Seguridad de Correo Electrónico

El uso de Firmas Digitales y Cifrado

GlobalSign

Contenidos

Introducción 03

La necesidad de la seguridad 04
En correos electrónicos

Firmas digitales y cifrado, 07
Conceptos básicos

Firmas digitales y cifrado 10
En acción

Seleccione la mejor solución de correo 15
electrónico para usted

Conclusión 17

Introducción.

¿Puede imaginarse haciendo negocios sin Correo electrónico? La conveniencia y la comunicación instantánea que el correo electrónico ofrece ha hecho de la comunicación electrónica un componente esencial del día a día de los negocios. Mas de 100 billones de correos electrónicos relacionados a actividades comerciales son enviados y recibidos diariamente[1]

Además de ofrecer muchos beneficios los correos electrónicos también poseen algunos riesgos. Los hackers son cada vez mas hábiles en sus ataques a organizaciones mediante el uso de mensajes electrónicos, incluyendo la interceptación para conseguir información confidencial o la falsificación de correos electrónicos (email spoofing) con la intención de direccionar a sitios webs con phishing o provocar descargas maliciosas.

Afortunadamente, hay algunas soluciones para correo electrónico que pueden ayudar a protegerlo a usted y a su organización de estas amenazas. Las firmas digitales de correo electrónico y el cifrado garantizan la privacidad del mensaje y evitan que la información confidencial caiga en las manos equivocadas. A la vez le asegura al receptor que el correo en verdad proviene de usted y que este no ha sido alterado desde que fue enviado.

Esta guía introductoria explica la necesidad de la seguridad para el correo electrónico en las organizaciones modernas. Nosotros nos enfocaremos en los riesgos de usar correos electrónicos, exploraremos como firmar digitalmente e encriptar los mensajes pueden ayudar a reducir estos riesgos, explicaremos también como usted debe firmar y cifrar los correos electrónicos.

Comencemos.

Capítulo 1.

La necesidad de la seguridad en correos electrónicos

Los riesgos de usar correos electrónicos

El correo electrónico es conveniente, pero a su vez posee riesgos. Miremos de forma más detallada dos de las principales amenazas a las que se enfrentan la organización y los usuarios finales.

Pérdida de la información

El correo electrónico es una herramienta de la cual dependemos diariamente. A su vez es muy fácil enviar información confidencial a otra persona, poniendo en riesgo que esta información caiga en las manos equivocadas.

53% *de los empleados ha recibido información organizacional confidencial no cifrada vía correo electrónico o como documento adjunto en un correo electrónico*[2]

21% *de los empleados reportaron el envió de información confidencial sin haber sido cifrada*[2]

Los costos de la perdida de la información son asombrosos, sin mencionar el daño que esto le hace a la reputación de la compañía y las repercusiones legales por violar las regulaciones relacionadas a la transmisión y el almacenamiento de la información sensitiva (Por ejemplo HIPPA, FIPPA, PCI).

22% *de las compañías experimenta perdida de información mediante correo electrónico cada año*[3]

$3.5 millones de Dólares *es el costo promedio de un ataque a la información de una compañía*[4]

Falsificación de correos (Email spoofing) / Phishing

El envió de coreos electrónicos desde una dirección de correo electrónico falsa, llamado spoofing de correo electrónico, es uno de los métodos más populares para llevar a cabo un ataque de phishing. Un hacker falsificara un email para que parezca que se trata de una compañía legítima (Por ejemplo un Banco) por lo general con la intención de engañar a los destinatarios para que descarguen malware o entren información confidencial en un sitio web falso, al cual el hacker podrá acceder.

El phishing es una amenaza creciente para las organizaciones modernas.

1/392 *Es la frecuencia de los ataques de phishing en correos electrónicos*[5]

300% *es la tasa de crecimiento de correos electrónicos que contienen phishing en el último año*[6]

Los hackers son cada vez más hábiles en hacerse pasar por otras organizaciones. Incluso personas con altos conocimientos en seguridad pueden ser engañados por un correo electrónico bien elaborado que contiene phishing.

33% *de los ejecutivos de las compañías Fortune 500 han caído en trampas de correos de phishing*[7]

Como las firmas digitales y la encriptación pueden ayudar

Afortunadamente, hay una solución para ayudar a mitigar las amenazas mencionadas anteriormente. La firma digital y el cifrado de correos electrónicos son una forma fácil de asegurar la privacidad de la información confidencial, comprobar el origen del correo y prevenir la manipulación del contenido.

Capítulo 2.

Firmas Digitales y Cifrado, conceptos básicos

¿Que es un certificado digital?

Usted necesita un certificado digital para firmar digitalmente y cifrar un correo electrónico, por lo cual creemos que lo mejor es comenzar entendiendo su significado. Los certificados digitales pueden ser usados para una variedad de casos, incluyendo SSL y firma de documentos, pero por motivos de simplicidad nos enfocaremos en como estos aplican para la seguridad de los correos electrónicos.

Usted puede pensar en un certificado digital como una especie de pasaporte virtual – una manera de verificar su identidad en transacciones en línea. Así como su Gobierno local necesita verificar la identidad antes de otórgale un pasaporte, una entidad de verificación conocida como Autoridad Certificadora (AC) necesita validar cierta información antes de emitir certificados digitales. El certificado es único para cada persona, siendo usado para firmar correos electrónicos, es una forma para que usted verifique que el mensaje en realidad proviene de usted.

¿Qué es S/MIME?

Es posible que usted haya escuchado el termino S/MIME cuando estaba buscando información sobre firmas de correo electrónicos y cifrado. S/MIME, o Segura/ Extensión de Multipropósito para Correo de la Internet, es el estándar en la industria para el cifrado de llave publica para información basada en MIME S/MIME ofrece dos funciones de seguridad de correo electrónico:

- Firmas Digitales
- Cifrado

Miremos de forma más detallada lo que cada uno de estos componentes ofrece.

¿Qué es una firma Digital?

La aplicación de una firma digital a un correo electrónico es muy similar a la vieja tradición de utilizar un sello de cera cuando se enviaban cartas. El destinatario de la carta sabia quien envió la carta debido al uso del sello único. Cuando usted usa su certificado emitido por una Autoridad Certificadora para verificar la firma de correo electrónico, el destinatario sabe que el correo electrónico realmente viene de usted.

¿Por qué debo firmar digitalmente mis correos electrónicos?

Cuando usted firma digitalmente un correo electrónico, una operación criptográfica enlaza su certificado digital y el contenido del correo electrónico en una huella digital única. La singularidad de los dos componentes de la firma – su certificado y el contenido del correo electrónico- ofrece los siguientes beneficios en seguridad:

Único a la persona que firma

Autenticación – cuando su certificado (validado por una Autoridad Certificadora) es usado para firmar un correo, los destinatarios tendrán la seguridad de que fue usted quien firmó el documento. Confirmando su identidad.

Único al documento

Integridad en el mensaje – Cuando la firma es verificada, esta confirma que el contenido del correo electrónico en el momento de la verificación sea igual al que estaba en el momento en el cual la firma fue aplicada. Hasta el cambio más minino del contenido en el documento original causará que esta parte falle.

¿Por qué debo cifrar mis correos electrónicos?

Cifrar un correo electrónico es como sellar su mensaje en una caja de seguridad a la cual solo el destinatario tiene acceso. Cualquier persona que intercepte el mensaje, ya sea en tránsito o en el servidor donde se encuentre almacenado, no será capaz de ver el contendió.
El cifrado de correos electrónicos ofrece los siguientes benéficos en seguridad:

Confidencialidad – debido a que el proceso de cifrado requiere información particular del remitente y de los destinatarios, solo ellos pueden ver los contenidos no cifrados.

Integridad del Mensaje - Parte del proceso de descifrado implica la verificación del contenido del correo cifrado original y el nuevo correo descifrado deben de ser iguales. Incluso el mas mínimo cambio en el mensaje original causará que el proceso de descifrado falle

Nota: el cifrado por sí solo no proporciona ninguna información sobre el remitente del mensaje. Recomendamos siempre incluir una firma digital cuando cifre un correo electrónico para probar la identidad del remitente.

Capítulo 3.

Firmas Digitales y Cifrado en Acción

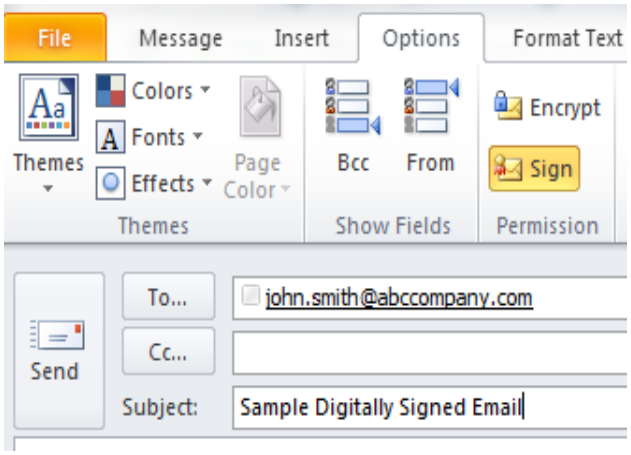
¿Qué necesito para firmar digitalmente y cifrar correos electrónicos?

1. Un certificado digital emitido por una Autoridad Certificadora compatible con S/MIME.
2. Un proveedor de correo electrónico compatible con S/MIME. La mayoría de los proveedores de correos electrónicos soportan S/MIME incluyendo:

- Microsoft Outlook
- Thunderbird
- Apple Mail
- Lotus Notes
- Mulberry Mail

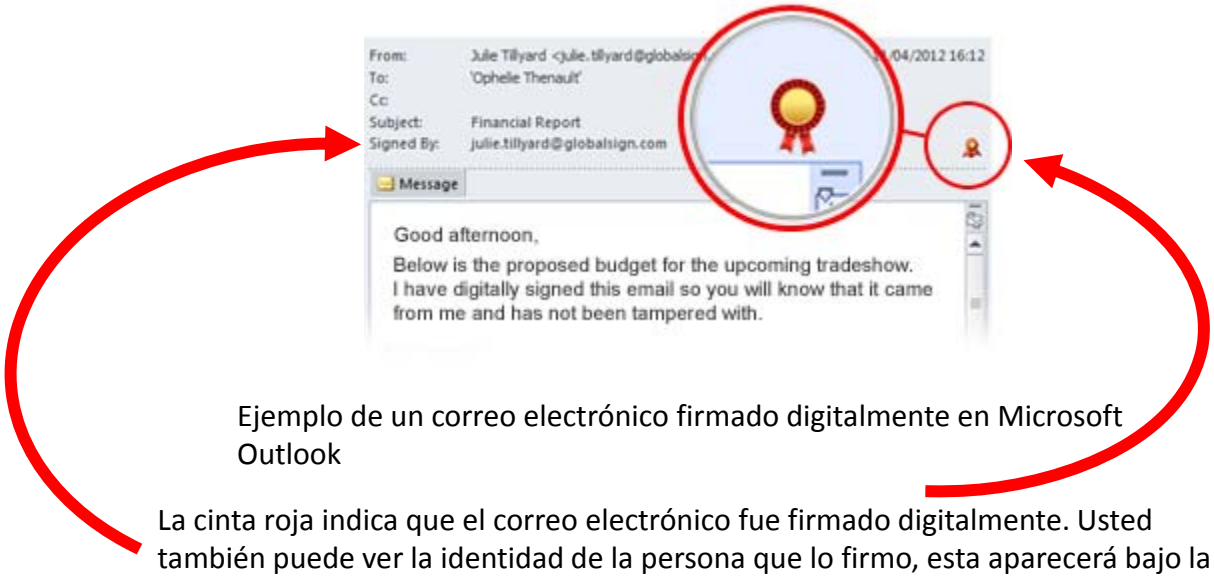
¿Cómo firmar digitalmente un correo electrónico

Para la mayoría de los proveedores de correos electrónicos, firmar digitalmente un correo electrónico es tan simple como darle clic a un botón. Muchos también ofrecen la opción de firmar digitalmente todos los mensajes que sean enviados.



Como se agrega una firma digital a un correo electrónico en Microsoft Outlook

¿Como un correo electrónico firmado digitalmente se debe ver?

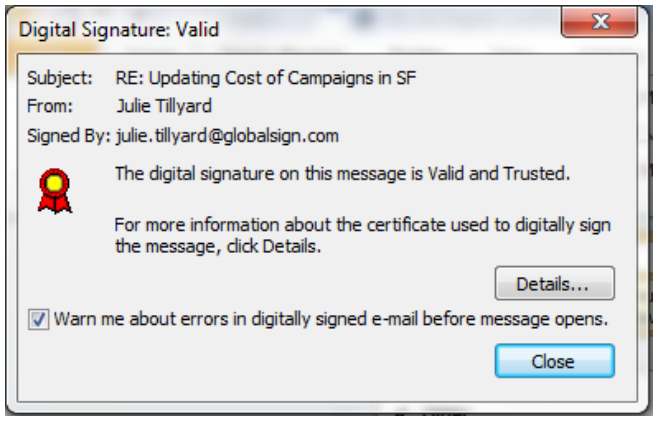


Ejemplo de un correo electrónico firmado digitalmente en Microsoft Outlook

La cinta roja indica que el correo electrónico fue firmado digitalmente. Usted también puede ver la identidad de la persona que lo firmo, esta aparecerá bajo la línea del asunto.
El destinatario del mensaje puede ver instantáneamente que el correo electrónico se firmó digitalmente y quien lo firmo. Él o ella pueden estar seguros de que el correo electrónico procede en realidad de la persona correcta y no ha sido falsificado, y que el contendió del correo no se ha cambiado desde su envió.

Dándole clic en la cinta roja va a verifica la validad de la firma y a la vez ofrece la opción de conseguir más detalles acerca del certificado que fue usado para ser firmado.

.

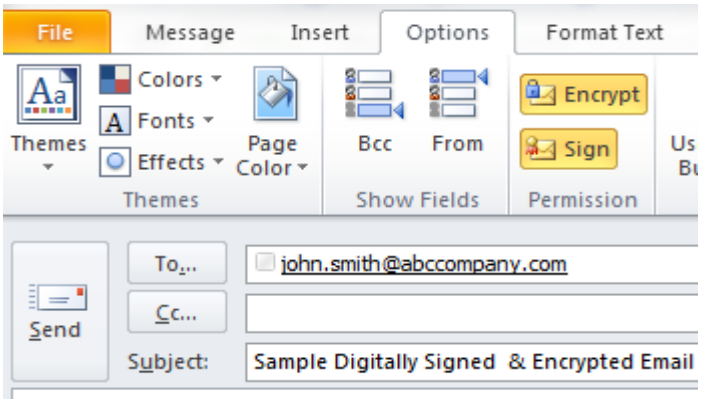


Detalles de la firma digital vistos desde Microsoft Outlook

.

¿Cómo cifrar un correo electrónico?

Muy parecido a firmar digitalmente un correo electrónico, el cifrado de un correo electrónico es usualmente tan simple como darle clic a la opción de cifrado en su proveedor de correo electrónico.



Como cifrar un correo electrónico usando Microsoft Office

De todas formas, hay una diferencia clave entre cifrado y firmas digitales.

Para enviar un correo electrónico cifrado, el destinatario debe también tener un certificado digital y las dos partes implicadas necesitan intercambiar llaves públicas (Parte de su certificado Digital).

Esto se debe al proceso criptográfico que tiene lugar durante el cifrado. La llave privada del remitente y la llave pública del destinatario son utilizadas para cifrar el contenido del correo electrónico, por lo cual necesitara las llaves con el fin de iniciar el proceso de cifrado

Si el usuario ya ha recibido un correo electrónico firmado digitalmente por el destinatario, él ya tiene la llave pública (ya que esta está incluida en la firma). Si no es así, deberá pedirle al destinatario que envié un correo electrónico firmado digitalmente.

Para más detalles sobre la criptografía de llave publica, el papel de las llaves públicas y privadas y como se utilizan en las firmas digitales y en el cifrado, consulte nuestro articulo relacionado http://www.globalsign.com/ssl-information-center/what-is-public-keycryptography.html

¿Cómo se ve un correo electrónico cifrado?

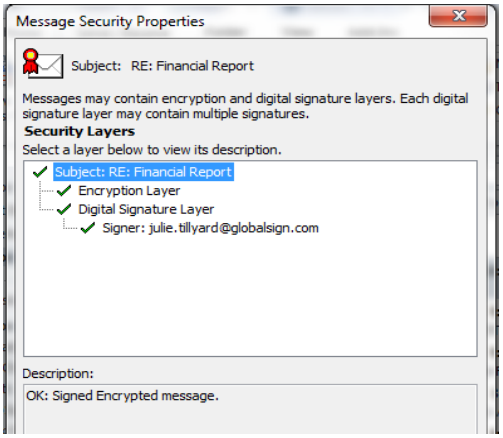
Ejemplo de un correo electrónico firmado digitalmente y cifrado visto en Microsoft Outlook

En este caso la cinta roja también indica que el correo electrónico fue firmado digitalmente y la identidad de la persona que firma aparece en la línea del asunto. También puede ver un candado lo que indica que el correo electrónico ha sido cifrado.

El destinatario del mensaje puede ver instantáneamente que el correo electrónico fue firmado digitalmente, que él o ella lo firmo, y que ha sido cifrado. Él o ella pueden estar seguros de que el correo electrónico en realidad procede de la persona correcta y no fue alterado, que el contenido no ha sido cambiado desde que fue enviado, y que el contenido no es visible para otras personas.

Al hacer clic en el candado este verifica que el correo electrónico ha sido cifrado y proporciona la opción de ver más detalles sobre el certificado digital utilizado para firmar y cifrar el correo.

.



Detalles de la firma digital vistos en Microsoft Outlook.

Capítulo 4.

Seleccione la mejor solución de Seguridad de correo electrónico para usted

¿Qué tipo de seguridad de correo electrónico debo de usar?

Es claro que las firmas digitales y el cifrado de correo electrónico pueden ayudarlo a mitigar las amenazas digitales como caer en la trampa de correos falsos (email spoofing) y la perdida de información, pero usted puede estarse preguntando si esta es la mejor solución de correo electrónico para usted. Hay muchos tipos de soluciones de seguridad de correos electrónicos y organizaciones que ofrecen este tipo de productos en el mercado, nosotros nos hemos tomado la tarea de recopilar algunas preguntas que se deben tener en mente cuando analice sus opciones.

- ¿Usted necesita enviar información sensitiva vía correo electrónico?
- ¿Qué tipo de regulaciones usted necesita seguir? (Por ejemplo, HIPPA; FIPPA; PCI regulaciones enfocadas a la trasmisión de información confidencial)
- ¿Ha sido su organización víctima de email spoofing u otro tipo de ataques Phishing?
- ¿Cómo la solución autenticara a la persona que envía el correo electrónico?
- ¿La solución asegura que el contenido de los correos no sean alterados después de que estos son enviados?
- ¿Cómo es el proceso de implementación? ¿ Sera fácil de implementar para el equipo de TI?
- ¿Esta solución será fácil de adoptar para usted y para otros usuarios en su organización?
- ¿Qué tipo de proveedor de correos electrónicos usted usa?

Hay muchas cosas que se deben de tener en cuenta cuando se esté analizando las posibles soluciones, pero nadie conoce su compañía mejor que usted. Sus mayores preocupaciones (Phishing, perdida de información, etc.), su infraestructura de correo electrónico, regulaciones que usted necesite cumplir, todos estos son factores únicos a su organización y son las que determinarán cual solución es la mejor para usted. Cada organización va a tener sus propios requerimientos y prioridades, esperamos que las preguntas formuladas anteriormente le ayuden a tener una idea clara al momento de evaluar sus opciones.

Conclusión.

A medida que las comunicaciones vía correo electrónico sigan creciendo, el riesgo de usarlo seguirá en aumento. Con amenazas como el Phishing y la pérdida de información creciendo diariamente, la seguridad electrónica debe ser prioridad para todas las empresas.

Usted ya conoce los riesgos de usar correo electrónico. Usted ha aprendido como las firmas digitales y el cifrado pueden ayudarlo a mitigarlos. Usted ya posee el conocimiento para comparar soluciones de seguridad de correos electrónicos. Entonces, ahora es hora de implementar un plan de seguridad de correos electrónicos para su empresa.

¿Tiene preguntas? Nosotros tenemos las respuestas.

www.globalsign.com | contacto@globalsign.com

Referencias.

[1] Email Statistics Report 2013-2017, The Radicati Group, Inc.

[2] SilverSky Email Security Habits Survey Report, SilverSky, 2013

[3] Best Practices in Email, Web, and Social Media Security, Osterman Research, Inc., January 2014

[4] Global Cost of Data Breach Study, Ponemon Institute, 2014

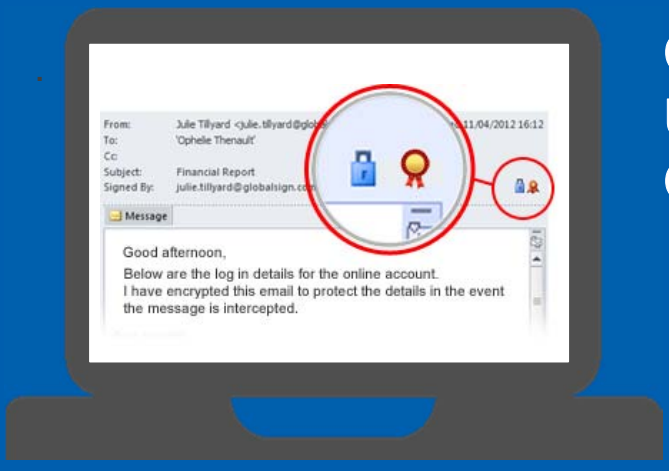
[5] Internet Security Threat Report, Volume 19, Symantec, 2014

[6] Spam Statistics Report, Kaspersky Lab, Quarter 3 2013

[7] A Security Officer Debate: Are simulated phishing attacks an effective approach to security awareness and training?, Wombat Security Technologies, 2013

GlobalSign hace posible que usted firme digitalmente y cifre sus correos electrónicas de forma fácil

Firmar digitalmente y cifrar sus correos electrónicos prueban el origen del correo electrónico, previenen la manipulación del mensaje, y protegen que la información confidencial caiga en las manos equivocadas. Regístrese para una demostración de la solución de GlobalSign de firma y cifrado de correos electrónicos para que se dé cuenta que tan fácil la seguridad de correos electrónicos puede ser.



CONTACTENOS PARA UNA DEMOSTRACIÓN GRATIS.

Nos puede contactar vía Telefónica al número +1-603-570-7076

O por correo electrónico contacto@globalsign.com

GlobalSign®