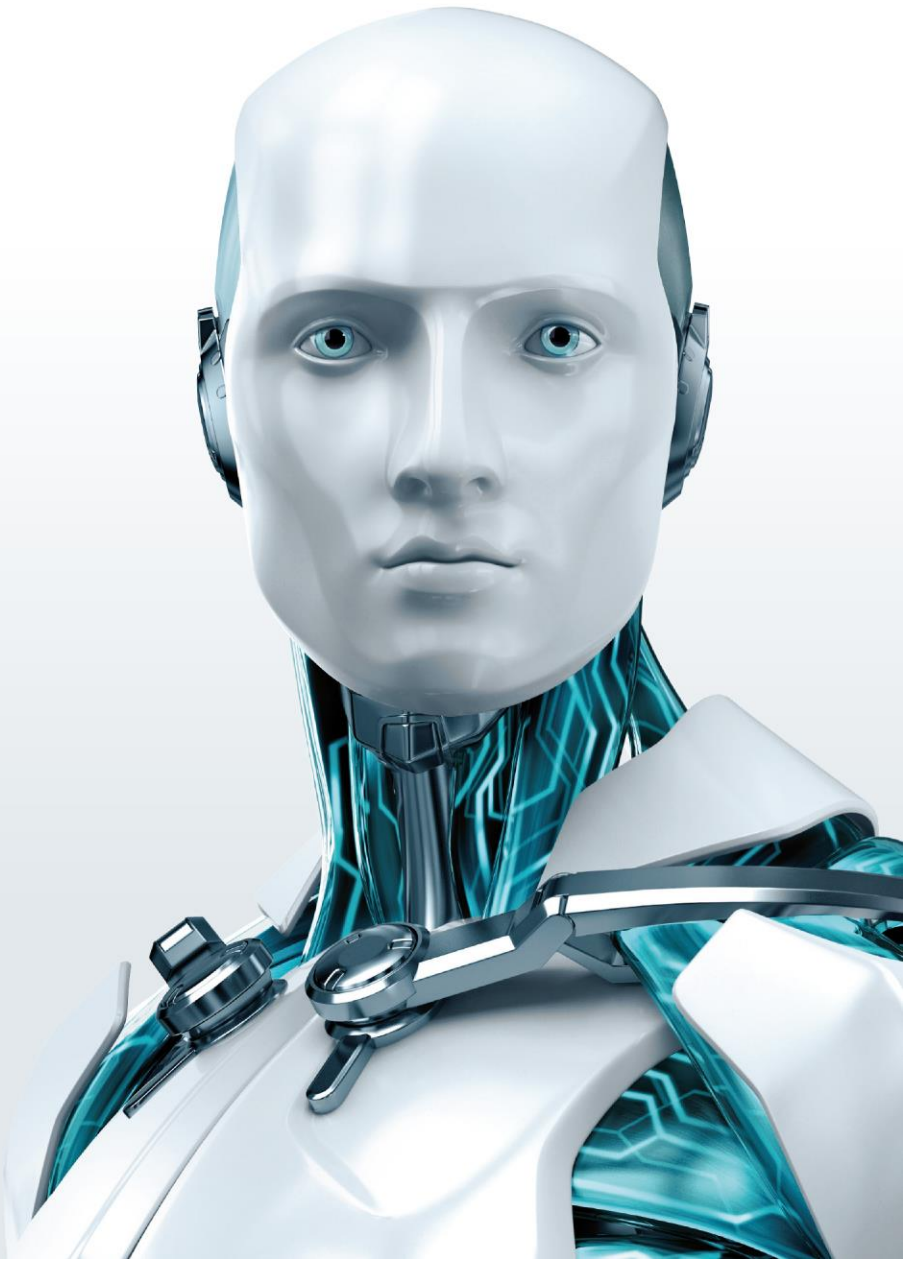
# ESET Secure Authentication

## Segundo factor de autenticación y cumplimiento de normativas



**Versión del documento 1.2**

6 de noviembre de 2013

www.eset-la.com

# Resumen: Segundo factor de autenticación y cumplimiento de normativas

| Región/País | Legislación/Normativa | ESET Secure Authentication cumple con el requisito explícito de la autenticación en dos fases | ESET Secure Authentication cumple con la necesidad de contar con una autenticación más fuerte |
|---|---|---|---|
| **Internacional** | Estándar ISO27001 | | ✓ |
| **Internacional** | PCI/DSS: Estándar de seguridad de datos para las tarjetas de pago | ✓ | |
| **Internacional** | ISAE 3402: Estándar internacional para trabajos de verificación nro. 3402 | | ✓ |
| **Estados Unidos de América** | HIPAA: Ley de portabilidad y responsabilidad de seguros médicos | | ✓ |
| **Estados Unidos de América** | FFIEC: Normativas del Consejo federal de certificación de instituciones financieras | ✓ | |
| **Estados Unidos de América** | Gobierno federal de los Estados Unidos de América | ✓ | |
| **Estados Unidos de América** | Ley de Sarbanes Oxley | | ✓ |
| **Reino Unido** | Código de conexión | | ✓ |
| **Sudáfrica** | PPI: Ley de Protección de datos de carácter personal | | ✓ |

## 1. Introducción

La necesidad de cumplir con las normas reglamentarias, de gobierno corporativo, de conformidad o de auditoría se convirtió en un hecho natural para la mayoría de las empresas que hacen negocios en el mundo corporativo dinámico de hoy en día. Muchas empresas se ven obligadas cada vez más a cumplir con las normas reglamentarias específicas que rigen en la empresa.

El presente documento pretende asistir a dichas empresas en este proceso respondiendo las siguientes preguntas:

- ¿A qué requisitos de cumplimiento de normativas puede estar sujeta la empresa?
- ¿Qué tienen que decir estos requisitos sobre la autenticación en dos fases?

El propósito es trazar una ruta a seguir sobre cómo puede aprovecharse fácilmente ESET Secure

Authentication para cumplir con las diversas normas de gobierno corporativo, y así elevar el cumplimiento de estándares.

# 2. Requisitos de cumplimiento de normativas

## Estándar ISO27001 (internacional)

La sección sobre el control del acceso en el código de buenas prácticas para la gestión de la seguridad de la información ISO 27002 describe los requisitos para el control del acceso desde conexiones de redes externas. Queda claro que esta norma de conformidad considera las conexiones externas como un riesgo significativo que requiere controles deliberados para proteger el acceso remoto. ESET Secure Authentication mejora considerablemente la adherencia del cliente a este requisito.

*11 Control de accesos*
*11.4 Control del acceso a la red*
*b) se aplican mecanismos de autenticación adecuados para usuarios y equipos;*
*11.4.2 Autenticación de usuarios para conexiones externas*
*Control: Deberían usarse métodos de autenticación adecuados para controlar el acceso de usuarios remotos.*
*Guía de implementación: La autenticación de usuarios remotos se puede lograr utilizando, por ejemplo, una técnica basada en cifrado, tokens de hardware o un protocolo desafío/respuesta. Las posibles implementaciones de dichas técnicas se pueden encontrar en diversas soluciones para redes privadas virtuales (VPN).*

**La sección sobre controles de acceso físicos de entrada es más explícita:**

*11.1.2 Controles físicos de entrada*
*[…] el acceso a áreas donde se procesa o almacena información confidencial debe estar restringido únicamente a individuos autorizadas a través de la implementación de controles de acceso apropiados, por ej., mediante la implementación de un mecanismo de autenticación en dos fases […]*

## PCI/DSS: Estándar de seguridad de datos para las tarjetas de pago (internacional)

El Estándar de seguridad de datos para las tarjetas de pago es el más explícito sobre la 2FA:

*Requisito 8: Asignar una identificación única a cada persona con acceso al equipo*

*8.3 Incorporar autenticación en dos fases para otorgarles acceso remoto (acceso en el nivel de la red originado*

*desde fuera de la red) a la red a empleados, administradores y terceros. (Por ejemplo, servicios de autenticación remota de llamadas de usuarios (RADIUS) con tokens; sistema de control de acceso mediante el control del acceso desde terminales (TACACS) con tokens; u otras tecnologías que faciliten la autenticación en dos fases).*

Nota: La autenticación remota requiere el uso de dos de los tres métodos de autenticación. El uso de un mismo factor dos veces (por ejemplo, dos contraseñas separadas) no se considera autenticación en dos fases.

**¿Cuándo se requiere la autenticación en dos fases?**

Todos los accesos remotos a la red en conformidad con el estándar PCI deben utilizar autenticación en dos fases. En términos simples, el acceso remoto se puede interpretar como cualquier conexión o acceso que cruce las redes públicas. Si alguna de las redes que se encuentran entre la fuente de acceso y el Entorno de datos de titulares de tarjetas (CDE) se considera pública o perteneciente y operada por otra entidad, el acceso debe considerarse remoto. Las tecnologías para las redes privadas virtuales (VPN) crean algunas excepciones interesantes, donde efectivamente provocan que redes remotas se comporten como redes locales.

A efectos de la disposición 8.3, las tecnologías VPN de punto a punto pueden considerarse accesos de red local, y el Acceso remoto o las tecnologías VPN de clientes deberían considerarse remotos. En ambos casos, quizá necesite hacer una revisión adicional para asegurarse de que los controles cumplen adecuadamente con los requisitos de utilizar autenticación en dos fases para el acceso remoto al CDE.

**Conceptos erróneos comunes**

Una idea equivocada frecuente sobre el Requisito 8.3 se puede ver en la interpretación y definición del término “autenticación en dos fases”. Algunas organizaciones interpretan la autenticación en dos fases como dos identificadores de autenticación aplicados independientemente a dos solicitudes de autenticación diferentes. En estos casos, cada solicitud de autenticación solo usa un único identificador de autenticación. Pero dos pasos de autenticación en una fase no equivalen a la autenticación en dos fases.

Otro error frecuente es que el Requisito 8.3 incluye todo el acceso al CDE, no solo el acceso remoto. En estos casos, las organizaciones pueden desplegar mecanismos de autenticación en dos fases para autenticar las solicitudes de acceso desde todas las redes conectadas, incluyendo aquellas que están conectadas a nivel local. Aunque esto excede el alcance del requisito 8.3, puede mejorar y proteger aún más el acceso al CDE.

Aunque la incorporación de pasos adicionales de autenticación puede mejorar la seguridad general de los mecanismos de acceso remoto, la mejora no equipara la mayor seguridad proporcionada por un mecanismo de autenticación en dos fases auténtico. El propósito del requisito 8.3 es asegurar que se utilicen dos identificadores de autenticación dentro de una misma solicitud de autenticación.

## ISAE 3402: Estándar internacional para trabajos de verificación nro. 3402 (internacional)

El Estándar internacional para trabajos de verificación (ISAE) nro. 3402, Informes que proporcionan un grado de seguridad sobre los controles en una organización de servicios, se desarrolló para proporcionar un estándar internacional de verificación que les permitiera a los contadores públicos emitir un informe para que lo utilicen las entidades usuarias y sus auditores sobre los controles en una organización de servicios que probablemente tengan un impacto o sean parte del sistema interno de control por estar relacionadas con la información financiera.

Es probable que los clientes de ESET Secure Authentication que son "organizaciones de servicios" y les proporcionan a sus clientes servicios asociados a TI deban implementar controles para cumplir con una auditoría ISAE 3402. El control del acceso suele ser típicamente la consideración clave de esta auditoría. La autenticación en dos fases en el acceso externo mejora la capacidad de la organización de servicios de este tipo para obtener una opinión favorable en la auditoría.

## HIPAA: Ley de portabilidad y responsabilidad de seguros médicos (Estados Unidos de América)

Un grupo asesor federal estadounidense recomendó en ciertos casos la autenticación en varias fases para el Nivel 3 de la Ley de HITECH: programa de incentivos para historiales médicos electrónicos, que también reglamenta los servicios de TI bajo HIPAA.

El Nivel 3 tiene previsto comenzar en 2015 y las reglas se encuentran en la etapa inicial de discusión en el Departamento de salud y servicios sociales.

## FFIEC: Normativas del Consejo federal de certificación de instituciones financieras (Estados Unidos de América)

El Consejo federal de certificación de instituciones financieras estadounidense es un organismo interinstitucional con la facultad de establecer principios y estándares uniformes así como formularios de informes para la certificación federal de instituciones financieras por el Comité de Gobernadores del Sistema de Reserva Federal, la Corporación Federal de Seguros de Depósito, la Administración Nacional de Cooperativas de Crédito, la Oficina de Contralor de la Moneda y la Agencia de Protección Financiera del Consumidor, y hacer recomendaciones para promover la uniformidad en la supervisión de las instituciones financieras.

En conformidad con la publicación del FFIEC donde se aconseja usar la autenticación en varias fases, muchos fabricantes comenzaron a ofrecer soluciones de autenticación que no cumplen con la definición del FFIEC de una "verdadera autenticación en varias fases". El más notable de estos enfoques es el de desafío/respuesta, generalmente acompañado por una imagen secreta compartida. La solicitud de información personal como respuesta a preguntas de desafío simplemente agrega más elementos "conocidos por el usuario", lo que es similar a un inicio de sesión, una contraseña o un código de identificación personal. Todas éstas son distintas soluciones que pertenecen a la misma categoría de autenticación. A menos que se combinen con uno de los otros dos factores, es decir, "algo que el usuario tiene en su poder" o "algo que el usuario es", no constituyen autenticación en varias fases.

Los organismos reguladores reiteradamente advirtieron sobre el uso de enfoques que funcionan mediante la solicitud de información personal. El 17 de junio de 2005, la Corporación Federal de Seguros de Depósito (FDIC) estadounidense publicó guías complementarias donde se advierte firmemente a las organizaciones financieras sobre la adopción de métodos de autenticación que usan información personal para autenticar usuarios:

"Aunque a los consumidores les preocupa el phishing y la confiabilidad de los mensajes de correo electrónico enviados por el banco, también les preocupa con mayor frecuencia la seguridad de su información personal. [...] Cuando los bancos piensan en los métodos de autenticación para clientes minoristas, deberían recordar que esos clientes valoran la seguridad y la protección de la información confidencial... Los consumidores requerirán una clara explicación de todos los mecanismos de seguridad y del uso de toda la información personal requerida para implementarlos. [...] Las limitaciones en el uso de la información personal y la existencia de protección privada son elementos importantes para la aceptación del consumidor. [...] A los consumidores también les preocupa el riesgo asociado a las grandes bases de datos con información personal y la posibilidad de que la información utilizada por los métodos de autenticación se vea comprometida, se copie o se imite. - FDIC"

El FFIEC clarificó su posición en el Suplemento de preguntas frecuentes publicado el 15 de agosto de 2006, donde rechazó firmemente esos enfoques:

"Por definición, la verdadera autenticación en varias capas requiere el uso de soluciones que correspondan a dos o más categorías de factores. El uso de varias soluciones pertenecientes a la misma categoría [...] no constituye una autenticación en varias capas. - FFIEC"

## Gobierno federal de los Estados Unidos de América (Estados Unidos de América)

Las normas reglamentarias de TI para el acceso a sistemas del Gobierno Federal requieren el uso de autenticación en dos fases para acceder a recursos confidenciales de TI, por ejemplo, cuando se inicia la sesión a dispositivos de la red para llevar a cabo tareas administrativas y cuando se accede a cualquier equipo usando un acceso con privilegios.

## Ley de Sarbanes Oxley (Estados Unidos de América)

Las normativas establecidas por la Ley de Sarbanes-Oxley (SOX) requieren que las organizaciones usen métodos más fuertes de autenticación para mitigar el robo de datos, evitar fraudes, y proteger la información de los clientes y la privacidad de los pacientes.

## Código de conexión (Reino Unido)

El segundo factor de autenticación ayuda a organizaciones en Reino Unido (por ej., ayuntamientos) a cumplir con los requisitos del "Código de conexión" que es requerido por los servicios gubernamentales en línea como la Extranet segura del gobierno de Reino Unido.

## PPI: Ley de Protección de datos de carácter personal (Sudáfrica)

La ley sudafricana PPI establece:

Principio 7 Garantías de seguridad
Medidas de seguridad sobre la integridad de la información personal
18. *(1) La parte responsable debe proteger la integridad de la información personal que tenga en su posesión o que esté bajo su control mediante la toma de las medidas técnicas y de gestión apropiadas y razonables para prevenir:*
*(b) el acceso ilegal a la información personal o su procesamiento.*

*(2) Para que tenga efecto la Subsección (1), la parte responsable deberá tomar medidas razonables para:*
*(b) establecer y mantener las precauciones apropiadas contra todos los riesgos identificados;*

Se puede argumentar que, dada la debilidad de los sistemas protegidos solamente por una contraseña en el panorama actual de TI (particularmente en lo que concierne a la reutilización de la misma contraseña), una organización responsable debe implementar 2FA (entre otras medidas) para reducir los riesgos que atentan contra la información personal bajo su control.