

HISPASEC



HISPASEC SISTEMAS
SEGURIDAD Y TECNOLOGÍAS
DE LA INFORMACIÓN.



www.hispasec.com



ORIGENES



HispaSec nace a finales de 1998 con el lanzamiento de "una-al-día", el primer servicio diario de información técnica en español sobre seguridad informática, creado por un grupo de especialistas con el propósito de divulgar y concienciar a los usuarios de la importancia de este sector en el campo de las nuevas tecnologías de la información.

El éxito cosechado por "una-al-día" y el resto de acciones públicas emprendidas por HispaSec (análisis, comparativas, desarrollos, etc.) origina, de forma espontánea, una demanda de servicios por parte de profesionales y empresas.

Para responder a dicha demanda se crea, en el año 2000, el laboratorio de seguridad informática Hispasec Sistemas. Hispasec Sistemas es una empresa de mercado carácter técnico, sin capital externo ni supeditación a intereses ajenos, gestionada íntegramente por los fundadores de HispaSec.

Lejos de desviarse del propósito original, el nuevo rumbo adoptado por Hispasec Sistemas permite mantener y aumentar los servicios públicos y gratuitos para la comunidad, así como atender la demanda creciente de profesionales y empresas.



FILOSOFIA

Seguridad, nuestra razón de ser

Hispasec nació por y para la seguridad de las tecnologías de la información. Desde su origen se ha especializado en sus diferentes áreas y concentra su inversión en crecer de forma dinámica según criterios puramente técnicos, siendo su principal activo el equipo humano y sus conocimientos.

Diferentes puntos de vista y un único propósito

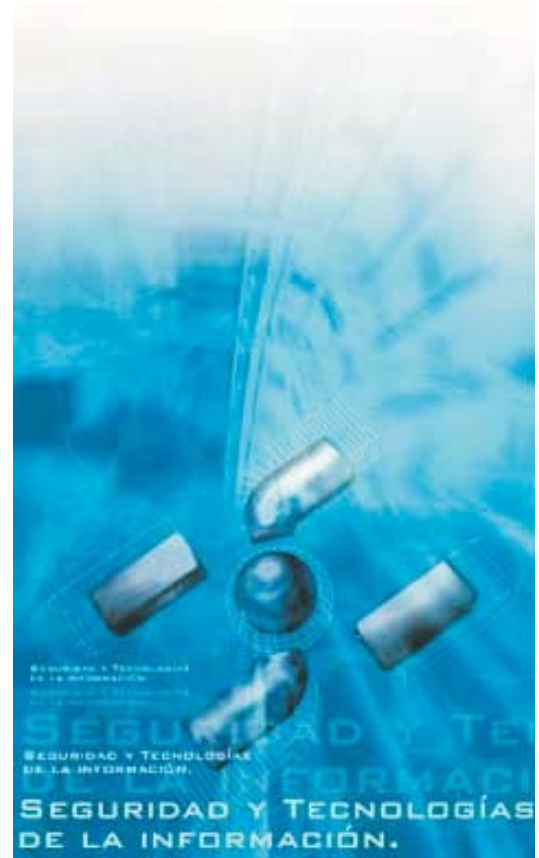
Un equipo multidisciplinar, compuesto por especialistas en las principales plataformas tecnológicas y áreas de la seguridad, permite afrontar los proyectos desde distintas perspectivas complementarias, para encontrar la solución idónea según el perfil y las necesidades de nuestros clientes.

Laboratorio independiente de terceras empresas y productos

Hispasec no distribuye productos de terceros ni tiene intereses económicos relacionados con ellos, condición indispensable para acometer los análisis con el rigor, independencia y objetividad necesarios, sin que ningún interés comercial adultere el proceso en perjuicio de nuestros clientes.

Consultoría experta y transferencia del conocimiento

Hispasec se enorgullece de trabajar "codo con codo" con nuestros clientes, con un servicio personalizado, donde se pone especial énfasis en ofrecer al cliente (in)formación crítica y establecer vías de contacto permanente que permitan su actualización, para participar de forma activa en el proceso continuo de mantener seguros sus sistemas y procesos.



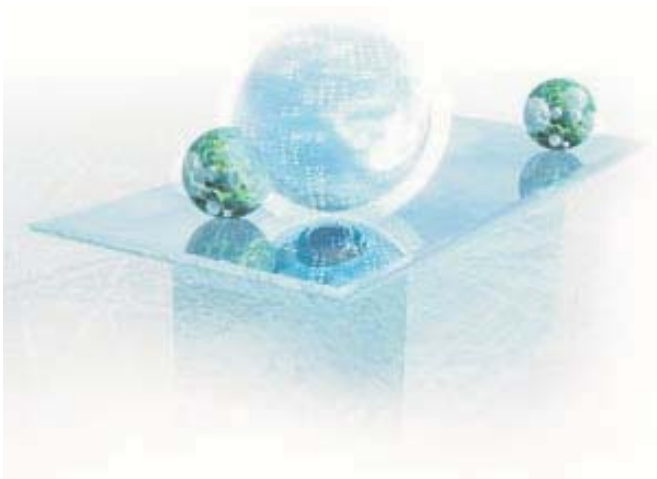


SERVICIOS: AUDITORIA

El servicio de auditoría, interna o perimetral, comprende el estudio de los sistemas para identificar vulnerabilidades y proponer medidas correctivas específicas, así como recomendaciones adicionales de seguridad proactiva.

Algunas fases genéricas del servicio son:

- Enumeración de redes, topología y protocolos
- Identificación de sistemas y dispositivos
- Análisis de servicios y aplicaciones
- Detección, comprobación y evaluación de vulnerabilidades
- Medidas específicas de corrección
- Recomendaciones sobre implantación de medidas proactivas



Adicionalmente, y en función de la casuística o especificaciones del cliente, se abordarán otros análisis, como pueden ser la auditoría del código fuente de aplicaciones públicas o propietarias, criptoanálisis de algoritmos de cifrado privados, etc.

Para abordar los análisis se utilizan herramientas y metodologías reconocidas, junto a utilidades y técnicas específicas desarrolladas por el equipo de Hispasec, fruto de la experiencia acumulada en este sector.

Durante la auditoría se realizan todo tipo de pruebas, incluyendo desbordamientos de búfer, inyección, cross-site scripting, denegación de servicio, etc.



SERVICIOS: CONSULTORIA



El servicio de consultoría pone a disposición del cliente el conocimiento, especialización, experiencia y puesta al día del equipo de Hispasec para abordar proyectos que contemplen en mayor o menor medida requisitos de seguridad.

Algunas de las áreas motivos de consultoría son:

- Criptología.
- Definición y revisión de Políticas de seguridad.
- Consultoría de Windows y Unix en general.
- Configuración y Desarrollo de redes y sistemas seguros.
- Sistemas de alta disponibilidad y clusters.
- Redes privadas virtuales (VPN).
- Análisis, evaluación y comparativas de soluciones de seguridad.
- Evaluación, adaptación, despliegue y mantenimiento de aplicaciones Open Source.
- Evaluación, implantación y gestión de soluciones antivirus corporativas.
- Sistemas de monitorización y alertas.
- Investigación y Desarrollo de soluciones específicas.

La independencia de Hispasec, al no distribuir productos de terceros ni supe ditarse a plataformas específicas, se presenta vital para abordar con el rigor y objetividad que se merecen el estudio, análisis y valoración de las soluciones a adoptar.





SERVICIOS: S.A.N.A.



Servicio de Análisis, Notificación y Alertas para profesionales y empresas

El Servicio de Análisis, Notificación y Alertas (SANA) es un completo sistema de información en tiempo real destinado a cubrir las necesidades de empresas y profesionales en materia de seguridad informática.

Diseñado por el equipo de Hispasec Sistemas, especialistas con una dilatada y contrastada experiencia en el sector, SANA ofrece un servicio de información sobre seguridad informática personalizado según el perfil de cada cliente. Así, por ejemplo, los usuarios de SANA recibirán puntualmente, en tiempo real, la información sobre nuevas vulnerabilidades que realmente puedan afectar a los sistemas de su empresa, junto con las medidas preventivas y/o parches para subsanarlas.

Basado en el conocimiento y tecnología desarrollada durante los últimos cinco años, y tomando como base el conocido servicio una-al-día, Hispasec Sistemas ha desarrollado un servicio de alertas profesional. Hispasec Sistemas registra una media cercana a las veinte (20) alertas de seguridad diarias, con este servicio los administradores podrán asegurarse de que reciben toda la información que afecte a sus sistemas de forma inmediata a que esta sea registrada y procesada en los Laboratorios de Hispasec Sistemas.

El equipo de Hispasec Sistemas publicará regularmente, en exclusiva para SANA, CheckLists, análisis, informes técnicos y diversa documentación sobre las plataformas motivo de la suscripción. Por último, el círculo se completa con la diaria recopilación y notificación de noticias del sector, artículos, informes y demás publicaciones que se ajusten al perfil e interés del cliente.





SERVICIOS: S.A.N.A.

Alertas por mail, SMS y web

En Hispasec Sistemas creemos que no basta con tener toda la información, sino que tenerla en el momento preciso también es crucial. Por ello, el servicio de alertas se presta con total disponibilidad en formato 24x7 a través de correo electrónico y SMS.

DraftProof

La avanzada tecnología propietaria **DraftProof** de Hispasec Sistemas, monitoriza un número ilimitado de foros, páginas web de fabricantes, servidores FTP de parches, boletines de vulnerabilidades y servicios de alerta temprana para, de forma rápida y automatizada, realizar el seguimiento y monitorización de un gran número de fuentes.



Alertas protegidas criptográficamente

HispaSec Sistemas es muy consciente de que el recurso más valioso hoy en el mundo de las Tecnologías de la Información es el tiempo. Nuestro objetivo es que HispaSec Sistemas llegue a ser una fuente de información de la que los departamentos de Tecnología puedan considerar fiable e indiscutible. Por ello, HispaSec Sistemas envía sus alertas por correo electrónico firmadas digitalmente, de forma que nuestros clientes puedan estar absolutamente seguros de su procedencia y de que no han sido manipuladas de ninguna manera.

Base de datos

Hispasec Sistemas dispone de una completa base de datos de vulnerabilidades y virus, sobre la cual se incorporan las nuevas vulnerabilidades. De esta forma se puede realizar un completo seguimiento de todos los problemas existentes y parches publicados para cada uno de los sistemas.

Informes mensuales

Todos los meses los suscriptores del servicio SANA recibirán un informe con estadísticas e información sobre las alertas enviadas y registradas durante el mes.



SERVICIOS: FORMACION



Seguridad en la infraestructura de red

Curso de Sistemas IDS y análisis forense de incidencias

Seguridad en aplicaciones J2EE

Curso de migración a ASP.NET

Desarrollo de Aplicaciones Internet Seguras en ASP.NET

Curso de Seguridad Internet en servidores UNIX (Solaris/Linux)

Curso de seguridad Internet en servidores Windows (NT/2000)





VirusTotal

VirusTotal

El mayor antivirus público de Internet



VirusTotal es un servicio de detección de virus, gusanos y malware en general, que permite analizar archivos con múltiples motores antivirus. Cualquier usuario de

Internet puede enviar archivos o mensajes sospechosos y obtendrá de forma gratuita un informe con el resultado del análisis.

Desarrollado por Hispasec Sistemas, VirusTotal integra los motores antivirus de ClamAV (ClamWin), Computer Associates (Iris, Vet), Doctor Web, Ltd. (DrWeb), Eset Software (NOD32), Fortinet (Fortinet), FRISK Software (F-Prot), Grisoft (AVG), H+BEDV (AntiVir), Ikarus Software (Ikarus), Kaspersky Lab (AVP), McAfee (VirusScan), Norman (Norman Antivirus), Panda Software (Panda Platinum), Softwin (BitDefender), Sybari (Antigen), Symantec (Norton Antivirus) y VirusBlokAda (VBA32). Adicionalmente a estos antivirus, Hispasec trabaja continuamente en la incorporación de nuevos motores que aumentarán, aun más si cabe, la capacidad de detección del servicio.

En la dirección los usuarios podrán acceder al formulario de análisis, a estadísticas globales en tiempo real sobre incidencias, así como a descripciones e información sobre virus y malware en general.

Además, los usuarios pueden reenviar directamente los mensajes o adjuntar los archivos sospechosos mediante correo electrónico a la dirección analiza@virustotal.com con el asunto ANALIZA. En breves instantes, dependiendo de la carga puntual del servicio, recibirán en su buzón el informe detallado del análisis.

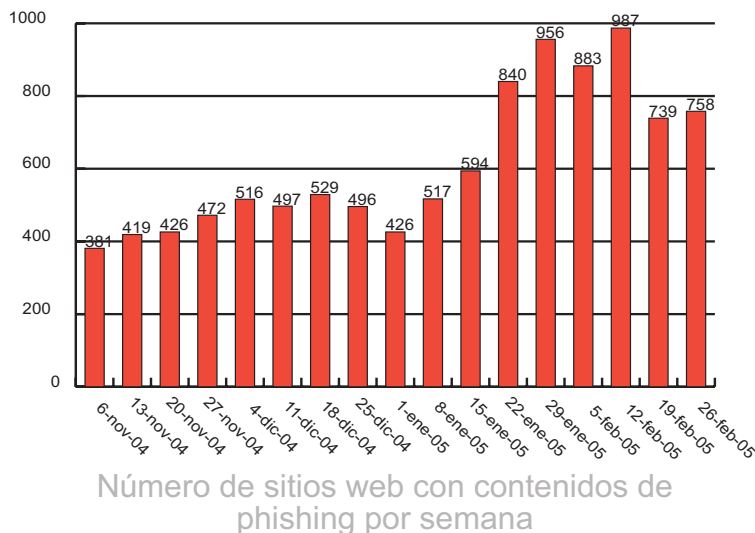




SERVICIO TEMPRANO ANTI-PHISHING

La continua proliferación de los ataques phishing contra entidades bancarias crea la necesidad de un servicio para contrarrestar los posibles fraudes a los clientes y el daño a la imagen corporativa que llevan consigo este tipo de estafas.

Una vez se lanza un ataque phishing el tiempo corre en contra de la entidad, por lo que se debe actuar de inmediato para mitigar el ataque y minimizar al máximo el número potencial de clientes afectados y el impacto mediático.



El Servicio Temprano Anti-Phishing es un sistema 24x7 de respuesta y actuación contra ataques phishing detectados.

El objetivo de este servicio es minimizar y mitigar los ataques phishing que pudieran tener como objetivo a los clientes de la entidad bancaria o comercio electrónico afectado mediante la suplantación de sus servicios.

Características:

- Servicio disponible 24h x 7d, 365 días al año.
- Requerimiento del servicio mediante correo electrónico al laboratorio de Hispasec Sistemas, que mantiene personal técnico 24x7.
- Una vez recibido el requerimiento del servicio, o detectado por el propio laboratorio, se procede de forma inmediata al análisis del phishing y se establecen las líneas de actuación.



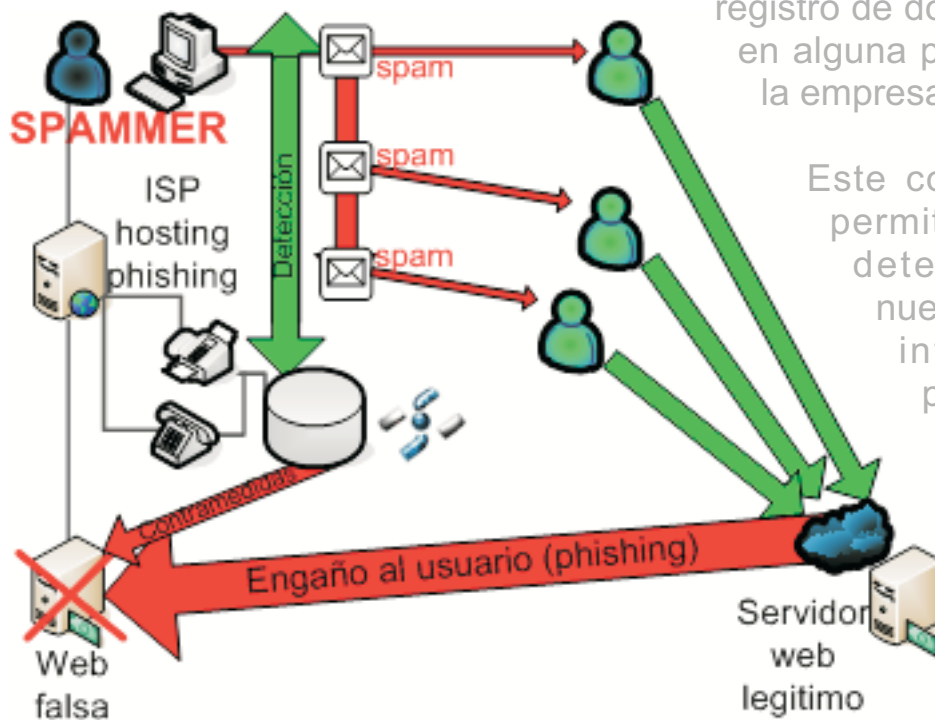
SERVICIO TEMPRANO ANTI-PHISHING

Monitorización y control de nombres en Internet. Proteger el poder de la marca.

En el mercado actual, las marcas tienen un gran valor para la empresa que las posee. Desde el nombre de la propia empresa, hasta los de los diferentes servicios o productos ofrecidos pueden ser empleados de forma incorrecta en Internet provocando un grave perjuicio para la compañía afectada.

El servicio de monitorización y control de nombres en Internet de Hispasec Sistemas (incluido como parte del servicio temprano anti-phishing) está destinado a supervisar y proteger las marcas de una empresa en Internet, detectando el

registro de dominios que hagan uso en alguna parte de las marcas de la empresa.



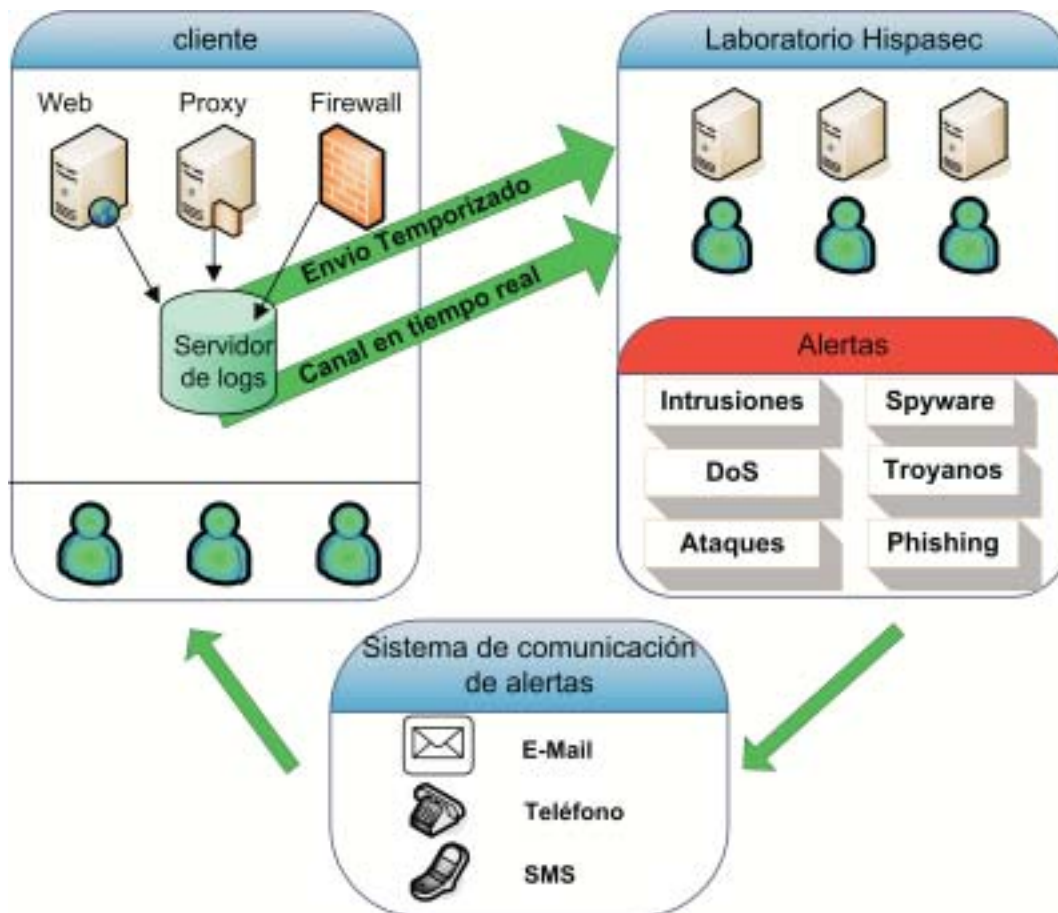
Este control puede llegar a permitir la identificación y detección proactiva de nuevos riesgos, ataques o intentos de estafa y phishing que afecten de forma directa a la seguridad informática o de los propios valores de la compañía.



LOG SECURITY INSPECTOR

Log Security Inspector es un sistema 24x7 de análisis del comportamiento, eventos y registros, sobre los sistemas perimetrales críticos del cliente, con gestión compartida entre Hispasec Sistemas (análisis profundo de seguridad) y el cliente (notificación de alertas e informes).

Mediante este servicio se logra monitorizar los logs y eventos de los sistemas críticos, en especial servicios web, firewalls, y sistemas perimetrales más expuestos a los ataques externos, a nivel de peticiones, logs y eventos, para la detección temprana de actividades sospechosas y prevención de intrusiones no autorizadas. Adicionalmente se recomienda incluir en este servicio los proxys de salida hacia Internet, ya que permiten la detección de spyware y troyanos que pudieran estar activos en la intranet del cliente.





LOG SECURITY INSPECTOR

Este servicio nace ante la necesidad de detección preventiva de los diferentes tipos de ataque o intrusiones que puede sufrir cualquier corporación. La mayoría de estos ataques perimetrales dejan huellas en los sistemas objetivo que pueden ser detectadas mediante el análisis de los logs o registros. Por ejemplo, un ataque a un servidor web suele estar precedido de una elevada cantidad de peticiones buscando explotar vulnerabilidades conocidas, o un ataque phishing puede ser detectado al examinar las cabeceras de procedencia de las visitas.

Características:

- Log Security Inspector necesita del acceso a los logs de los sistemas a monitorizar, dependiendo del número será necesario instalar un sistema en la red del cliente que actúe como recolector. Este sistema podrá configurarse para recoger o recepcionar directamente los logs de los sistemas (push o pull). Si el volumen es considerable, en vez de realizar el envío de logs al exterior en tiempo real, se podría analizar en el mismo sistema mediante una conexión permanente con el laboratorio de Hispasec Sistemas a través de Internet, reduciendo al mínimo el ancho de banda requerido por el servicio (menos de 10Kb).
- Monitorización 24h x 7d, 365 días al año.
- El análisis de los registros se hará de forma mixta, mediante el uso de herramientas propietarias y siempre bajo la supervisión de un técnico especialista en seguridad, dotando de una mayor capacidad al sistema en comparación con otras aplicaciones de seguridad basadas exclusivamente en software que no son capaces de detectar ataques personalizados o variaciones de los patrones reconocidos.
- Alertas y notificación mediante e-mail y SMS (con posibilidad de estudiar otras vías: clientes desktop, mensajería instantánea, etc).

Ejemplos de alertas, notificaciones y status:

- Detección y notificación de intentos de ataque por diccionario, fuerza bruta, inyección de código.
- Detección temprana de intentos de explotación de vulnerabilidades por parte de gusanos, herramientas automatizadas y ataques personalizados.
- Detección y monitorización de ataques phishing partiendo de la detección de visitas de usuarios que han podido ser víctimas del mismo.



CONTACTO

HISPASEC SISTEMAS

Parque Tecnológico de Andalucía.
Avda Juan Lopez Peñalver, 21
Campanillas - 29590- Málaga, España.

Tel: (+34) 902 161 025
(+34) 951 010 548

Fax: (+34) 951 010 589

e-mail: hispasec@hispasec.com

