



DOCUMENTO TÉCNICO

---

## VeriSign® Identity Protection



Where it all comes together.™



**CONTENIDO**

+ Introducción	3
+ Cómo evitar robos de identidad	4
Autenticación fuerte	5
Detección de fraude	6
+ VeriSign® Identity Protection Services	7
VeriSign® Identity Protection Authentication Service	7
VeriSign® Identity Protection Fraud Detection Service	8
+ The VeriSign® Identity Protection Network	9
VeriSign® Identity Protection Shared Authentication Network	9
VeriSign® Identity Protection Fraud Intelligence Network	10
+ VeriSign: un socio de confianza	11
Inteligencia compartida y Protección de la privacidad	11
+ Servicios futuros	12
Identity Proofing Services	12
Mutual Authentication Services	12
+ Más información	12



# VeriSign® Identity Protection

## + Introducción

El fenómeno del robo de identidades sigue proliferando y se ha convertido en un problema de importancia para empresas y clientes. Según Gartner, se han registrado unos 14.800 millones de dólares en pérdidas relacionadas con el robo de identidad entre abril de 2004 y mayo de 2005. Si bien estas pérdidas son significativas en sí mismas, es aún más inquietante el impacto negativo que ha tenido en las empresas cuyos clientes han sido víctimas de estos delitos. Pérdida de clientes, reducción de los volúmenes de transacciones y de los precios del stock han hecho que las pérdidas sean un grave problema para la mayoría de las empresas.

Teniendo en cuenta el impacto del robo de identidad en los negocios en línea y las directrices de regulación de la autenticación fuerte, cada vez más empresas están considerando aplicar opciones de comprobación de autenticación de su base de clientes en línea. Si sus clientes llegan a su negocio mediante Internet, conoce la importancia de identificarlos de una forma segura. La autenticación poco segura ha llevado al robo de identidades por Internet, al phishing y al fraude financiero en línea. A medida que más y más clientes utilizan equipos informáticos y teléfonos móviles para comprar, gestionar sus finanzas y acceder a información médica, el riesgo de fraude y de robos de identidad aumenta.

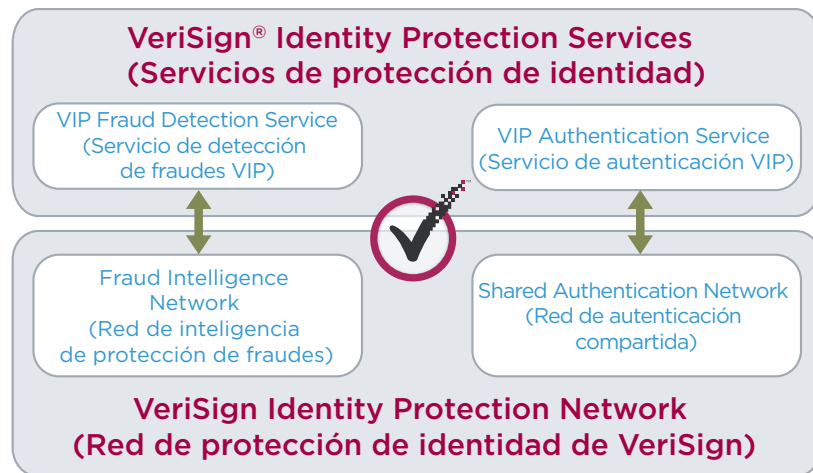
Durante muchos años, las empresas han utilizado la autenticación fuerte para asegurar el acceso de sus empleados y socios a aplicaciones y redes corporativas. El riesgo de permitir un acceso no autorizado a activos corporativos justificaba la inversión y el cambio en el comportamiento necesario para aplicar la autenticación fuerte y suponía una sencilla evaluación de riesgo/recompensa para la empresa. Sin embargo, teniendo en cuenta que estas soluciones empresariales se habían diseñado para aplicaciones de un volumen reducido, su uso para asegurar aplicaciones de clientes no es completamente factible. Extender el uso de estas soluciones de autenticación de empresas a millones de usuarios de una manera rentable es poco menos que imposible. Para dar cabida a las necesidades especiales de este nuevo segmento de autenticación de clientes, es necesario aplicar un sistema de autenticación totalmente nuevo.

VeriSign® Identity Protection Services (Servicios de protección de identidad de VeriSign) (VIP) es un conjunto integral de servicios de autenticación y protección de la identidad que permite que las aplicaciones de cara al público ofrezcan a los usuarios finales una experiencia segura en línea a un precio razonable. VeriSign aloja los servicios VIP y es posible acceder a ellos a través de los protocolos estándar de red para conseguir una fácil integración en las aplicaciones existentes de Internet. VIP permite una seguridad invisible gracias a VeriSign® Identity Protection Fraud Detection Service (Servicio de detección de fraudes), así como una mayor seguridad visible a través de VeriSign® Identity Protection Authentication Service (Servicio de autenticación y de protección de identidad de VeriSign). Para reducir al mínimo los costes y potenciar al máximo la seguridad compartiendo inteligencia y recursos, los servicios VIP están respaldados por la sólida VIP Network (Red VIP). La Red VIP permite compartir credenciales de autenticación mediante la VIP Shared Authentication Network (Red de autenticación compartida VIP) y compartir inteligencia de protección de fraudes a través de la VIP Fraud Intelligence Network (Red de inteligencia de protección de fraudes VIP). Los valores exclusivos de VIP son:

1. **Integral:** VeriSign® Identity Protection (VIP) incluye tanto medios invisibles (VeriSign® Identity Protection Fraud Detection Service (Servicio de detección de fraudes)) como visibles (VeriSign® Identity Protection Authentication Service (Servicio de autenticación VIP)) para asegurar las identidades en línea.
2. **Sencillo:** VIP permite una mayor sensación de seguridad para el consumidor, proporcionando una forma de uso similar al estilo actual de la web. El enfoque único basado en servicios VIP permite a las empresas delegar en terceros cualquier complejidad.

3. **Inteligente:** La Red VIP ofrece a las empresas una mayor visibilidad, lo que a su vez supone un mayor conocimiento de la situación general. Gracias a la gestión por parte de VeriSign de la infraestructura de Internet/DNS (Domain Name System, Sistema de nombres de dominio) y su infraestructura de autenticación compartida, VeriSign cuenta con una visión única e integral de inteligencia a nivel de todo Internet que no está al alcance de otras soluciones basadas en software.
4. **De confianza:** VeriSign lleva mucho tiempo siendo proveedor de servicios de autenticación para más de 500.000 sitios web: más del 93 % de la prestigiosa lista Fortune 500, los 40 bancos más importantes del mundo y 47 de los 50 mayores sitios de comercio electrónico. Como resultado, el sello VeriSign Secure Site Seal resulta enormemente significativo para el usuario y lleva mucho tiempo asociado a un comercio de confianza.

Este documento técnico describe cómo funcionan los componentes principales de VIP y cómo se complementan en la Red VIP.



#### + Cómo evitar robos de identidad

El robo de identidades y el fraude son problemas crecientes para los negocios basados en Internet, que afecta al coste de las operaciones comerciales, aleja a los clientes de las transacciones en línea y obliga a los estados a establecer leyes y regulaciones. En un estudio publicado en 2003, la Comisión Federal de Comercio (FTC, Federal Trade Commission) estimaba que el robo de identidades y el fraude suponía un coste medio de 10.200 dólares por incidente. En 2005, la Comisión Federal de Comercio descubrió que un 55% de todo el fraude se originaba en sitios web o por correo electrónico. Un estudio reciente sobre particulares en Estados Unidos realizado por Forrester Research establecía que el 36% de los consumidores no habían realizado un seguimiento de sus compras de bienes y servicios en red por motivos de seguridad. Las leyes estatales de Estados Unidos dirigidas especialmente a empresas de servicios financieros, como la última directriz sobre *autenticación en un entorno bancario en Internet*, aprobada por el Consejo Federal de Examen de Instituciones (FFIEC, Federal Financial Institutions Examination Council), han acentuado la necesidad de probar e implantar sistemas eficaces de autenticación fuerte.

VeriSign cree que la mejor forma de evitar robos de identidad y situaciones de fraude es mediante un sistema por capas. Para dificultar el robo de identidades, VeriSign recomienda adoptar sistemas de autenticación fuerte. Para dificultar que se utilicen identidades robadas, VeriSign recomienda adoptar sistemas de detección de fraude.

### Autenticación fuerte

La primera línea de defensa contra el robo de identidades es la autenticación fuerte. *Autenticación* es el proceso de validar que un usuario final es quien dice ser. El objetivo es distinguir entre un usuario real y un impostor. El método más simple y más extendido de autenticación con sistemas informáticos es mediante un nombre de usuario y una contraseña. La idea es que un usuario posee un factor único: una contraseña secreta. El usuario inicia sesión con un nombre de usuario y una contraseña. El nombre de usuario identifica la cuenta. La contraseña demuestra que el usuario es quien dice ser. Si sólo el usuario real conoce la contraseña secreta y el usuario actual demuestra que conoce la contraseña, entonces el usuario actual debe ser el usuario real.

### Problemas con las contraseñas

En teoría, este sistema debería funcionar perfectamente. Idealmente, todos los usuarios finales deberían escoger contraseñas que sean difíciles de adivinar, seleccionar una contraseña diferente para cada cuenta y no compartir nunca esta contraseña con otras personas. Desafortunadamente, los usuarios finales nunca eligen buenas contraseñas, no suelen elegir contraseñas diferentes para cuentas diferentes o mantienen sus contraseñas en secreto.

La gente suele elegir contraseñas simples que sean fáciles de recordar y con frecuencia utilizan nombres, palabras comunes y fechas. Los atacantes lo saben y a menudo averiguan una contraseña de usuario utilizando datos que conocen acerca de ese usuario (como su fecha de nacimiento, los nombres de sus hijos u otros datos) o simplemente averiguando palabras o fechas de forma aleatoria.

La mayoría de los usuarios tienen diferentes cuentas con servicios diferentes. Pocos usuarios pueden recordar una contraseña diferente para cada cuenta, por lo que la mayoría de usuarios utilizan la misma contraseña en todos los sitios web. Si se averigua la contraseña de un sitio, se averigua la contraseña de todos los sitios. Los atacantes pueden beneficiarse de ello creando un sitio web “gratuito” que requiera que el usuario se registre para ese servicio. La mayoría de los usuarios utilizarán el mismo nombre de cuenta y de contraseña que utilizan para su correo electrónico, su banco y para sitios de comercio electrónico. Finalmente, los correos electrónicos de phishing y los sitios web se han utilizado para defraudar a los usuarios. Muchos usuarios no saben distinguir entre sitios web reales y falsos y acaban facilitando su información de cuenta a terceras partes malintencionadas.

### Un factor adicional

La autenticación de múltiples factores está diseñada para afrontar estos problemas. Un sistema de autenticación adecuado combinará al menos un factor principal (un dato que el usuario conoce) con un factor secundario (un dato que el usuario tiene o que el usuario es). Si un atacante roba únicamente el primer factor, no podrá falsear el segundo factor y no podrá completar el proceso de autenticación. Si un atacante roba el segundo factor, no conocerá el primer factor y no podrá completar el proceso de autenticación. Existen muchos tipos diferentes de factores secundarios. Algunos de los factores más comunes incluyen tokens hardware, certificados digitales y dispositivos biométricos. Dependiendo de las necesidades específicas de una empresa, un sistema de autenticación puede requerir más de dos factores. Por ejemplo, un sistema puede requerir una frase clave, un certificado digital y un sensor de huellas digitales, combinándolo con algo que el usuario conoce, algo que el usuario tiene o algo que el usuario es.

### Detección de fraude

La segunda línea de defensa contra el robo de identidad es la detección de fraudes. Las técnicas de autenticación fuerte pueden reducir en gran medida, pero no pueden detener todos los ataques de fraude.

En primer lugar, la infraestructura necesaria para autenticación fuerte está aún por establecer. Son pocos los clientes que están familiarizados con las técnicas de autenticación fuerte como tokens OTP (Contraseña de un solo uso, One Time Password) y certificados digitales. Muchos clientes deberán aprender cómo utilizar esta tecnología. Además, las soluciones de autenticación fuerte pueden requerir grandes inversiones para las que las empresas pueden no estar preparadas.

En segundo lugar, las técnicas de autenticación fuerte para evitar robos de identidades no son infalibles. Aunque el robo de un dispositivo de segundo factor puede ser más difícil que diseñar un sitio web de phishing, no es algo imposible para este tipo de delincuentes. Asimismo, es posible que otras personas, como parientes o trabajadores domésticos, puedan robar tokens de autenticación de un usuario. Según un estudio reciente realizado por Javelin Strategy y Better Business Bureau, “Cuando la víctima puede identificar la persona que comete el robo de identidad, casi la mitad (el 47 por ciento) de todos los robos se perpetra por amigos, vecinos, empleados domésticos, familiares o parientes (personas conocidas)”. Si un atacante consigue robar o falsificar las credenciales de autenticación de usuarios, es deseable evitar que robe dinero o más información de la cuenta de un usuario.

### Detección de transacciones sospechosas

La mayoría de las veces, las acciones de un usuario se ajustan a un patrón. Por ejemplo, un usuario puede iniciar sesión en la cuenta de su banco desde su oficina en Barcelona durante la jornada de trabajo y volver a iniciar sesión desde su casa en Madrid el fin de semana. Normalmente comprueba el estado de sus cuentas, realiza sus pagos en línea y se desconecta. Ahora, suponga que alguien inicia sesión en esta cuenta de usuario desde un equipo en Rusia a primerísima hora de la mañana un martes e intenta transferir todo el dinero de la cuenta a un banco suizo. Esta transacción es una anomalía que no se ajusta al patrón normal. Utilizando algoritmos sofisticados, un equipo informático puede “aprender” patrones normales de uso con el tiempo y detectar si una transacción no encaja en el patrón. A este proceso se le denomina detección de anomalías y se puede utilizar para detectar transacciones potencialmente fraudulentas.

Igualmente, la mayoría de empresas han aprendido de la experiencia que algunas transacciones son arriesgadas de forma inherente. Incluso si el sistema de aprendizaje de la máquina no las clasifica como anómalas, algunas transacciones son tan sospechosas que cualquier empresa se tomará la molestia de volver a comprobarla. Por ejemplo, un sitio de comercio electrónico de los Estados Unidos puede querer volver a comprobar todas las operaciones realizadas desde Asia o todas las compras superiores a 10.000 dólares. Una solución completa de fraudes permite a las empresas establecer reglas como esta para detectar transacciones sospechosas.

### Confirmación de la identidad

No todas las transacciones sospechosas son fraudulentas. En ocasiones, un usuario final puede hacer algo inesperado, como iniciar sesión desde una ubicación diferente o realizar una transferencia por una cantidad elevada. Un sitio web no desea impedir que un usuario legítimo inicie sesión en un servicio o que realice una transacción, pero sí desea comprobar dos veces la identidad del usuario para asegurarse de que la transacción ni es fraudulenta. Por lo tanto, un sistema de detección de fraudes se debería complementar por un sistema de *confirmación de identidad*. El sistema de confirmación de identidad es un sistema automatizado de confirmación de la identidad del usuario final. El sistema debería permitir que el usuario final confirme su identidad fácil y rápidamente, sin contactar con el servicio de ayuda al cliente. De esta forma se ayuda a reducir el coste de confirmación de la identidad al sitio web y reducir las incomodidades para el usuario final.

### + VeriSign® Identity Protection Services

Los servicios VIP son una solución de niveles múltiples que proporciona mecanismos visibles e invisibles para asegurar las transacciones en línea y evitar los robos de identidad. VIP Fraud Detection Service (Servicio de detección de fraudes) ofrece funcionalidades de control invisibles del lado del servidor y VIP Authentication Service (Servicio de autenticación VIP) proporciona soluciones de autenticación fuerte más visibles, basadas en estándares y ambos servicios aseguran que una persona es quien dice ser.

#### VeriSign® Identity Protection Authentication Service

VeriSign Identity Protection Authentication Service proporciona una seguridad fuerte y visible para las aplicaciones de comercio en línea. VIP Authentication Service permite a las empresas emitir y/o aceptar fácilmente diferentes credenciales para diferentes usuarios. VIP Authentication Service (Servicio de autenticación VIP) proporciona una solución global y de alta seguridad disponible para las transacciones del cliente. Es ideal para las transacciones de mayor valor, que entrañan mayores riesgos.

VIP Authentication Service admite los estándares abiertos y permite la utilización de cualquier dispositivo compatible con OATH (Open Authentication, Autenticación abierta) en la autenticación. VIP Authentication Service incluye una serie de opciones para los factores suplementarios, incluyendo dispositivos de hardware autónomos, como los tokens de OTP (Contraseña de un solo uso, One Time Password), así como los dispositivos de software, como el OTP activado por voz, teléfonos móviles con OTP y OTP en mensajes SMS.

VIP Authentication Service se basa en una infraestructura de validación compartida respaldada por VeriSign que permite a las empresas implementar autenticación fuerte sin tener que soportar la carga de gestionar y operar infraestructuras propias de autenticación.

#### Gestión del ciclo de vida de las credenciales

Para los clientes de VIP Authentication Service (Servicio de autenticación VIP) que no quieren generar credenciales y aplicar todos los procesos necesarios inherentes (como verificación, distribución y servicio técnico de token), VeriSign ofrece una solución externa mediante el portal VIP. En la generación de credenciales directamente a los clientes, VeriSign se encarga de su creación, distribución y del primer nivel de servicio técnico a los clientes directamente. De esta forma las empresas pueden delegar la complejidad del proceso de verificación, distribución y servicio técnico de token en VeriSign, mientras que permite la autenticación fuerte de factores múltiples en sus aplicaciones en línea de forma fácil y sencilla.

#### Validación de credenciales

VIP admite los estándares abiertos y permite la utilización de cualquier dispositivo compatible con OATH (Open Authentication, Autenticación abierta) en la autenticación. OATH es una solución fruto de la colaboración de todo el sector para desarrollar una arquitectura de referencia abierta integrando los estándares existentes abiertos para una adopción completa de la autenticación fuerte. Al apoyar los estándares abiertos, la solución VIP AS puede dar cabida a una gama amplia de dispositivos de uso sencillo como PDA, memorias USB y teléfonos móviles, así como opciones de token autónomas más tradicionales, que se pueden utilizar para aportar una seguridad adicional.

VIP Authentication Service dispone de una serie de opciones de doble factor de autenticación, que incluye dispositivos de hardware autónomos, como los tokens de contraseña de un solo uso (OTP), Smart Cards, tokens USB así como certificados, OTP de pregunta/respuesta y activada por voz y software de teléfonos móviles. VIP hace posible que pueda ofrecer todas estas opciones a sus clientes hoy mismo, y pueda estar preparado para las opciones de autenticación de mañana. Los desarrolladores de sitios web pueden acceder a VIP Authentication Service (servicios de autenticación VIP) mediante un conjunto sencillo de API, con independencia de los factores suplementarios del usuario final.

### Integración con VIP AS

VIP AS está diseñado para integrarse fácilmente en las aplicaciones de Internet nuevas o existentes. Proporcionamos autenticación fuerte como un servicio de Internet que permite su integración como aplicación de fondo o del usuario. Un sitio web puede elegir contactar con nuestro servicio directamente mediante RADIUS, web service o cualquier otro protocolo. De forma alternativa, nuestro servicio permite a un sitio web integrarse en nuestro servicio mediante redirecciones http o métodos AJAX.

### Portal VeriSign® Identity Protection

VeriSign ofrece el portal VIP para clientes VIP que no quieran ofrecer servicio técnico a los clientes directamente y para usuarios finales que reciban credenciales de otras fuentes (como tiendas al por menor). El portal VIP es un sitio web que proporciona servicios y ayuda a usuarios finales, incluyendo sincronización de tokens OTP, reparaciones o sustitución o dispositivos con anomalías, así como informar de dispositivos perdidos o robados.

### VeriSign® Identity Protection Fraud Detection Service

El aspecto invisible de VIP es el Fraud Detection Service (Servicio de detección de fraudes, FDS). VIP FDS es un servicio que funciona en tiempo real detectando y evitando robos de identidad y transacciones fraudulentas. Incluye un sistema basado en normas y un exclusivo motor de comportamiento heurístico. El servicio está diseñado para proporcionar un servicio simple y evitar las intrusiones en sitios web y para usuarios finales. Si el sistema detecta una transacción sospechosa, los usuarios finales podrán confirmar rápidamente su identidad mediante un sistema automatizado. Dicho sistema automatizado puede solicitar al usuario que se identifique más claramente con cualquiera de los siguientes tipos de credenciales: contraseña de un solo uso, pregunta y respuesta única o una llamada al servicio de atención al cliente.

VIP Fraud Detection Service cuenta con cuatro ventajas clave:

- Invisible al cliente. VIP FDS no modifica la experiencia del usuario: un usuario inicia sesión en el sitio web de igual forma que siempre.
- Fácil de implementar. VIP FDS es una solución implementada sólo a nivel de servidor, que no requiere que el usuario final realice ningún cambio.
- Inteligencia. VIP FDS incluye tanto sistemas basados en reglas como en motores de autoaprendizaje de comportamiento para identificar los fraudes.<sup>8</sup>
- Conformidad. VIP Fraud Detection Service supone una forma económica de cumplir las normativas gubernamentales.

### Detección del fraude: Funcionamiento

VIP Fraud Detection Service utiliza una combinación de reglas y algoritmos aprendidos por el equipo para evitar el fraude. La aplicación web transmite la información en cada transacción a VIP FDS incluyendo encabezados del navegador web, direcciones IP y otros datos. El sistema VIP FDS (Servicio de detección de fraudes) comprueba una base de datos para obtener más información acerca de la dirección IP que incluye datos sobre ubicación geográfica, el tipo de conexión y el proveedor de acceso a la red.

El primer componente de VIP FDS es un eficaz sistema basado en reglas. Muchas empresas han luchado contra el fraude en línea durante largos años y conocen las tácticas empleadas por los delincuentes para robar dinero, bienes o identidades. Adicionalmente, los expertos de VeriSign han identificado muchos patrones comunes de transacciones fraudulentas. El motor de reglas de VIP FDS permite a las empresas utilizar este conocimiento para luchar contra el fraude. Los clientes pueden seleccionar entre un conjunto de normas predefinidas desarrolladas por VeriSign o pueden definir sus propias reglas utilizando una interfaz de usuario intuitiva. Además, los servicios profesionales de VeriSign pueden ayudar a identificar patrones sospechosos y aplicar reglas automatizadas para detectarlos.

El segundo componente del sistema VIP FDS es un sistema de autoaprendizaje automatizado de detección de anomalías. Mediante avanzados algoritmos de clúster, VIP FDS utiliza características de inicios de sesión de usuario – de tipo de navegador web, direcciones IP, fecha y hora, información del propietario de la cuenta y otras características – para generar un perfil de comportamiento normal de cada usuario. Cuando un intento de inicio de sesión no coincide con el patrón anterior, es posible que el inicio de sesión se haga desde otro equipo, en un día diferente o incluso desde un país diferente y el sistema VIP FDS marca la transacción como sospechosa.

Si el sistema VIP FDS detecta una transacción sospechosa, transmite la transacción a un sistema de confirmación de identidad antes de autenticar al usuario. El sistema le pide al usuario información adicional para confirmar su identidad, dependiendo del grado de riesgo. El sistema puede realizar más preguntas para confirmar la identidad o enviar un mensaje mediante un mecanismo externo, como una llamada de teléfono, un mensaje SMS o un correo electrónico. Si el usuario confirma su identidad correctamente, podrá iniciar sesión normalmente. Si el usuario no puede confirmar su identidad, se le solicitará que se ponga en contacto con el servicio de atención al cliente.

#### **+ VeriSign® Identity Protection Network**

De forma independiente, VIP Fraud Detection Service (Servicio de detección de fraudes) y VIP Authentication Service (Servicio de autenticación VIP) ofrecen una potente propuesta de valor: un conjunto completo de servicios, fácil de implantar y rentable que reduce los riesgos de fraude, mejora la seguridad y facilita el cumplimiento de las normativas vigentes. Sin embargo, VIP ofrece muchas más cosas.

La Red VIP es un conjunto de servicios que conforman VIP Fraud Detection Service y VIP Authentication Service. La Red VIP está formada por dos componentes: la Shared Authentication Network (Red de autenticación compartida) y la Fraud Intelligence Network (Red de inteligencia contra fraudes). Los servicios VIP se ven reforzados por los efectos de la red: La Red VIP ofrece una reducción de costes, una mejor experiencia del usuario final y una mayor seguridad gracias a los servicios de red. El servicio Shared Authentication Service ayuda a las empresas a compartir recursos de autenticación para reducir costes y mejorar la experiencia de los usuarios finales. El servicio Fraud Intelligence Network Service fomenta que los comercios compartan recursos de inteligencia sobre el fraude de identidades en línea para mejorar la seguridad.

Los clientes pueden elegir suscribir el servicio independiente o aumentar los beneficios de los usuarios de la red contratando ambos servicios. La Red VIP combina los dos servicios fundamentales VIP en un marco comercial único que facilita el proceso de compartir costos, datos y recursos.

#### **VeriSign® Identity Protection Shared Authentication Network**

La autenticación de factores múltiples puede ser un proceso costoso de aplicar y mantener para las empresas. Una empresa debe generar tokens para los clientes, proporcionar formación para su uso, modificar las aplicaciones para usar tokens de autenticación, ayudar a los clientes con tokens perdidos o incorrectos, responder a preguntas de los usuarios acerca de los tokens y muchas otras tareas.

Además, los clientes pueden rechazar la autenticación de factores múltiples, porque no es un proceso simple y que consume mucho tiempo. El servicio VIP Shared Authentication Service proporciona una solución a estos problemas. La mayor parte del éxito de las tarjetas de crédito tiene que ver con su generalización: funcionan de la misma forma en todas partes y se pueden utilizar en casi todos los sitios. Es raro que los clientes encuentren cajeros automáticos en los que sus tarjetas no funcionen. Creemos que es más probable que los usuarios finales adopten los factores secundarios si pueden utilizar el mismo dispositivo para todos los entornos y si el dispositivo es válido para todos los servicios. La Red VIP ayuda a solucionar estos requisitos.

Al compartir la infraestructura de autenticación entre los usuarios de la red, se reducen en gran medida los costes de implantar y mantener factores secundarios. Al adoptar el estándar VIP, las empresas pueden asegurar que los usuarios finales se beneficiarán de una experiencia simple y coherente en Internet. Al confiar la gestión del ciclo de vida de tokens a VeriSign, se elimina la carga de la gestión de tokens de segundo factor y de infraestructura.

Para proporcionar Shared Authentication Network (Red de autenticación compartida), hemos desarrollado un marco para compartir recursos e inteligencia entre los miembros de la red.

#### Funciones en la red

Existen dos funciones en la VIP Shared Authentication Network. Una empresa que genera credenciales Shared Authentication Network para sus clientes, se convierte en una entidad emisora de credenciales. Una empresa que permite a su usuario completar la autenticación mediante credenciales Shared Authentication Network se denomina *Parte de confianza*. Una empresa puede representar ambas funciones – generando credenciales a algunos usuarios y aceptando credenciales de terceras partes emitidas por otros. Una entidad emisora de credenciales puede incluir sus propios tokens, pero también puede incluir el logotipo de VIP Network. Una entidad emisora de credenciales es el primer punto de contacto de un usuario en la Red VIP.

La entidad emisora de credenciales es el punto de contacto con el usuario final. Los clientes contactan con la entidad emisora de credenciales para las preguntas de servicio al cliente de primer nivel, como problemas de sincronización y restablecimientos de PIN. VeriSign puede ayudar resolviendo problemas de mucha mayor entidad y opcionalmente, con todos los servicios de atención al cliente.

Si una empresa está comprometida con la autenticación fuerte, podrá emitir tokens que podrán utilizarse en la Red VIP. Las entidades emisoras de credenciales obtendrán todos los beneficios de las partes de confianza, además de costes inferiores por transacción, oportunidades de promocionar su marca a través del token y de un mayor control de la experiencia web de sus clientes finales. La Red VIP es una solución fácil para asegurar las webs de los usuarios actuales.

#### Compartir credenciales

Para fomentar la compatibilidad y la facilidad de uso, existen dos normas clave en la VIP Shared Authentication Network:

- Si una empresa emite credenciales de segundo factor a sus usuarios, acepta que esos usuarios utilicen las credenciales para identificarse en cualquier servicio de la red VIP.
- Una empresa miembro de la red VIP acepta la credencial de autenticación emitida por cualquier miembro de la red.

Resumiendo, si un usuario recibe una credencial que forme parte de la Red VIP, el usuario final reconoce que puede utilizar esa credencial como un segundo factor en cualquier sitio de la red.

#### VeriSign® Identity Protection Fraud Intelligence Network

Los delincuentes de Internet utilizan diferentes mecanismos para capturar información personal incluyendo sitios web de phishing, grabadores de las pulsaciones del teclado, comercios electrónicos falsos y robos de bases de datos. Con frecuencia, los delincuentes intentan utilizar la misma información en diferentes sitios web, probando información de inicio de sesión en procedimientos de ensayo y error, estableciendo múltiples cuentas fraudulentas u otras actividades malintencionadas. En el mundo real, los bancos y las empresas de tarjetas de crédito saben que los atacantes reutilizan la información robada y han establecido consorcios para compartir datos e identificar aplicaciones fraudulentas y cuentas de uso. Este mismo sistema se puede utilizar para detener el robo de identidades y las cuentas fraudulentas en Internet.

VIP Fraud Intelligence Network (VIP; Red de inteligencia frente al fraude de protección de la identidad de VeriSign), consiste en un mecanismo para compartir la inteligencia frente al fraude entre empresas y en Internet, y que se integrará en el servicio VIP Fraud Detection Service como opción de valor añadido. Engloba dos niveles de inteligencia compartida. El primer nivel incluye la ampliación del servicio VIP Fraud Detection Service para comparar patrones de conducta en tiempo real entre los sitios web participantes. VIP Fraud Intelligence Network puede contribuir a detectar y detener ataques que no podrían detectarse con los datos procedentes de un solo sitio. Para detectar el fraude, VIP Fraud Intelligence Network no necesita información de identificación personal, sino que puede utilizar seudónimos exclusivos imaginarios para identificar a los usuarios finales en los sitios web.

El segundo nivel de inteligencia compartida consiste en la implantación de inteligencia en el ámbito de Internet proporcionada por VeriSign derivada de las operaciones de la infraestructura de VeriSign. VeriSign utiliza la infraestructura DNS para toda Internet y mediante toda la experiencia que cosecha la inteligencia relacionada con las actividades de fraude en tiempo real que otros proveedores no disponen.

#### + VeriSign: un socio de confianza

Los servicios y la Red VIP están respaldadas por VeriSign, la empresa líder de servicios de seguridad por Internet. Actualmente, más de 34.000 sitios web lucen el logotipo VeriSign Secured Seal, que permite a los usuarios confirmar la identidad de los sitios de comercio electrónico. VeriSign es una de las marcas que inspiran más confianza entre los usuarios de seguridad por Internet.



VeriSign es un proveedor de servicios de confianza para terceras partes para una amplia gama de aplicaciones, que va desde la emisión de certificados SSL a sitios web de comercio electrónico, a proporcionar servicios de mensajería SMS entre operadores o a proporcionar servicios de información de códigos electrónicos de productos. Aportamos la misma experiencia a la Red VIP.

VeriSign gestiona múltiples servicios fundamentales para Internet y las redes de telecomunicaciones, incluyendo los registros de los dominios .com y .net, autoridades emisoras de certificados SSL y redes de señalización SS7. El personal de VeriSign cuenta con décadas de experiencia en la gestión de infraestructuras críticas, garantizando su seguridad y disponibilidad. VeriSign controla, gestiona y protege las redes de otras muchas instituciones financieras, utilidades, agencias gubernamentales y empresas mediante sus infraestructuras de Managed Security Services (servicios de seguridad gestionada). VeriSign supervisa la gestión de los servicios VIP, por lo que puede confiar plenamente en su seguridad y fiabilidad.

Por último, la división iDefense de VeriSign se encarga de investigar amenazas y vulnerabilidades nuevas. Además, los investigadores de iDefense controlan los foros de hackers en inglés, ruso, chino y otros idiomas. Utilizamos las investigaciones originales de iDefense para identificar nuevos métodos de fraude y mejorar el servicio VIP Fraud Detection Service.

Ninguna otra empresa le protegerá mejor contra el fraude ni protegerá a sus clientes del robo de identidades.

#### Inteligencia compartida y protección de la privacidad

Cuando una empresa entra a formar parte de la Red VIP, acepta a compartir sus recursos de inteligencia con el resto de miembros de la red para proteger a sus usuarios contra el fraude. VeriSign utiliza los datos de inicio de sesión de los clientes para ayudar a luchar contra el fraude. Para proteger la privacidad del usuario final, VeriSign no comparte directamente estos registros con los miembros de la red.

### + Servicios futuros

En la actualidad, VIP Services y VIP Network son servicios de inteligencia de autenticación simples, integrales y de bajo coste. Sin embargo, estamos trabajando en otras iniciativas para aumentar las funcionalidades de protección de identidad de VIP Services y VIP Network.

#### Identity Proofing Services

Cuando un usuario se registra por primera vez en un sitio web, el sitio web debe validar la identidad del usuario. Si el usuario no tiene una relación en el mundo real con el sitio web, puede ser una situación arriesgada. Los ladrones de identidad lo saben y con frecuencia abren cuentas utilizando nombres de terceras personas. El informe de FTC Clearinghouse ha detectado que más del 20% de los incidentes de fraude bancario, el 60% de tarjetas de crédito y el 95% del telefónico y de utilidades estaba relacionado con la creación de cuentas nuevas.

VeriSign anticipó que VeriSign® Identity Proofing Services (Servicios de acreditación de identidad, VIP IPS) estarían diseñados para ayudar a los sitios web a identificar a los usuarios cuando se registren para beneficiarse de nuevos servicios. VIP IPS realiza al usuario una serie de preguntas acerca de su identidad, de forma que deben demostrar quien dicen ser. Utilizando información de múltiples fuentes ajenas a Internet, VIP IPS confirma la identidad del usuario. Además, VIP IPS puede detectar intentos de registro sospechosos. Un sitio web puede realizar otras investigaciones posteriores para confirmar la identidad de un usuario, solicitando la confirmación ajena a Internet de la identidad del usuario antes de conceder acceso a servicios financieros, información de salud u otros datos.

#### Mutual Authentication Services (Servicios de autenticación mutua)

La autenticación de factores múltiples hace que los ataques diseñados para capturar las contraseñas de los usuarios finales, como phishing, grabadores de las pulsaciones del teclado o la interceptación de comunicaciones, hayan quedado obsoletas. Afortunadamente, estos son los ataques más frecuentes que utilizan los hackers en la actualidad. Sin embargo, los ataques de interposición (como los ataques “evil twin” (gemelo malintencionado) a configuraciones inalámbricas) están proliferando y pueden suponer un grave problema en el futuro.

VeriSign está trabajando actualmente con proveedores de navegadores para facilitar que los usuarios finales puedan distinguir con mayor facilidad los negocios legítimos de impostores. Los proveedores trabajan en nuevas interfaces que muestren más información acerca de un certificado digital de un sitio (como el logotipo de una empresa) en el navegador web. Los grupos industriales también trabajan en nuevas normativas que deban cumplir los usuarios poder conseguir los certificados de las entidades emisoras, de forma que los usuarios finales sepan en quién pueden confiar. Además, VeriSign colabora con entidades de normativas y estándares como OATH en el desarrollo de técnicas adicionales de autenticación de usuarios. Con la llegada de estos servicios, VeriSign piensa ampliar el conjunto de servicios VIP para ofrecer una experiencia aún más segura a los usuarios finales.

### + Más información

Los servicios de seguridad de VeriSign protegen las interacciones en línea, lo que permite a las empresas gestionar los riesgos relacionados con la reputación, la gestión y el cumplimiento de la normativa legal del modo más sencillo y económico posible. Si desea obtener más información acerca de VeriSign Identity Protection, llame al teléfono 900 93 1298 o envíe un correo electrónico a [ventas@verisign.es](mailto:ventas@verisign.es).

**Para obtener más información, visítenos en [www.verisign.es](http://www.verisign.es).**

2006 VeriSign Spain, S.L. Todos los derechos reservados. VeriSign, el logotipo de VeriSign, “Where it all comes together,” y otras marcas comerciales, marcas de servicio y diseños son marcas registradas o no registradas de VeriSign y sus subsidiarias en los Estados Unidos y otros países. El resto de las marcas comerciales son marcas registradas de sus respectivos propietarios.

00022322