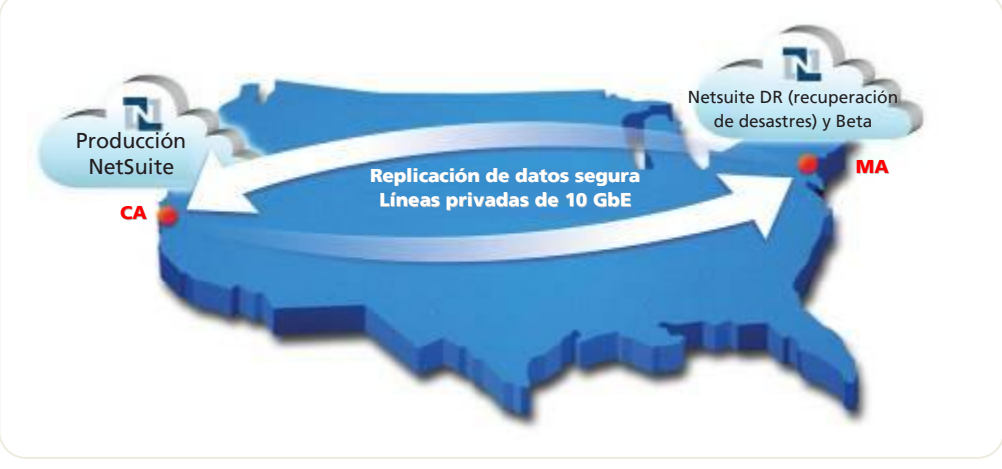
Hoja Informativa del Centro de Datos NetSuite

Administración, Seguridad y Disponibilidad de Datos de clase empresarial

NetSuite es el mayor proveedor de ERP del mundo, y ayuda a más de 10,000 organizaciones, procesa 1,500 millones de operaciones por trimestre e invierte más de $35 millones al año en Investigación y Desarrollo, además tiene 2.2 millones de sesiones únicas por trimestre. NetSuite también tiene un récord de 12 años manteniendo la seguridad de los registros de nuestros clientes.

Arquitectura del centro de datos NetSuite

NetSuite maneja dos centros de datos geográficamente separados: un Centro primario en California y uno secundario en Massachusetts. El centro de datos secundario proporciona funciones de espejo de datos, recuperación de desastres y capacidad de conmutación por fallos, en caso que el centro primario no funcione. Las instalaciones de ambos centros de datos son operadas por un proveedor de colocación líder, que otorga protección contra incendios y temblores así como calefacción, enfriamiento y energía de respaldo. La aplicación NetSuite es de múltiples tenedores y todos los servidores, almacenamiento y discos duros están integrados en varias capas de redundancia.



NetSuite proporciona un Centro de Datos primario y uno secundario

Datos sobre la infraestructura del centro de datos de NetSuite

Administración de datos

- **Redundancia:** Muchas capas en el sistema NetSuite implementan niveles múltiples de redundancia. Este diseño permite que falle uno o más elementos sin interrumpir el servicio, ya que cuenta con múltiples sistemas redundantes en línea, que asumen automáticamente el procesamiento y cubren el componente que falló.
- **Recuperación de Desastres:** la información en el centro de datos primario en California se replica y sincroniza en el centro de datos secundario en Massachusetts. En caso que falle el centro primario de datos, todas las operaciones se mudan hacia el centro secundario.
- **Escalabilidad:** Desde Enero de 2011, después de 12 meses, NetSuite da apoyo a 10,000 organizaciones con más de 4,000 millones de solicitudes de clientes por mes. NetSuite ha diseñado sus sistemas para adecuarlos a los picos e irrupciones durante el uso y para que se escale de manera suave, a fin de satisfacer el incremento de volumen y transacciones.

Certificado en Estados Unidos por EU Safe Harbor

Certificado por TRUSTe Privacidad

PCI Security Standards Council

SAS70 Completed Type II Audit

Seguridad de la Aplicación

- **Codificación:** La transmisión de la ID y contraseña únicas del usuario, así como de los datos resultantes de la conexión, tienen una codificación SSL de 128 bits. El resto de datos está codificado utilizando estándares como AES para aplicaciones simétricas y SHA2 para aplicaciones "Hash", según lo establecido en el PCI-DSS.
- **Acceso Exclusivo de la Aplicación:** El sistema está dividido en capas que separan los datos de la aplicación NetSuite misma. Los usuarios de la aplicación sólo pueden acceder a los componentes de la misma y no a la base de datos subyacente u otros componentes de infraestructura.
- **Nivel de RolAcceso e Inactivo Desconectar:** Los clientes pueden asignar a cada usuario un rol específico con permisos específicos para sólo ver y utilizar aquellos componentes relacionados con su trabajo. Existe un rastro de auditoría completo para cada transacción, en donde es posible seguir los cambios mediante los detalles de ingreso del usuario y una marca de tiempo cada vez que se hace un cambio. El sistema también detecta conexiones inactivas y automáticamente bloquea la pantalla del navegador a fin de evitar el acceso no autorizado desde una computadora desatendida.
- **Restricciones de Dirección IP:** Se pueden colocar restricciones al acceso a una cuenta NetSuite desde computadoras y/o lugares específicos. Esto es muy útil para los clientes a quienes les interesa saber no sólo quién tiene permiso para ingresar a su cuenta de NetSuite, sino también desde dónde entran a ella. Esta característica reduce significativamente el riesgo de que terceros tengan acceso a la cuenta del usuario.
- **Políticas de Contraseña Robustas:** NetSuite ofrece minuciosas opciones de confirmación de contraseñas que van desde la longitud de la misma hasta la caducidad de la contraseña de un usuario y el marco de tiempo que se desee. Los clientes pueden configurar políticas de contraseñas estrictas para asegurarse que las contraseñas nuevas sean diferentes a las anteriores y que sean lo suficientemente complejas como para incluir una combinación de números, letras y caracteres especiales. Las cuentas también se bloquean después de varios intentos incorrectos. Para los clientes que desean un mayor nivel de control de acceso, NetSuite ofrece autenticación de factores múltiples utilizando un simple Token físico. Además de ingresar sus propias contraseñas, los usuarios deben tener tokens físicos que generen contraseñas aleatorias de un solo uso. Éstas contraseñas criptográficamente robustas evitan que intrusos, miradas indiscretas, decodificadores de contraseña, phishers, etc. tengan acceso a la cuenta del usuario.

Seguridad Operativa

- **Monitoreocontinuo:** NetSuite emplea numerosos sistemas de detección de intrusos (IDS) para identificar tráfico malicioso que intente entrar a sus redes. Se bloquean todos los intentos no autorizados para ingresar al centro de datos y se registra e investiga cualquier intento de conexión no autorizado. También se cuenta con antivirus de grado empresarial para proteger el sistema contra troyanos, gusanos, virus y otro malware, evitando que éstos afecten el software y las aplicaciones.
- **Separación de Funciones:** Además de la investigación obligatoria de los antecedentes de los empleados de todos los niveles operativos de NetSuite, se separan las responsabilidades del trabajo. Se sigue el principio de menor autoridad (POLA) y a los empleados sólo se les dan los privilegios necesarios de acuerdo a sus funciones.
- **Acceso Físico:** Los operadores de ambos centros de datos mantienen políticas y controles de seguridad muy estrictos para permitir el acceso sin acompañante al personal de operaciones de NetSuite previamente autorizado:

Certificado en Estados Unidos por EU Safe Harbor

Certificado por TRUSTe Privacidad

PCI Security Standards Council

SAS70 Completed Type II Audit

  - La primera capa de seguridad incluye tarjetas de proximidad con ID con fotografía y un sistema de identificación biométrica. Este sistema de autenticación de factores múltiples proporciona seguridad adicional contra tarjetas extraviadas u otros intentos de usurpación de personalidad. Los lectores de tarjetas de proximidad se localizan en los principales puntos de entrada y se utilizan para asegurar las áreas críticas dentro de los centros de datos.
  - Portales para una sola persona y trampas T-DAR que garantizan que sólo se autentica una persona a la vez, a fin de evitar intrusiones. La detección y prevención de ingresos simultáneos e intrusiones utilizando puertas seguras aumenta significativamente la efectividad del sistema de control de acceso.
  - Además, todas las puertas del perímetro cuentan con alarma y monitoreo, y todos los muros, puertas, ventanas exteriores y la entrada principal están construidos con materiales con categoría de protección balística de Underwriters Laboratory (UL). La vegetación y otros objetos alrededor del centro de datos están colocados de tal manera que no pueda ocultarse un intruso.

- **Instalaciones Custodiadas:** Los guardias de seguridad de las instalaciones monitorean todas las alarmas, actividades del personal, puntos de acceso, envíos y recepción, además de asegurar de que se sigan correctamente los procedimientos de entrada y salida sobre una base de 24X7. Los guardias cuentan con un entrenamiento sobre lo que acontece, así como con desarrollo de actividades En los puntos de entrada y en otras áreas aseguradas dentro del perímetro están colocadas numerosas cámaras de vídeo vigilancia de circuito cerrado con capacidad panorámica, inclinación y acercamiento. Los vídeos se monitorean y almacenan para su revisión.
- **Auditorías de Desempeño del Centrode Datos:** La Gerencia de Operaciones de NetSuite implementa dichas auditorías, siendo éstas apropiadas para cumplir las normas SAS70 Tipo II y PCI. El exhaustivo proceso de gestión de riesgo de NetSuite se modeló basándose en la publicación especial 800-30 del Instituto Nacional de Estándares y Tecnología (NIST) y las series de estándares ISO27000. Se realizan auditorías periódicas para ayudar a asegurar que el desempeño del personal, cumplimiento de procedimientos, funcionalidad de equipo, registros de autorización actualizados y rondas de inventarios clave estén por encima de la media.
- **Certificaciones de Seguridad:** NetSuite pasó la auditoría SAS 70 Tipo II, está certificado por PCI-DSS y cuenta con una certificación EU-US Safe Harbor. NetSuite definió su Sistema de Administración de Seguridad de la Información en base a los estándares NIST, incluyendo los estándares de las series 800-53 e ISO27000.
  - Una de las cuatro principales firmas de auditoría está preparando una auditoría SAS 70 Tipo II para NetSuite. El reporte de auditoría SAS 70 muestra que hemos atravesado una profunda auditoría de nuestro ambiente de control, incluyendo controles de seguridad de dato y redes, procedimientos de respaldo y restauración de datos, disponibilidad del sistema y desarrollo de aplicación. Los requerimientos de la sección 404 de la ley Sarbanes-Oxley hace que el reporte de auditoría SAS 70 Tipo II sea esencial para el proceso de informe sobre la efectividad del control interno y sobre los reportes financieros de la compañía.
  - En cumplimiento con los requerimientos PCI-DSS, NetSuite ofrece autenticación de tarjeta de crédito con 3D Secure, también conocida como Verified by Visa (Verificado por Visa) y MasterCard Secure Code (Código Seguro MasterCard). 3D Secure agrega un más alto nivel de protección contra fraude de tarjeta de crédito. A los compradores se les pide crear contraseñas de autenticación de sus tarjetas de crédito o se les pide que ingresen su contraseña, si es que ya tienen una asignada.

Certificado en Estados Unidos por EU Safe Harbor

Certificado por TRUSTe Privacidad

PCI Security Standards Council

SAS70 Completed Type II Audit

– El EU-US Safe Harbor es clave para la transferencia de datos personales desde los países de la Unión Europea (UE) a Estados Unidos. Las organizaciones de la UE saben que las organizaciones que se certifican a si mismas ante el marco del U.S.-EU Safe Harbor proporcionan una protección 'adecuada' a la privacidad, según lo definido en la Directiva de la Comisión Europea sobre la Protección de Datos. NetSuite se apega a los Principios de Privacidad Puerto Seguro (Safe Harbor Privacy Principles) publicados por el Departamento de Comercio de Estados Unidos, relacionados con los datos personales de individuos que la EEA recibió de sus subsidiarias, clientes y otros socios de negocios. Se puede confirmar la participación de NetSuite en el programa U.S.-EU Safe Harbor mirando la lista pública de las organizaciones Safe Harbor publicada en http://safeharbor.export.gov/list.aspx.

Disponibilidad.

- **Compromiso de Nivel de Servicio (SLC):** El SLC de NetSuite garantiza un tiempo de funcionamiento de 99.5% (fuera de las ventanas de mantenimiento programadas) de las aplicaciones NetSuite en producción para todos nuestros clientes. Se dispone de un crédito si NetSuite no entrega sus servicios de aplicación con un tiempo de funcionamiento de 99.5%. Hemos promediado consistentemente un tiempo en funcionamiento real de 99.97% y tenemos disponibles para nuestros clientes una página Web que muestra, en todo momento, el estado del sistema http://status.netsuite.com.
- **Conexiones aInternet redundantes:** La red se construyó para cumplir o exceder los estándares mundiales de telecomunicaciones comerciales relacionados con disponibilidad, integridad y confidencialidad. Ambos centros de datos de NetSuite tienen tres canales de 1GBps de ruta múltiple diseñados de tal manera que pueden fallar dos conexiones al mismo tiempo sin tener impacto en la experiencia del usuario. Esta redundancia asegura que la conectividad es confiable y el máximo de tiempo de funcionamiento sin cuellos de botella en la transmisión de datos en un solo punto hacia o desde el centro de datos.
- **Sistemas de energía de respaldo:** NetSuite diseñó una solución para tener energía limpia y continua, se instalaron sistemas de energía ininterrumpida (UPS) con una configuración redundante, considerando los controles ambientales para los espacios de colocación. Cada sistema de batería está diseñado para trabajar a carga completa durante 15 minutos sin un generador. Los generadores de emergencia típicamente otorgan energía de respaldo en menos de 10 segundos y tienen el tamaño suficiente como para soportar toda la instalación con la carga máxima. Además de los sistemas de UPS, NetSuite hace uso de módulos de administración de energía y de unidades de distribución de energía en los pisos del centro de datos para un sistema físicamente integrado y eléctricamente redundante para selección de fuente, aislamiento, distribución, monitoreo y control de la energía que va a las cargas del equipo de cómputo.
- **Sistemas HVAC:** El aire acondicionado de ambos centros de datos está configurado para permitir una disipación de calor adecuada, permitiendo que los sitios operen dentro de un rango de temperatura aceptable. Para mantener el flujo de datos del aire acondicionado se utiliza un sistema redundante de unidades de HVAC N+1 dentro de cada ubicación. Las unidades HVAC se alimentan de sistemas eléctricos normales y de emergencia, para mantener su disponibilidad. Además, se han instalado tanques de agua fría, puesto que se requiere mantener las unidades de aire acondicionado funcionando durante su transición de energía directa a energía de generador durante emergencias.
- **Supresión de incendios:** En los centros de datos de NetSuite se emplearon los métodos más modernos de supresión de incendios. El sistema utiliza detectores de humo con tecnología de punta, complementados por detectores de calor y sistemas de aspersión de tubo seco.
- **Ingeniería sísmica:** Los centros de datos operados por NetSuite cuentan con equipo de aislamiento sísmico para amortiguar el movimiento en las instalaciones además de que se instalaron apuntalamientos contra temblores en todos los bastidores de los equipos. Los bastidores están anclados a la losa de concreto debajo del piso elevado del centro de cómputo.

Certificado en Estados Unidos por EU Safe Harbor

Certificado por TRUSTe Privacidad

PCI Security Standards Council

SAS70 Completed Type II Audit