

INFORME TÉCNICO EVALUACIÓN DE SOFTWARE DE CIFRADO Y FIRMAS DIGITALES

1. NOMBRE DEL AREA

UNIDAD DE OPERACIONES - OFICINA DE SOPORTE TÉCNICO (UO - OST)

2. RESPONSABLES DE LA EVALUACIÓN

Ing. Oliver Aguilar Torres

3. CARGO

Administrador de Base de Datos

4. FECHA

06 de febrero 2007

5. PROPÓSITO

Adquirir 5 Licencias de software para cifrado datos y generación de firmas digitales para la Dirección Ejecutiva.

6. JUSTIFICACION

Al respecto, se recomienda la adquisición de dichas licencias, debido a lo siguiente:

- Es necesario que la información que se envía y recibe al más alto nivel de la institución viaje de manera encriptada y firmada, con lo que se asegura la autenticidad, integridad y confidencialidad de los datos.
- Es así, que se requiere utilizar algún software que permita la encriptación de los datos y la firma de documentos, y de esta manera hacer que la comunicación generada por la Dirección Ejecutiva, esté debidamente protegida.

7. ANÁLISIS DE LAS PROPUESTAS DE SOLUCIÓN EVALUACIÓN COMPARADA DE LAS HERRAMIENTAS DE CIFRADO Y FIRMAS DIGITALES

Actualmente en el mercado existen dos herramientas que se considera conveniente evaluar a fin de definir una solución:

- PGP
- GPG

OBJETIVO GENERAL

Proporcionar la mejor protección de seguridad a la información que se envía y recibe en la Dirección Ejecutiva de la DINI.

OBJETIVOS ESPECÍFICOS

- Implementar una herramienta que permita a la Dirección Ejecutiva cifrar los datos que viajan por la red interna de la Institución.
- Implementar una herramienta que permita generar firmas digitales, con lo que se garantiza la autenticidad de la persona que género o envió un documento.

PRODUCTOS A EVALUAR

El producto a evaluar es un programa que cifra los datos, mediante un método llamado criptografía de clave pública, así como también facilita la autenticación de documentos mediante el empleo de firmas digitales.



En el mercado existen dos productos que utilizan los mismos mecanismos y métodos de cifrado de datos:

- PGP (Pretty Good Privacy)
- GPG (GNU Privacy Guard)

La IETF se ha basado en el diseño de PGP para crear el estándar de Internet OpenPGP.

A diferencia de protocolos de seguridad como SSL, que sólo protege los datos en tránsito (es decir, mientras se transmiten a través de la red), PGP también puede utilizarse para proteger datos almacenados en discos, copias de seguridad, etcétera.

GPG o es una herramienta para cifrado y firmas digitales, que viene a ser un reemplazo del PGP pero con la principal diferencia que es software libre licenciado bajo la GPL. GPG utiliza el estándar del IETF denominado OpenGPG.

CONSIDERACIONES PREVIAS

Es importante mencionar que la herramienta PGP es posible adquirirla con la compra de licencias, por lo que se encuentra garantizado su correcto uso, por la PGP Corporation. Por otro lado, GPG es una herramienta que utiliza los mismos métodos de cifrado que PGP, y su uso no requiere de la compra de licencias, puesto que se encuentra bajo licenciamiento GPL (Open Source), pero no se cuenta con el respaldo ni la garantía de ninguna empresa que responda ante cualquier problema que ocurra con el producto.

FUNCIONALIDAD DE LA HERRAMIENTA

La herramienta debe contener las siguientes funcionalidades:

- **Whole Disk** asegura la totalidad del sistema. Previene acceso no autorizado y elimina el riesgo de robo y extracción de información almacenada.
- **Virtual Disk** asegura archivos, directorios, dispositivos USB y CD. Previene acceso no autorizado a dispositivos móviles y fijos elimina el riesgo de robo y extracción de información almacenada en caso de pérdida o robo.
- **Mail** encripta automáticamente y firma digitalmente los mensajes de e-mail y archivos adjuntos o attachments. Se busca mantener la confidencialidad de ésta información durante su envío/recepción, transporte y almacenamiento. Asimismo, permite establecer la integridad de la información.
- **Secure Messenger** protege las sesiones AOL® IM.
- **Zip** comprime automáticamente y encripta mensajes, datos adjuntos y archivos. Permite almacenar, transportar y compartir información de forma segura.
- **Shred** provee el borrado permanente e ilegible de información.

9. ANÁLISIS COMPARATIVO DE VALORES DE MERCADO, COSTO

Como se detalla a continuación:

Nº	Producto	Precio	Cantidad	Total
1	PGP	249.00	5	1,245.00
2	GPG	00.00	5	00.00

Nota: los precios no incluyen IGV y están expresados en dólares Americanos.



10. BENEFICIOS

La Herramienta protege la información confidencial en el e-mail y archivos, asegura los datos en la computación móvil, facilita el cumplimiento con regulaciones de seguridad de la información existentes y emergentes, y permite a la Institución cumplir a nivel de usuario con los requerimientos de seguridad de la información.

11. COMENTARIOS FINALES A LA EVALUACIÓN

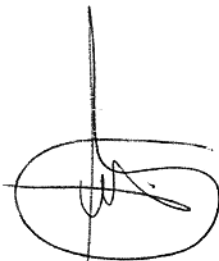
Después de un análisis, se recomienda la herramienta PGP, puesto que se cuenta con el respaldo y soporte de la empresa PGP Corporation, asimismo, se el PGP se encuentra en el cuadrante de Gartner (ver anexo 1), para el caso de GPG no esta considerado dentro del cuadrante de Gartner.

Además la IETF se ha basado en su diseño para crear el estándar de Internet OpenPGP.

PGP es el proveedor de sistemas de encriptación y de firma digital más utilizado y el más importante, dando total garantía de seguridad (Ver anexo 2).

12. CONCLUSIÓN SOBRE EL ANÁLISIS DE LAS PROPUESTAS DE SOLUCIÓN

La evaluación se ha realizado de forma transparente, con el objetivo de obtener lo más adecuado para la institución, asimismo, a prevalecido la seguridad, es así, que el empleo de software que no tenga el respaldo de ninguna empresa, seria perjudicial y riesgoso para la DINI, sobretodo tratándose de herramientas que cifraran datos privados y firmaran documentos digitales de la Dirección Ejecutiva.



Ing. Oliver Aguilar Torres
Unidad de Operaciones
OST - DINI



CESAR AUGUSTO BERROCAL DEL AGUILA
Jefe (e) de la Oficina de Soporte Técnico
Dirección Nacional de Inteligencia