*Por:* ***Juan Oliva***
*Editor:* ***Paul Estrella***

# Seguridad en Implementaciones de voz sobre IP

## Desafíos y oportunidades de soluciones de código abierto

Las disponibilidad de soluciones de Voz sobre IP actual, ha permitido que miles de empresas a nivel mundial adopten esta tecnología. Siendo la herramienta principal en entornos de "comunicaciones unificadas", ha permitido integrar a la telefonía con sistemas de procesamiento de datos y gracias a eso a un universo de aplicaciones que han combinado, extendido o creado nuevas funcionalidades.

Hay muchos estándares disponibles que han permitido generar esta convergencia con un impacto dramático en la disponibilidad y la reducción de costos.

La voz sobre IP, al ser una tecnología digital, donde el protocolo IP es su base fundamental, no deja de estar expuesta a las vulnerabilidades existentes en entornos de red. En la actualidad, hay poca exposición y documentación sobre problemas de seguridad existentes y emergentes, lo cual contrasta con los niveles de perdida económica a los que está expuesta una implementación empresarial de este tipo.

Por esta razón es necesario desarrollar el correcto aseguramiento de la plataforma seleccionada, así como de su entorno, ya que normalmente no existe un sólo punto o vector de ataque, y la plataforma de voz sobre IP no es el único servicio de software en una empresa.

Es importante tener un panorama general, adquirir el conocimiento y sobre todo conocer todos los elementos que interactúan con la plataforma; no sólo los elementos de hardware y software, sino también las personas, administradores de red, integradores y especialistas, ya que son quienes mantienen y ejecutan las reglas de seguridad en distintos niveles.

Este documento brinda un panorama general de los lineamientos y consideraciones a tomar en cuenta para brindar seguridad a plataformas de Voz sobre IP.

Copyright © 2014 Elastix

## Estado actual de la seguridad en sistemas VoIP

Algunas amenazas no son muy diferentes a las que existen actualmente en una red de datos, como por ejemplo inyecciones de SQL a nivel de aplicaciones Web, DoS (denial of service) en servicios como RDP o http y robo de sesiones o *password cracking*[1] en SSH y sistemas Web.

Varios de los servicios mencionados son parte de una plataforma Voz sobre IP en la actualidad, así que no hacen mas que arrastrar este tipo de problemas, o visto desde otro punto de vista, "incrementan el interés de un atacante". No estamos hablando sólo de conseguir acceso a una base de datos o a un servidor, sino de la posibilidad de hacer una buena cantidad de llamadas telefónicas que podrían traducirse en miles de dólares.

Sin embargo si hablamos de Voz sobre IP, de manera exclusiva, nos encontramos con SIP que es el protocolo de señalización que ha tenido mayor aceptación en la industria, y sobre el cual podemos puntualizar algunas amenazas potenciales.

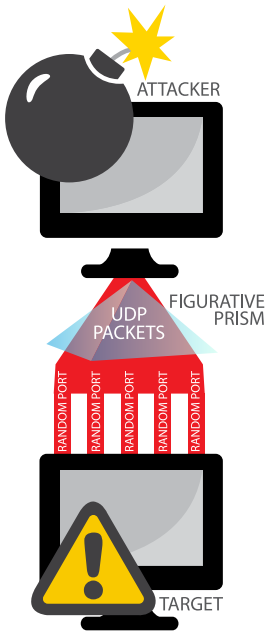
## Eavesdropping (escucha no autorizada)

Es una técnica que se desarrolla para realizar capturas de llamadas. Esto, evidentemente, está más ligado con el espionaje y es un estado colateral de realizar un ataque conocido como "Man-in-the-middle" u hombre en el medio. Si este se puede realizar, es posible capturar comunicaciones.

Esto se basa en lo que se denomina envenenamiento de la tabla ARP, que es enviar mensajes ARP falsos con la finalidad de asociar la dirección MAC del atacante, con la dirección IP del objetivo atacado, haciéndose pasar por un router o una PBX, por ejemplo.

Una vez conseguido, es posible no sólo capturar conversaciones basadas en protocolo RTP, sino también toda información que pase a través de servicios que no estén encriptados.

## Ataques de denegación de servicio (DoS) en VoIP




Son normalmente scripts, cuyo objetivo es generar inundación de paquetes. Desde esta perspectiva, existen dos tipos:

> Los que causan esta condición haciendo uso de los llamados métodos del protocolo SIP. El más conocido es el llamado INVITE FLOOD, el cual genera tantas peticiones a la plataforma VoIP, que al final el sistema termina atendiendo sólo al atacante y hace que los usuarios válidos ya no puedan usar el servicio, además de generar un consumo excesivo de procesamiento y memoria en el sistema.
>
> El otro es el que produce inundación de ancho banda de internet o más conocido como UDP FLOOD, el cual genera también muchos paquetes, pero con el objetivo de consumir todo el ancho de banda contratado por la víctima, sobre todo operadores o empresas de venta de tráfico de voz.

Estos tipos de ataques son complicados de manejar, ya que dispositivos de seguridad perimetral como Firewalls, UTMs (*Unified Threat Management*) o IPSs (*Intrusion Prevention System*), no pueden repeler este ataque con bloqueos tradicionales; por el contrario, es necesario usar equipos especializados para desviarlos.

1 *Proceso de intentar adivinar contraseñas de usuarios.*

Copyright © 2014 Elastix

## Ataques de fuerza bruta en SIP (SIP brute force Attack)

Es el ataque más común desarrollado hacia plataformas de Voz sobre IP. Se trata de adivinar textualmente las contraseñas de entidades SIP creadas en el servidor. Una vez robadas las credenciales, es posible autenticarse contra el servidor o la plataforma Voz sobre IP, para generar llamadas.

La capacidad de "adivinar" contraseñas se realiza con herramientas que automatizan este proceso, un ejemplo es la suite SIPVicious, con la cual se desarrolla un proceso denominado enumeración de entidades, para luego desarrollar el proceso de password cracking usando diccionarios en archivos de texto plano. Este tipo de ataque es muy similar al que se realiza al servicio SSH.

## VoIP Spam (SPIT - Spam over Internet Telephony)

Esta no es una vulnerabilidad en sí, sino intromisiones a la privacidad al momento de recibir llamadas no solicitadas para tratar de vender algún producto, tal como sucede desde hace mucho años con el correo electrónico. Este es uno de los usos más comunes para dialers de llamadas.

## Caller ID Spoofing

Es la capacidad de modificar el Caller ID para personificar a una persona o a una empresa, por ejemplo un banco. En el pasado implementar este tipo de ataques requería una infraestructura de telefonía bastante compleja y costosa, hoy esto ya no es así, ya que la gran mayoría de plataformas Voz sobre IP permiten reescribir este campo telefónico.

## La seguridad en soluciones propietarias

Las soluciones propietarias presentan una amplia gama de productos para cada necesidad, que muchas veces representan las tendencias a nivel tecnológico y de servicios en el mercado y que después se convierten en necesidades de los clientes.

La realidad es que muchas de estas soluciones son implementadas como cajas negras de cara al cliente o al integrador certificado. Esto responde a una óptica orientada hacia “políticas de control de soluciones”, ya que en cuanto menos pueda ver que tenga dentro, menos posibilidades tengo de encontrar vulnerabilidades o fallos de seguridad.

Sin embargo, en este ámbito del mercado, nadie esta libre de tener fallos, hasta en las mejores cajas de seguridad se pueden presentar problemas. En plataformas Voz sobre IP propietarias es posible encontrar vulnerabilidades de buffer overflow (falla en el control de datos que se copian sobre memoria), ejecución remota de comandos y denegación de servicio, siendo estos fallos más comunes de lo que uno pueda imaginar.

Copyright © 2014 Elastix

Para "descubrir" estos fallos basta dar un recorrido por sitios como exploit-db - *http://www.exploit-db.com* - o Packet Storm - *http://packetstormsecurity.com* - y realizar búsquedas de algunas de las marcas más representativas. Basado en ello, no es posible vender ninguna solución como la más segura.

Un tema importante a mencionar, está relacionado con las remediaciones o correcciones, las cuales suelen ser mucho más costosas. Lo más sencillo que puede pasar, es que sólo estén dirigidas a un cambio en la versión de firmware, lo cual puede implicar inversión a nivel de licencias. La otra cara de la moneda es más compleja e incluye un cambio de equipo total. En este caso podríamos enfrentarnos a la disyuntiva de comprar una caja nuevamente o quedarnos vulnerables.

## La seguridad en soluciones Open Source, oportunidades

Las soluciones Open Source no están libres de reportes de seguridad, la ventaja es que por un lado existen empresas que están detrás del desarrollo y por otro también comunidades de desarrolladores que lo soportan.

En este punto es importante mencionar que, a diferencia de soluciones propietarias, donde el 90% del desarrollo, revisión y corrección se realiza casa adentro, las distribuciones Open Source cuentan con un número importante de personas en diferentes partes del mundo, bajo diferentes ambientes de trabajo, que se suman al trabajo del desarrollador principal, permitiendo que estas soluciones se desarrollen a una mayor velocidad, lo cual incluye mejoras y correcciones.

Esta situación ha sido aprovechada por varias soluciones open source, las que han evolucionado hasta convertirse en referentes en ciertos sectores de la industria de software y en claros competidores en otros. No es de extrañar que más del 90% de supercomputadores en el mundo usen Linux. Soluciones como: Asterisk, Drupal, Firefox, Zimbra, Endian, Zentyal son un claro ejemplo de que este tipo de modelo de negocios funciona y es sostenible.

Otro tema importante con respecto a soluciones Open Source, es que se encuentran bajo el escrutinio de desarrolladores independientes, de su comunidad y del público en general, de tal manera que se detecte software oculto destinado a la recolección de datos o a cualquier propósito que no se relacione con el objetivo promocionado por el desarrollador principal.

## Elastix como una herramienta más de los sistemas de información empresariales

Elastix es una solución de comunicaciones unificadas de código abierto basada en Linux y Asterisk, con funcionalidades que van mas allá de una central telefónica convencional. La plataforma contiene herramientas que proveen mensajería unificada, fax virtual, sistema de mensajería instantánea corporativa, entre otras.

Un sistema de comunicaciones unificadas como Elastix no es un elemento aislado en una empresa, forma parte del flujo de procesos de la misma de tal manera que establezca un estado ideal de convergencia. Un claro ejemplo es el desarrollo de sistemas para consulta de datos desde la línea telefónica, lo cual combinado con motores de "Text-to-Speech" (texto a voz), automatiza y hace más ágiles los procesos de atención, permitiendo optimizar recursos.

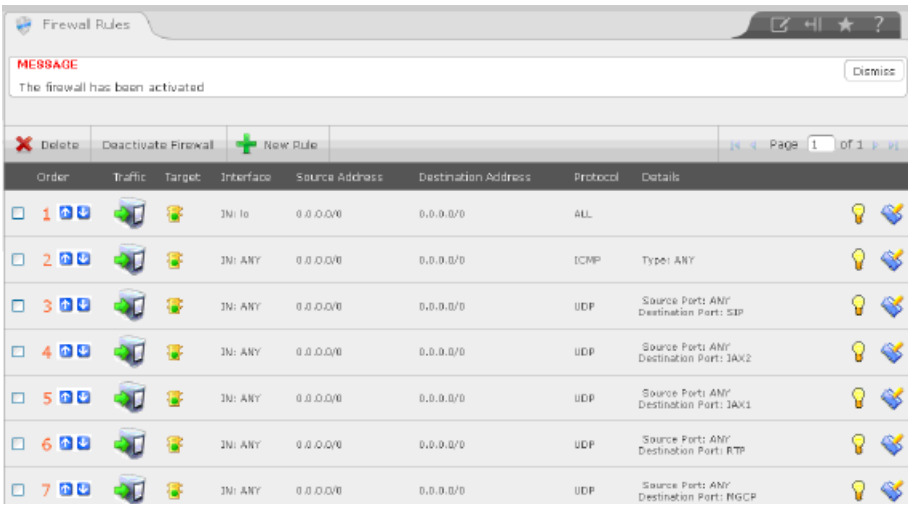
Copyright © 2014 Elastix

Otro ejemplo importante es la posibilidad de que un cliente pueda realizar una llamada telefónica y ser atendido automáticamente al hacer clic en la página web de una empresa usando un *navegador*[2]. El conjunto de estos elementos proveen valor agregado, no solo a la empresa, sino a los clientes que esperan siempre una respuesta inmediata.

## ¿Qué trae Elastix a nivel de seguridad?

Elastix, a partir de la versión 2.0, incorpora un módulo de seguridad, el cual es una herramienta importante que incluye un completo gestor de Firewall para el manejo de puertos y servicios.

Para muchos, el manejo y gestión de iptables y firewall a nivel de núcleo en distribuciones basadas en Linux puede ser un dolor de cabeza, principalmente porque la aplicación provee muchas características. Sin embargo, la incorporación de esta opción permite la administración de los puertos de acceso de manera más amigable y concreta, especialmente en escenarios donde tenemos que filtrar por origen (a la interfaz web por ejemplo) o cuando tenemos que habilitar los puertos SIP y RTP y denegar todo lo demás.




El módulo permite además hacer una "auditoría", la cual muestra todos los accesos permitidos y fallidos a la interfaz de administración, esto es útil para hacer un seguimiento de accesos.

Otra funcionalidad, denominada claves débiles, hace un recorrido de las contraseñas de todas las extensiones configuradas, verificando si estas cumplen con las políticas de contraseñas seguras.

2 *Un proceso que combina varias tecnologías, incluyendo WebRTC, VoIP y una distro VoIP.*

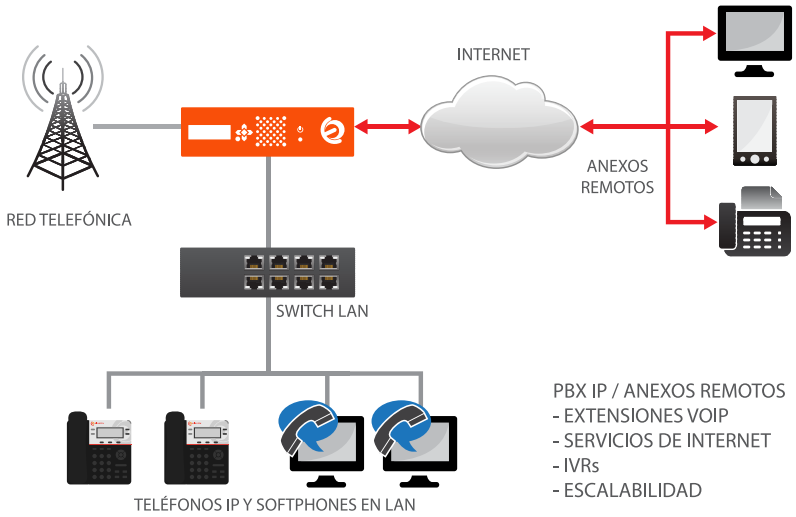
## ¿Cómo complementar la seguridad?

**Infraestructura, capacitación, prácticas recomendadas**

La implementación de seguridad en plataformas de Voz sobre IP suele plantear preguntas complejas, ya que en realidad todo depende de la necesidad de accesibilidad y servicios que necesitemos incorporar.

Algunos escenarios incluyen:

- Elastix hacia la *PSTN*[3], extensiones locales y administración remota.
- Elastix hacia PSTN, extensiones locales, administración remota, proveedor *VoIP*[4] para llamadas salientes.
- Elastix hacia PSTN, extensiones locales, administración remota, proveedor VoIP para llamadas salientes y entrantes con DID.
- Elastix hacia PSTN, anexos locales, administración remota, proveedor VoIP para llamadas salientes y entrantes con DID, extensiones remotas.




Estos escenarios no son únicos y el acceso a la tecnología hace que se vuelvan cada vez más complejos. Sin embargo, actualmente existen herramientas y modelos de infraestructura que se pueden implementar para brindar aseguramiento.

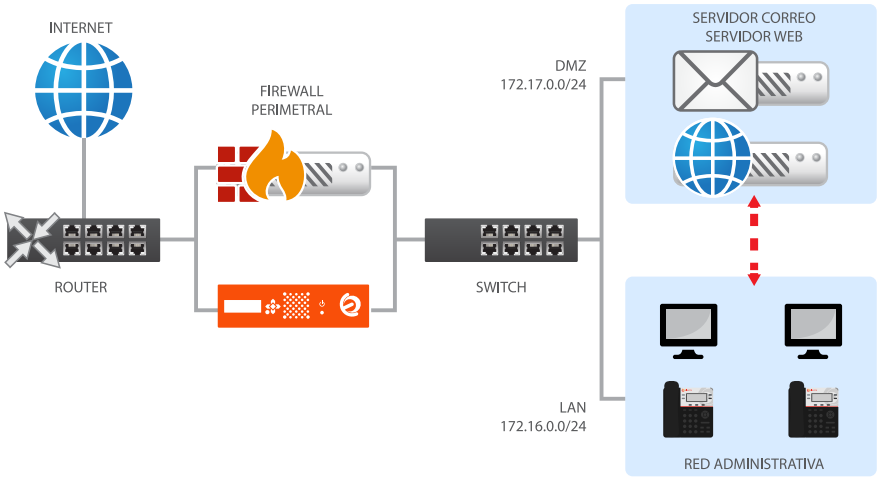
Un desafío importante es el posicionamiento de un firewall de perímetro, sobre todo cuando la gestión del mismo no está a cargo del cliente. Hay que ser claro desde el inicio, no es imposible hacer funcionar correctamente Elastix detrás de un firewall, pero es necesario mucha coordinación y afinamiento.

Más importante aún, el firewall no se debe considerar como un elemento que garantice al 100% la seguridad, eso sería un gran error. Es necesario ir mucho más allá y una de las opciones es implementar software que reaccione proactivamente ante ataques desde su inicio.

Dos soluciones que funcionan bastante bien son Fail2ban y Snort, y es recomendable considerarlas en la etapa de diseño de la implementación.

3 *Public Switched Telephone Network / Red telefónica conmuntada.*
4 *Voz sobre IP*

Copyright © 2014 Elastix




## Responsabilidades

Establecer obligaciones es un aspecto muy delicado, ya que existen diferentes personas involucradas en un proceso de implementación y sobre todo en el mantenimiento de la plataforma. Cada persona necesita de coordinación y establecimiento de roles y responsabilidades.

Dos roles básicos en una implementación son:

### Rol de Integrador o Especialista

Es el profesional que provee la solución y quien realiza la implementación después de un análisis adecuado, el cual debe ser realizado junto al cliente.

Algunas de sus responsabilidades son:

- Identificar las necesidades del cliente.
- Establecer el posicionamiento adecuado de la plataforma en base a las necesidades.
- Implementar las funcionalidades solicitadas por el cliente.
- Conocimientos de riesgos inherentes a la plataforma.

### Rol de cliente

Este es probablemente el rol más importante, ya que es la persona que finalmente mantiene el sistema, pero más aún, es quien establece el requerimiento inicial, quien elige el proveedor, quien establece el presupuesto de la implementación y quien debe tomar las decisiones previas a la implementación.

Es un rol que incluye al gerente de la empresa, el encargado de *TI*[5] y al administrador de sistemas, esto tomando en cuenta un escenario ideal. Debe tener suficiente conocimiento para preservar el funcionamiento de la plataforma.

Algunas de sus responsabilidades son:

- Conocer los riesgos internos (LAN) y externos (internet).
- Mantener contraseñas seguras en general.
- Establecer como prioridad la seguridad frente a la flexibilidad.
- Asesorarse siempre con una empresa especialista, ya sea mediante un contrato de soporte o por servicios puntuales.
- Solicitar al operador telefónico brindar límites de salida hacia la PSTN.
- Capacitar al personal técnico en las soluciones implementadas.
- Capacitar al personal técnico de manera frecuente en temas de seguridad.

5 *Tecnologías de la Información*

## Desafíos hacia el futuro

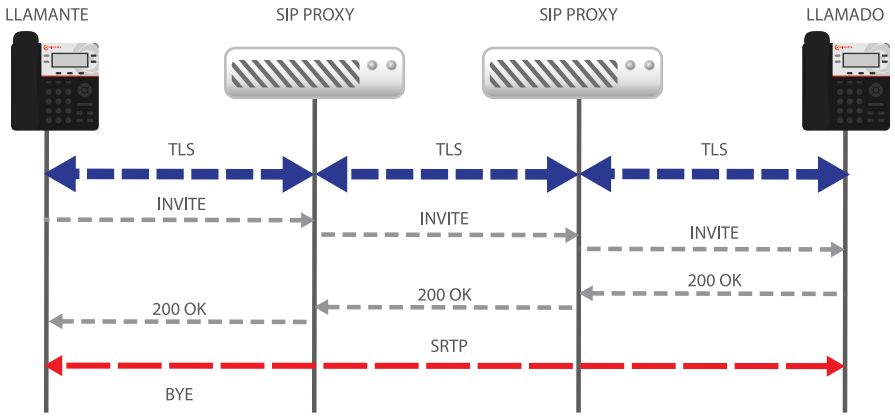
Los desafíos hacia el futuro están del lado de la movilidad y el fácil acceso a los recursos.

Las empresas y usuarios finales están cada vez más relacionados con el fácil uso de herramientas a nivel de cliente, como Hangouts o Skype.

Bajo esta alfombra que nos cubre viene la interrogante de siempre, *¿Cómo resolver el problema de la seguridad?*

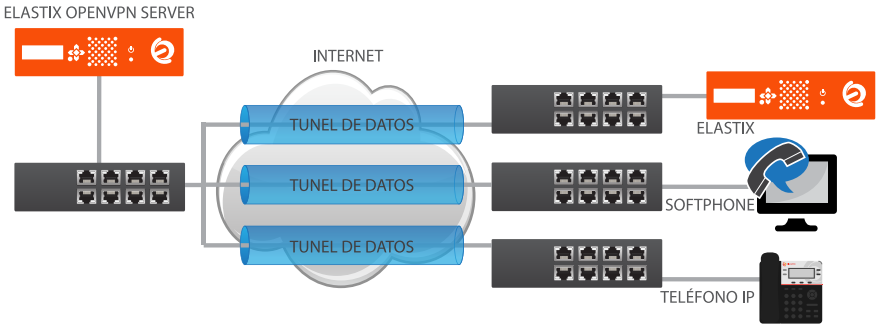
Una respuesta sencilla es "pensar en mecanismos de seguridad para cada escenario".

Un ejemplo importante es la seguridad de la comunicación, orientado a enlaces remotos y conexiones entre sucursales, y que deben estar dirigidos a dificultar el acceso a los paquetes de voz y al sniffing ilegal. Herramientas como TLS (Transport Layer Security) y SRTP (Secure Real-time Transport Protocol) que aunque suenen muy complejas, son protocolos estándares soportados en Elastix. Su correcta implementación puede garantizar la confidencialidad de las comunicaciones en ambientes donde se requiere minimizar al máximo este tipo de riesgo.




Otro ejemplo se relaciona con ambientes colaborativos como el teletrabajo, en donde las extensiones remotas son una necesidad clave. Para este caso, la implementación de redes privadas virtuales o "VPNs", brindan mucha flexibilidad, ya que existe una amplia gama de ordenadores, laptops, terminales telefónicas y dispositivos móviles que incorporan software tipo cliente para VPN.

Esta solución no sólo nos permite establecer conexión a nuestra red privada de manera segura, sino que además, en el caso de implementaciones VoIP, elimina los problemas relacionados con NAT Transversal.



## Acerca del Autor

Juan Oliva Cordova
@jroliva
http://jroliva.wordpress.com/

Es consultor de seguridad informática y Telefonía IP con mas de 10 años de experiencia en el campo. Está muy involucrado en proyectos de pruebas de penetración, análisis y explotación de vulnerabilidades, entre otras tareas de la seguridad informática. También desarrolla proyectos de implementación y aseguramiento de plataformas de telefonía IP, basadas en Elastix, proyectos de CallCenter, soluciones en la nube y hosted PBX.


Parte del desafío incluye además la difusión de medidas de seguridad de manera paralela con el lanzamiento y evolución de soluciones de software y hardware. La tecnología ha avanzado tan rápido, que no ha permitido transmitir adecuadamente las necesidades de implementación a nivel de infraestructura y conocimiento. Cada vez se hace más necesario contar con un asesor adecuado en tecnología, ya sea casa adentro o con empresas especializadas.

De esta forma se logra que la organización se pueda enfocar en el núcleo de su negocio, el cual en la mayoría de los casos no es la tecnología, sino el uso de ella para alcanzar objetivos.

Evidentemente, la capacitación y el entrenamiento constante es vital. Hoy el profesional tiene una mayor responsabilidad y es claro que contar con destrezas o conocimientos en seguridad es un valor agregado que marca una diferencia importante a la hora de realizar una implementación.

El equipo de Elastix, por ejemplo, está consciente de esta necesidad, por lo cual ha diseñado un curso de seguridad como parte de su programa de entrenamiento. El objetivo es complementario, ya que las buenas prácticas se transmiten desde la instalación de la plataforma.

## Conclusiones

Es claro que con el avance tecnológico seguirán apareciendo vulnerabilidades, sin embargo también se desarrollan mecanismos de protección que son necesarios seguir, el reto siempre va a estar en el orden del conocimiento, análisis y aplicación, de tal manera que determinemos una solución para cada necesidad.

**Elastix® Security Master**

Sea parte del selecto grupo de Profesionales Certificados Elastix