muchas instancias de servidor como parte de nuestro mantenimiento y crecimiento diario regular. Asimismo, usamos dichos procedimientos para recuperarnos de instancias deficientes y otros errores, lo que nos permite poner en práctica nuestro proceso de recuperación todos los días.

Principalmente, el funcionamiento de HubSpot se basa en la redundancia de la infraestructura, la replicación en tiempo real y las copias de seguridad. 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.

4.5.2 Estrategia de copia de seguridad

HubSpot garantiza que los datos se copien y respalden en diversos almacenes de datos durables. El período de retención de las copias de seguridad depende de la naturaleza de la información. Los datos también se copian en las zonas disponibles y en las ubicaciones de la infraestructura para proporcionar una tolerancia a los fallos dentro de una zona disponible, así como la capacidad de expansión y de respuesta, cuando sea necesario. Además, para la capacidad de recuperación de datos, se han implementado y aplicado las siguientes políticas:

- Los datos (producción) del cliente se respaldan aprovechando diversas copias de la información en línea para la protección de datos inmediata. Todas las bases de datos de producción tienen, como mínimo, una copia principal (maestra) y una réplica (subordinada) de los datos en línea en cualquier momento específico. La copia de seguridad de una base de datos incluye los últimos siete días; de esta manera, la restauración se puede realizar fácilmente. Se utiliza la duplicación en tiempo real para las copias instantáneas que se toman y almacenan en un servicio secundario que se realiza al menos una vez al día y siempre que sea posible. Todos los conjuntos de datos de producción se almacenan en una instalación de almacenamiento de archivos distribuida, como S3 de Amazon.
- Ya que utilizamos los servicios de nube privada para el alojamiento, el respaldo y la recuperación, HubSpot no utiliza infraestructura física o medios de almacenamiento físicos dentro de sus productos. Además HubSpot no suele producir o utilizar otros medios impresos (por ejemplo, papel, cinta, etcétera) como una alternativa para poner nuestros productos a la disposición de los clientes.
- Por defecto, todos los respaldos se protegerán con restricciones de control de acceso en las redes de infraestructura del producto de HubSpot, listas de control de acceso en los sistemas de archivo que guardan los archivos de respaldo o mediante las protecciones de seguridad de la base de datos.

4.6 Seguridad corporativa de HubSpot

4.6.1 Autentificación y autorización de empleados

HubSpot aplica una política de contraseña corporativa según el estándar en la industria. Esta política requiere el cambio de contraseñas al menos cada 90 días. También requiere una longitud mínima de 8 caracteres para la contraseña, y los requisitos de complejidad incluyen caracteres especiales, letras mayúsculas y minúsculas, además de números. HubSpot prohíbe compartir la cuenta y la contraseña entre los empleados.

Por lo general, los empleados se autentican a la infraestructura del producto de HubSpot utilizando claves SSH. Donde se permiten las contraseñas, la política de contraseña requiere que contengan 12 caracteres. Además, muchas de las funciones que usamos para crear los productos de HubSpot utilizan la autenticación con varios factores o están protegidos con un solo inicio de sesión en las soluciones que permiten la autenticación de múltiples factores.

4.6.2 Gestión de acceso

HubSpot reglamentó y automatizó los procedimientos de autorización y autentificación para que los empleados accedan a los sistemas de HubSpot, incluidos los productos de marketing y ventas. Todos los accesos quedan registrados. Más a menudo, se otorga acceso en función de un modelo de control de acceso basado en funciones. El acceso just-in-time (JITA) se incorpora a los procedimientos automatizados en torno a un conjunto de mecanismos de autorización rigurosos.

Creamos un vasto 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 analiza nuestro producto y la infraestructura empresarial varias veces al día para garantizar que los permisos otorgados sean correctos, para administrar los eventos de empleado, para revocar cuentas y accesos cuando sea necesario, para compilar registros de solicitudes de acceso y para recopilar evidencia de cumplimiento de cada uno de nuestros controles de seguridad de tecnología. Estos sistemas internos recorren la infraestructura y validan que cumpla con las configuraciones aprobadas las 24 horas del día.

4.6.3 Verificación de antecedentes

Todos los empleados de HubSpot se someten a una extensa revisión de antecedentes por parte de un tercero antes de hacerles una oferta formal de empleo. En particular, para todos los empleados potenciales, se revisan el empleo, la educación y los antecedentes penales. La verificación de las referencias se realiza a discreción del gerente que hace la contratación. Todos los empleados reciben capacitación de seguridad durante el primer mes de empleo como parte del Programa de Seguridad de HubSpot junto con la capacitación de seguimiento para la función específica. Todos los empleados deben cumplir con los Acuerdos de Confidencialidad y la Política de Uso Aceptable como parte del acceso a las redes corporativas y de producción.

4.6.4 Gestión de proveedores

Recurrimos a pocas empresas proveedoras de servicios que mejoran la capacidad de los productos de HubSpot para satisfacer tus necesidades de marketing y ventas. Contamos con un programa de administración 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 salvaguardias apropiadas para el servicio proporcionado y el tipo de datos intercambiados. El cumplimiento constante de las medidas de protección esperadas se administra como parte de nuestra relación contractual con ellos. Nuestro equipo de seguridad, el consejo general y la unidad empresarial a la que pertenece cada contrato coordinan consideraciones únicas para nuestros proveedores como parte de la administración de contratos.

4.6.5 Conciencia de la seguridad y políticas de seguridad

Para lograr que nuestros empleados del área de ingeniería, asistencia y otros estén en sintonía con respecto a la protección de nuestros datos, HubSpot desarrolló y mantiene una Política de seguridad de la información escrita. La política cubre los requisitos de tratamiento de datos, consideraciones de privacidad y respuestas a violaciones, entre otros temas.

Con esta política, y la gran cantidad de medidas de protección y normas vigentes, también nos aseguramos de que los empleados de HubSpot estén bien capacitados para desempeñar sus funciones. Se ofrecen múltiples niveles de capacitación en seguridad a los empleados de HubSpot, según sus funciones y el acceso resultante. Los empleados nuevos reciben una formación general de concienciación de seguridad que abarca todos los requisitos de seguridad de HubSpot. Después de la formación inicial, hay disponibles diferentes alternativas de formación basadas en la función del empleado. Los equipos de ingeniería de HubSpot son quienes proporcionan capacitación específica para desarrolladores. En general, las sesiones de capacitación en ingeniería se realizan semanalmente, y una parte de ellas incluye documentación de seguridad. Se ofrecen capacitaciones periódicas a través de actualizaciones regulares, avisos y publicaciones wiki internas.

4.7 Gestión de incidentes

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, basados en tendencias históricas, para facilitar el seguimiento de incidentes, la asignación de tareas, la escalación 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. Nos ponemos en contacto con el cliente (y los demás clientes afectados) por correo electrónico o telefónicamente (si el correo electrónico no fuera suficiente). Proporcionamos actualizaciones periódicas según se requiere para garantizar la solución correcta de incidentes.

Nuestro director de seguridad revisa todos los incidentes relacionados con la seguridad, presuntos o comprobados, y coordinamos con los clientes afectados utilizando los medios más adecuados, según la naturaleza del incidente.

5 CARACTERÍSTICAS DE SEGURIDAD DEL PRODUCTO

El programa de seguridad de HubSpot está diseñado para proteger todos los productos de HubSpot. En cada producto, se toma ventaja de las buenas prácticas de seguridad de desarrollo de aplicaciones comunes así como de la seguridad de la infraestructura y las configuraciones de alta disponibilidad.

Ya sea que nuestros productos sean gratuitos o pagados, con muchas o pocas funciones, HubSpot siempre se esfuerza por mantener la privacidad de la información que nos confías. Los datos que almacenas en los productos de HubSpot son tuyos. Implementamos nuestro programa de seguridad para protegerla y la utilizamos solo para proporcionarte el servicio de HubSpot. Nunca compartimos información con nuestros clientes y jamás la vendemos.

5.1 MARKETING HUB

Acerca de: el producto Marketing Hub es nuestra solución de automatización del marketing líder en la industria. Proporciona herramientas efectivas fáciles de usar para gestionar tu estrategia de inbound marketing.

Alojamiento: La infraestructura del sistema de gestión de contenidos (CMS) principal se aloja en Amazon Web Services y Google Cloud Platform. La estrategia de alojamiento de HubSpot permite capacidades adicionales de redundancia, flexibilidad de arquitectura y capacidad de respuesta de la infraestructura. Nuestros procesos de implementación utilizan la seguridad de la red, la seguridad del servidor y las funciones de disponibilidad antes descritas.

Firewall de aplicaciones web: Los sitios de clientes alojados en los productos de HubSpot utilizan las protecciones de nuestro Firewall de Aplicación Web (WAF) de clase mundial. Por defecto, tu sitio web, tus blogs, las páginas de destino y otros tipos de presencia en línea alojados en HubSpot están protegidos ante ataques de aplicaciones web, como la denegación de servicios distribuida (DDoS). Cuando se producen eventos de seguridad, los equipos de operaciones de seguridad y operaciones técnicas de HubSpot actúan de inmediato para asegurarse de que tus sitios se encuentren protegidos siempre, las 24 horas del día, los 365 días del año.

Seguridad de la capa de transporte: Los clientes de marketing de HubSpot tienen la capacidad de habilitar y configurar los servicios de TLS para sus sitios, páginas de destino y medios de interacción con visitantes relacionados. De forma predeterminada, los certificados TLS utilizan nombres alternativos de sujeto y se gestionan a través de Akamai, nuestro proveedor de contenidos. Si te gustaría aprovechar las otras opciones de la TLS, consulta nuestras ofertas SSL con tu empleado de HubSpot favorito. Para obtener más información acerca de cómo comenzar, consulta este artículo de HubSpot Academy.

Opciones de cifrado: Por defecto, los sitios web de los clientes que usan HTTPS se configuran para permitir TLS 1.0, 1.1 y 1.2. Es posible eliminar la compatibilidad para uno o más de estos algoritmos. Los clientes también pueden habilitar la Seguridad de Transporte HTTP Estricta (HSTS) para su dominio alojado por HubSpot. Para hacer estos cambios, ponte en contacto con Asistencia Técnica de HubSpot o con el mánager del éxito del cliente.

5.2 HubSpot CRM

Acerca de: HubSpot CRM es uno de los tantos productos que le encantará a tu equipo de ventas. Los profesionales de ventas pueden empezar a usar el CRM sin costo y sin dolores de cabeza. Los primeros pasos para comenzar a utilizar HubSpot CRM solo toman unos minutos en la página del producto HubSpot CRM.

Seguridad por defecto: HubSpot CRM se beneficia de las mismas medidas de seguridad sofisticadas que ayudan a proteger los otros productos de HubSpot. Utilizamos el desarrollo avanzado de software seguro, la gestión de infraestructura y las metodologías de alerta que hemos perfeccionado en nuestros años de desarrollo de productos.

Integraciones de correo y bandeja de entrada conectada: Como usuario de HubSpot CRM, puedes conectar tu bandeja de entrada de correo electrónico de Gmail, Office365 o habilitada para IMAP. Las integraciones con Gmail y Office365 están protegidas por las capacidades de integración nativas en estos productos y autorizadas por estas. La integración de IMAP permite que tu bandeja de entrada conectada sincronice el correo con HubSpot CRM desde otros servicios de correo. Cuando un usuario configura una integración con IMAP, los productos de HubSpot actúan como cliente de IMAP. Los servicios compatibles con las integraciones con IMAP tiene varias protecciones integradas: los datos se cifran en tránsito de extremo a extremo; los datos se cifran en reposo a nivel del campo además de a nivel de la base de datos; los controles de acceso garantizan solo el acceso autorizado a la información.

Privacidad: Ya sea que nuestros productos sean gratuitos o pagados, con muchas o pocas funciones, HubSpot siempre mantiene la privacidad de la información que nos confías. Los datos que almacenas en los productos de HubSpot son tuyos. Lo utilizamos solo para proporcionarte el servicio de HubSpot.

Alojamiento: La infraestructura de HubSpot CRM está almacenada en Amazon Web Services para tomar ventaja de la redundancia y flexibilidad de la infraestructura que existe en toda la infraestructura de HubSpot. Nuestra estrategia de alojamiento también garantiza la infraestructura de clase mundial, y la seguridad y disponibilidad en la red.

Control de acceso: HubSpot CRM ofrece funciones intuitivas y fáciles de usar que dan el acceso correcto a los miembros del equipo de ventas correctos. Consulta el artículo de nuestra base de conocimientos para obtener más información acerca de las funciones del usuario.

5.3 HubSpot Sales

Acerca de: los productos de Sales Hub también incluyen el paquete galardonado de HubSpot con herramientas de ventas que ayudan a los profesionales a interactuar mejor con sus oportunidades de venta y mejorar la conversión.

Alojamiento: la infraestructura principal interna de Sales se aloja en Amazon Web Services y las capacidades adicionales se proporcionan a través de Google App Engine. Nuestra estrategia de alojamiento toma ventaja de la redundancia y flexibilidad de la estructura que existe en toda la infraestructura de HubSpot.

Almacenamiento de datos: Sales Hub almacena los meta datos de los mensajes de correo electrónico para brindar seguimiento de correo electrónico, envoltura de enlaces y servicios de conexiones. Los

datos se guardan en almacenes protegidos dentro de la infraestructura de HubSpot, y el acceso a los datos está íntegramente controlado. El acceso a los almacenes de datos está asignado a un limitado y pequeño grupo de empleados de HubSpot según sus funciones, y este acceso está limitado a quienes lo necesitan para responder a la atención al cliente y a solicitudes relacionadas.

Actualización perfectamente integrada: las herramientas de Sales están diseñadas para ayudar a incrementar tu productividad. Uno de los pasos que dimos para mejorar su experiencia es la actualización automática del plugin. En lugar de ser interrumpidos por notificaciones recurrentes para actualizar tu software, el plugin hace su proceso de actualización sin estorbarte en el camino.

6 AUDITORÍAS DE TERCEROS Y CERTIFICACIONES DE LOS CONTROLES DE SEGURIDAD DE HUBSPOT

HubSpot cuenta con la certificación TRUSTe de privacidad empresarial y cumple con el Escudo de Privacidad (Privacy Shield) UE-EE. UU.. También obtuvimos la clasificación SkyHigh de CloudTrust "Enterprise Ready" (empresa lista). Nuestros servicios se alojan en los proveedores de centros de datos de primer nivel Amazon Web Services y Google Cloud Platform. Todos los proveedores de infraestructura de HubSpot cuentan con la certificación SOC 2 Tipo II e ISO 27001 y mantienen las instalaciones protegidas contra intrusiones electrónicas y físicas.

7 ALCANCE Y USO DEL DOCUMENTO

HubSpot valora la transparencia en las maneras en que brindamos soluciones a nuestros clientes. 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.