

BAICOM
networks

GO SECURE. GO BAICOM.

Quienes Somos

BAICOM networks es una empresa orientada a proveer Servicios de Seguridad Informática con el concepto de MSSP (Managed Security Service Provider) fundada a comienzos del 2003 por un grupo de ingenieros que integraron y trabajaron con importantes empresas de renombre en Argentina adquiriendo gran experiencia en el campo de las telecomunicaciones y la tecnología.

Algunas de las mencionadas empresas son:

AT&T Latin América
Techint
Telefónica de Argentina
PriceWaterhouse & Coopers
Alcatel
Sadmitec
UADE (Universidad Argentina de la Empresa)
UOL-Sinectis

Nuestra metodología de trabajo se basa en estándares internacionales como ser:

- Norma IRAM-ISO IEC 17799
- Control Objectives for Information and Related Technology (COBIT)
- Metodología OSSTMM (Open Source Security Testing Methodology)

Filosofía

Nuestra empresa prioriza el éxito en el cumplimiento de las metas de nuestros clientes, prestando servicios fundados en la ética y la credibilidad de las relaciones, comprendiendo sus necesidades a través del trabajo en equipo para la gestión de un servicio de calidad, con tecnología de punta y recursos confiables.

Trabajamos con total integridad, volcando una gran experiencia al servicio de las necesidades de nuestros clientes, respondiendo creativa y efectivamente con servicios que elevan al máximo la calidad del producto final.

Estamos enfocados en la satisfacción de las necesidades de nuestros clientes con el fin de proveer y mantener un servicio exclusivo, innovador, con soluciones que faciliten el éxito sostenido de sus actividades.

Servicios

Operación	Auditoria	Consultoría	Normativa
■ Análisis de Vulnerabilidades	■ Test de Penetración	■ Diseño de Arquitectura Segura de Red	■ Políticas de Seguridad
■ Gerenciamiento e Implementación de dispositivos de Seguridad	■ Análisis de Aplicaciones de Red	■ Análisis Forense	■ Manuales de Procedimiento
■ Adecuación permanente de la estrategia de Seguridad	■ Auditoria de Red	■ Análisis de Comportamiento	■ Estándares de Seguridad
■ Gestión de Logs		■ Hardenning	
■ Control de Cambios		■ Nuevas Tecnologías	
■ Protección de Aplicaciones y Servidores		■ Capacitación	
■ Outsourcing de Seguridad			

Servicios > Operación de Seguridad

Por medio de la Operación de la Seguridad Informática, BAICOM ofrece a sus clientes una solución muy conveniente para resolver la problemática de Seguridad dentro de la empresa.

A través de su equipo de profesionales altamente especializados en las distintas tareas y tecnologías, se apunta a trabajar en forma permanente y proactiva, de manera de poder garantizar la confidencialidad, integridad y disponibilidad de la información de su empresa.

Para esto se trabaja en distintos aspectos:

- **Análisis de Vulnerabilidades**

Proporcionaremos una radiografía del estado de la seguridad actual de la organización.

Nuestro método no intrusivo ayuda a tener una visión global del estado de sus redes e infraestructura de IT, sin llegar a explotar las fallas y vulnerabilidades que se encuentren durante el Estudio.

Esta destinado a identificar cualquier exposición o vulnerabilidad que pudiese existir en sus equipos, para que pueda contar permanentemente con información protegida, correcta y consistente. Se generara así una capacidad de crecimiento controlada y preparada para cualquier nuevo proyecto.

Todos los procedimientos son testeados en un ambiente aislado de laboratorio, logrando una mayor efectividad e inteligencia en los resultados que arrojan los procesos automáticos.

BAICOM proporciona informes técnicos detallados que incluyen objetivo, fecha y hora, tipo de riesgo, recomendación, screenshots, referencias, diagramas, etc.

Las recomendaciones contienen una explicación detallada de los métodos correctivos a seguir, orientadas netamente a la resolución del problema, con el fin de facilitar la tarea del personal de IT.

- **Gerenciamiento e Implementación de dispositivos de Seguridad**

Se implementan y gestionan equipos de seguridad que demandan especialización y alta carga de recursos humanos, como IDS/IPS/Firewalls/etc., revisándose constantemente las configuraciones, correlacionando ataques de manera de reducir falsos positivos a través de la optimización de reglas, y de esta manera trabajar en seguridad pro activamente.

- **Adecuación permanente de la estrategia de Seguridad de la empresa**

La situación relevada en cuanto a riesgos latentes, criticidad de cierta información para determinados procesos y los tiempos del mercado obligan a delinear una estrategia de seguridad.

Esta básicamente priorizara las medidas correctivas que sugiramos considerando los riesgos críticos, los presupuestos, recursos disponibles, situación de mercado y competencia, etc.

De esta manera se trabaja activamente en esta área, adecuando esta estrategia permanentemente de acuerdo a las necesidades de la empresa.

- **Gestión de logs**

Utilizamos nuestra plataforma de Centralización y Correlación de Eventos para reunir toda la información de sus aplicaciones, sistemas operativos y dispositivos. De esta manera se garantiza la existencia de los registros de actividades de todas las plataformas y usuarios, permitiendo de esta manera reconstruir prácticamente cualquier evento realizado en su empresa.

De esta manera monitorearemos ininterrumpidamente aquellos dispositivos críticos para la seguridad de su red.

Esta tarea se realiza en forma continua durante todo la operación de la seguridad de la empresa, asegurando la integridad de la información manejada por los sistemas de la misma y liberando recursos internos clave importantes para la implementación de medidas correctivas.

- **Control de Cambios**

Proporcionamos el debido seguimiento y consultoría de implementación de las medidas correctivas que entregan nuestros informes asegurando así el cumplimiento de los tiempos detallados en el plan de trabajo.

Este punto implica la resolución de problemas o temas relacionados al normal funcionamiento de los equipos antes mencionados.

- **Protección de Aplicación y Servidores**

Brindamos la información necesaria para poder actualizar las versiones y/o parches correspondientes a las nuevas vulnerabilidades que surgen a diario, de acuerdo a las que aplican a los servicios de la empresa.

De la misma manera garantizamos nuestra gestión conjunta con el personal de la empresa para su correcta aplicación.

- **Outsourcing de Seguridad**

BAICOM networks brinda el servicio de Outsourcing de Seguridad Informática, por medio del cual, apunta a que la empresa tercerice el 100% del departamento de seguridad informática en nosotros, logrando de esta manera un total foco en su negocio.

Servicios > Auditorías de Seguridad

Dentro del campo de auditoría, estos son algunos de los servicios que brindamos:

- **Test de Penetración**

Consiste en una serie de pruebas intrusivas que intentan vulnerar y penetrar al sistema, asemejándose a los eventos reales que pudiesen generar ataques informáticos, pero en un ambiente de seguridad controlado con el fin de detectar puntos débiles en los sistemas del cliente.

Este estudio puede ser en distintas modalidades:

Standard: En esta modalidad, el test se realiza con cierta información brindada con anterioridad al comienzo del análisis del cliente a BAICOM, de manera de buscar acortar los tiempos de pruebas.

Black Box: En este escenario el cliente no brinda ningún tipo de información a BAICOM, salvo el direccionamiento IP a analizar, de manera de poder simular 100% a un atacante externo sin información interna de la empresa.

La metodología del Test de Penetración es la siguiente:

- *Reconocimiento*
 - Determinación de objetivos y planificación
 - Obtención de Información
- *Análisis y Procesamiento*
 - Búsqueda de puntos débiles
 - Análisis de vulnerabilidades
- *Penetración y Consolidación*
 - Ingeniería Social
 - Explotación de vulnerabilidades
 - Escalada de privilegios
- *Calificación y Conclusión*
 - Determinación del nivel de seguridad
 - Sugerencias orientadas a la resolución de problemas de seguridad

- **Análisis de Aplicaciones Web**

Con la constante aparición de nuevas aplicaciones Web, su correspondiente exposición en Internet o a través de una Intranet, hace falta evaluar la seguridad de dichas aplicaciones.

Además, teniendo en cuenta que la mayor cantidad del tráfico generado entre la aplicación y el usuario debería ser encriptado (utilizando certificados), se genera una brecha de seguridad muy importante, donde ni siquiera los IDS pueden entrar en juego. Esto se debe a que al estar encriptado el tráfico que genera esta aplicación el IDS no lo puede analizar, en definitiva, se torna en una caja ciega que debemos estar seguros de que manera la estamos exponiendo.

Los análisis que se realizan de aplicaciones Web, se realizan de dos maneras:

- **Con Credenciales:** Se realizan las pruebas correspondientes con usuarios validos del sistema, de manera de poder analizar exactamente cuales son los accesos reales que se le esta dando a un usuario autorizado.

- **Sin Credenciales:** Se realizan las pruebas sin usuarios validos, buscando quebrar la seguridad de la aplicación y tratando de ganar acceso como un usuario cualquiera que pueda tener acceso a la aplicación.

- **Auditoria de red**

En esta auditoria, se busca tener en claro cual es el nivel de seguridad de los distintos medios de acceso de red (VPNS, WiFi, WIMAX, LAN, WAN, etc) de la empresa, buscando de esta manera tener los distintos accesos acotados y controlados de la mejor manera posible.

Servicios > Consultoría en Seguridad

Dentro del área de consultoría, algunos de los servicios que brindamos son:

- **Diseño de Arquitectura Segura de Red**
Tanto si usted se encuentra diseñando una nueva red, como si esta revisando la arquitectura de su red actual desde una perspectiva segura, nuestros profesionales podrán asistir a su empresa en estas tareas, de manera de poder garantizar la mayor seguridad posible en su nueva infraestructura.
- **Análisis Forense**
Ante un incidente informático, con el asesoramiento de BAICOM networks, usted podrá identificar los ataques consolidados y examinar los métodos que fueron utilizados. Esto le permitirá conocer más sobre las nuevas técnicas de Hacking y desarrollar estrategias para evitar que impacten nuevamente.
- **Análisis de Comportamiento**
Consiste en detectar un comportamiento anómalo o no esperado de un sistema o aplicación ante distintos eventos del ambiente. Estos eventos son controlados y manipulados con diferentes técnicas y metodologías para probar posibles respuestas y comportamientos que puedan brindar los sistemas en estudio y pongan en juego la seguridad del entorno.
- **Hardening**
Nos ocupamos de elevar los estándares de seguridad de los sistemas Microsoft / Unix / Linux, junto con sus dispositivos de Networking y Wireless.

Una vez alcanzados los estándares impuestos por la ISO 17799 y apuntando a una mejora constante, se realizan pruebas de Hardening cuyo objetivo es llegar a un nivel superior de seguridad.

- **Nuevas Tecnologías**

BAICOM le ofrece la posibilidad de asesorarlo en la adquisición de nuevas tecnologías, de manera que pueda usted tener cubierto el aspecto seguridad a la hora de tomar la decisión de la elección de una nueva tecnología para su empresa.

- **Capacitación**

Teniendo en cuenta la criticidad de la concientización, hemos desarrollado planes de capacitación de "Awareness" de manera de poder concientizar a los distintos niveles de usuario de la empresa sobre la correcta utilización de los recursos, los riesgos de seguridad, las políticas de la empresa, etc.

Servicios > Normativas de Seguridad

Se plantea la generación de políticas y estándares desde cero o bien una revisión de las políticas actuales alineándolas con los objetivos de su empresa tomando como marco de referencia y ajuste las Normas ISO 17799 o SOX, según corresponda a su organización.

- **Políticas de Seguridad**

Muchas compañías basan su negocio y operación sobre Internet, en otras, Internet es un medio importante pero no crítico para la obtención de los objetivos corporativos.

Considerando estas diferencias, es que evaluaremos la criticidad de la información para cada proceso de manera de lograr una correcta acción de las políticas a implementar y la actividad de la empresa.

- **Manuales de Procedimiento**

- ✓ Garantiza que los procedimientos de seguridad sean uniformes y coherentes en toda la organización.

Pone por escrito la obligación de la empresa para con la seguridad de la información, previniendo posibles negligencias.

- ✓ Provee una guía práctica para la formación de los usuarios.
- ✓ Permite definir prioridades para la inversión en seguridad, concentrándose primero en las áreas con mayor necesidad.
- ✓ Asegura que la inversión en sistemas de seguridad se corresponde con las necesidades de la empresa, evitando desembolsos innecesarios y excesivos.
- ✓ Proporciona la confianza necesaria a la empresa y usuarios, demostrando que la seguridad es un factor que es importante dentro de la empresa y que se aborda correctamente.
- ✓ Alinea los objetivos departamentales al de la organización.

- **Estándares de Seguridad**

Nuestro expertise en la seguridad de plataformas y sistemas operativos es amplio, cada empresa tiene una problemática particular y ya sea por estrategia o costos diferentes son las combinaciones elegidas.

El alcance de nuestro trabajo, abarca tanto infraestructuras basadas en soluciones comerciales como así también aquellas basadas en un enfoque Open Source en donde es crítico asegurar los niveles de soporte o capacitación de empleados internos.

Soluciones

- Monitoreo Perimetral (IDS/IPS)
- Centralización y Correlación de Eventos
- Defensa Web
- Navegación Controlada
- Análisis de Consumo Web
- Antispyware de Red
- Antispam y Antivirus de Correo
- Firewalling
- Priorización de Trafico
- Balanceo de Carga
- Wifi

Soluciones > **Monitoreo Perimetral**

Administración centralizada

Control, monitoreo, actualización de patrones y análisis 7x24x365 desde BAISOC (BAICOM Artificial Intelligence Security Operation Center).

De ser necesario, los operadores pueden intervenir los equipos del cliente para crear e implementar políticas de supervisión y respuesta ante ataques.

Información concisa

Mediante la interfaz Web de la aplicación SEM (Security Event Manager), el cliente tiene acceso a un informe detallado de los incidentes ocurridos en tiempo real.

Performance y Confiabilidad

El Monitoreo Perimetral protege su red, consumiendo un mínimo de ancho de banda, sin interrumpir la disponibilidad de la red.

Bloqueo dinámico

Permite una confiable e inmediata respuesta ante ataques, bloqueando el tráfico no deseado.

Admite el tráfico autorizado sin interferir en la performance de la red.

MAP | Monitoreo Activo Perimetral

El servicio Activo está compuesto por un sensor ubicado estratégicamente por medio del cual se controlan y neutralizan todos los posibles ataques a las redes corporativas de los clientes en tiempo real.

Presenta la posibilidad de establecer acciones a realizar en caso de detectar ataques, evitando así que los mismos impacten sobre la organización, preservando la integridad de la red.

MPP | Monitoreo Pasivo Perimetral

El servicio Pasivo está compuesto por un sensor ubicado estratégicamente por medio del cual se controlan todos los posibles ataques a las redes corporativas de los clientes en tiempo real.

Este servicio, al ser no intrusivo, no afecta el funcionamiento de los dispositivos del cliente.

Soluciones > Centralización y Correlación de Eventos

Administración centralizada

Control, monitoreo y gestión de Logs multiplataforma desde BAICOM.

Información concisa

Mediante la interfaz Web de la aplicación SEM (Security Event Manager), el cliente tiene acceso a un informe detallado de los incidentes ocurridos en tiempo real.

Performance y Confiabilidad

Con las bases de datos duplicadas, no se altera la performance y se garantiza la total integridad y disponibilidad de la información.

Alarmas

El sistema Core cuenta con un agente inteligente que recorre los datos en la base, buscando patrones anómalos preconfigurados, o nuevos que se agreguen.

Además, los agentes, colectores y Core pueden generar alarmas, si se dan ciertas condiciones de errores.

Los siguientes eventos pueden ser disparadores de alarmas:

- cantidad excesiva de mensajes, con algunos valores en común entre ellos, en un intervalo de tiempo.
- superación de umbrales configurable de valores numéricos en el mensaje de log
- otros eventos del sistema (disco sin espacio, agentes caídos)

Soluciones > Navegación Controlada

Esta solución ayuda a las empresas a asegurarse de que sus empleados acceden de manera segura y productiva a los recursos de la red e Internet.

La misma presenta la ventaja de administración centralizada de nombres de usuarios y contraseñas ya que posee integración con LDAP.

Proporciona control de acceso, filtrado de URL's, contenidos y tipos de encabezados salientes.

Alguno de los controles que pueden realizarse son:

- Filtrado por redes locales
- Filtrado por polls de ips locales
- Filtrado de destinos
- Filtrado por horarios
- Redireccionamientos

Mejora la seguridad

Mejora la seguridad de la red proporcionando un punto de control para el tráfico de Internet registrando todas las transacciones realizadas por los usuarios.

Proporciona controles para limitar el acceso a documentos o sitios Web basándose en usuarios individuales, grupos, direcciones IP, hosts, etc.

Aumenta la performance de la red

Utiliza un modelo de caching altamente eficiente el cual distribuye los datos donde los usuarios los necesitan, reduciendo los tiempos de espera.

Caching flexible y escalable

Proporciona un eficiente y transparente almacenamiento de información Web bajo demanda.

El mismo es actualizado periódicamente para asegurar de tener siempre el último contenido disponible.

Mejora la productividad

Por defecto, el sistema no permite contactarse con personas fuera de la LAN de la organización.

Encriptación

Todas las comunicaciones se realizan de forma encriptada a fin de asegurar la integridad y confidencialidad de la información

Soluciones > Análisis de Consumo Web

La solución de permita obtener reportes de la estructura actual de acceso a Internet de manera personalizada según los requerimientos del departamento de Sistemas y en forma On Line.

La información será obtenida de la base de datos en el que actualmente se depositan los logs de actividad del uso de Internet de los usuarios.

A partir de esta información y teniendo los parámetros definidos sobre las consultas que se desean automatizar, se personalizara la aplicación que generara los reportes solicitados y podrán ser consultados desde la red interna de la empresa utilizando un navegador de Internet u exportando los datos a un Excel en formato CSV (texto delimitado por comas).

Entre los reportes mas destacados podemos enumerar:

- ✓ Sitios mas visitados
- ✓ Usuarios que realizan mas consultas
- ✓ Paginas web por usuario
- ✓ Trafico por Ip
- ✓ Trafico por Host
- ✓ Reportes de consumo pico
- ✓ Reportes por tipo de contenido
- ✓ Reportes de performance

Soluciones > Antispam y Antivirus de Correo

La solución abarca la implementación de los sistemas de Antivirus y Antispam para evitar la llegada de virus por email y de correo no deseado.

Los servidores de correo Postfix contarán con un sistema de Antivirus y Antispam, el cual, después de asegurar que los correos no contienen virus o no son reconocidos como Spam, serán enviados al servidor Microsoft Exchange.

Estos sistemas cuentan con soporte ilimitado de mailboxes y la actualización de patrones se realiza automáticamente y no posee cargos adicionales por las mismas.

Características de Antivirus

Se utilizará el Antivirus ClamAV el cual presenta las siguientes características:

- ✓ Scanner de línea de comandos
- ✓ Fast, multi-threaded daemon
- ✓ Actualización de base de datos con soporte para digital signatures
- ✓ Biblioteca C de scanner de virus
- ✓ Detección de más de 28000 virus, worms y trojan's
- ✓ Análisis de archivos RAR (2.0), Zip, Gzip, Bzip2, Tar, MS OLE2, MS Cabinet files, MS CHM (HTML comprimido), MS SZDD
- ✓ Soporte para mbox y Maildir
- ✓ Actualización de patrones sin cargo
- ✓ Sin límite de casillas

Características de Antispam

Se utilizará el Antispam SpamAssassin el cual presenta las siguientes características:

Es un filtro extensible de email que se utiliza para identificar Spam. Utiliza una amplia gama de las pruebas avanzadas de análisis heurístico y estadístico en los encabezados de email y el texto del cuerpo del email para identificar el "spam", también conocido como correo no deseado.

Las tácticas de identificación de spam utilizadas son:

- ✓ Análisis de encabezados
- ✓ Análisis de texto
- ✓ Listas negras
- ✓ Clasificador para aprendizaje
- ✓ Bases de datos Hash distribuidas
- ✓ Actualización de patrones sin cargo
- ✓ Sin límite de casillas

Soluciones > **Firewalling**

Con el objeto de implementar un esquema de alta disponibilidad, la solución puede contar con un esquema de backup que garantizará el constante funcionamiento del esquema de seguridad deseado.

Es decir, un esquema de 2 firewalls en cluster, de manera que puedan balancear carga y tener un esquema de failover, de manera de seguir funcionando por más que uno de los equipos falle.

La solución soporta todos los protocolos y servicios comúnmente utilizados como HTTP, SMTP, FTP, SQLNet y Telnet, como así también aplicaciones multimedia.

Permite la generación de reglas de NAT y PAT, que podrán definirse, diferenciando protocolo, IP destino / IP origen, mascara IP origen/ IP destino, puerto destino / puerto origen.

También soporta, mediante el Proxy Squid, la autenticación, autorización y accounting de cierto tipo de tráfico (mínimo http y FTP) a través de Radius o TACACS.

Posee mecanismos incorporados en el software para detener ataques basados en el "flooding" de SYN.

Será posible actuar en la red como un "next hop" o como en modo transparente y soportar la técnica de "Stateful Inspection"

Soporta 802.1q en todas sus interfaces.

Los servicios de QoS con soporte y rendimiento equivalente al LLQ y limitación de ancho de banda serán soportados, así como el protocolo OSPF, al considerarse necesarias las siguientes funcionalidades:

- ✓ Autenticación de paquetes mediante MD5
- ✓ Predistribución de rutas entre procesos OSPF (incluyendo rutas OSPF, estáticas y directamente conectadas)

También DHCP Server, Client y Relay. Como la gestión vía Web, SNMP y Syslogs. La autorización de comandos por niveles localmente o mediante AAA.

Soluciones > Priorización de Trafico

Con la ayuda de esta solución, usted podrá manipular la priorización de tráfico de su empresa, de manera de poder garantizar la calidad de servicio necesaria para sus implementaciones y no necesariamente generar gastos adicionales en la contratación de mayor ancho de banda.

Algunas de las funcionalidades que tiene son:

Classifier/Marker:

Identifica los grupos de paquetes que recibe un servicio específico y analiza la información sobre la clase de paquete, procedencia o ambas.

La clasificación puede ser simple (asigna más recursos a los paquetes recibidos en una interfaz en particular) o compleja (asigna un porcentaje del ancho de banda disponible a los paquetes destinados a una dirección en particular).

Queuing:

Protege y aísla el tráfico para cerciorarse de que el tráfico más importante sea manejado apropiadamente.

Buffer Management:

Define que políticas se utilizaran si el ancho de banda se satura, asegurando que el tráfico de alta prioridad pase a través del equipo.

Shaping:

Restringe cierto tráfico para asegurarse que las aplicaciones no envíen tráfico más allá del ancho de banda que les fue asignado.

Soluciones > Balanceo de Carga

BAICOM ofrece servicios de Balanceo de Carga y Conmutación por contenido, sumado a los servicios de Cache Engine, Áreas de Almacenamiento (SAN) y Conexiones Seguras (SSL).

Provea a sus sitios la capacidad de trabajar distribuidos, de crecer en forma transparente sin preocuparse por nada más que en la utilización de los servicios en una forma completamente segura.

Soluciones > Wifi

La solución de WiFi es un Gateway para redes de acceso público que combina un Access Point inalámbrico, un Router de IP y un Controlador de Acceso para redes WiFi.

Permite tener el control de autenticación, mantenimiento de cuentas y rutéo hacia redes LAN o Internet en un solo appliance.

Presenta tres modos de implementación:

- ✓ Como un sistema de venta prepaga de minutos de Internet
- ✓ Permite instalar varios HIS en distintas ubicaciones centralizando las tareas de billing y accounting en un servidor remoto
- ✓ Permite la autenticación a servidores LDAP o RADIUS para acceder a los recursos corporativos en forma inalámbrica

Acceso Público:

- Home Page redirection (pre y post autenticación)
- Administración de ancho de banda

Autenticación y Autorización:

- Autenticación por medio de MAC Address
- Asignación de IPs mediante DHCP

Diferenciación del Servicio:

- Tráfico con o sin encriptación

Administración:

- Consola de información y control vía Web
- Consola de monitoreo de estado del HIS
- Estadísticas de concurrencia
- ABM de QoS (Quality of Service)

Contacto

Tel/Fax: +54 11 5032 3366

Email Institucional: info@baicom.com

Email Recursos Humanos: rrhh@baicom.com

Sitio Web: www.baicom.com

Riobamba 436 8vo Ofic. 16 (C1025ABJ)
Capital Federal - Buenos Aires - Argentina