HasarServicios

Seguridad informática

Servicio de seguridad informática

GrupoHasar

Introducción

El Servicio de Seguridad informática tiene como objetivo elevar los niveles de protección y seguridad de red a los más altos estándares de la industria, para que su organización pueda hacer un uso más eficiente y seguro de internet.
Los pilares de nuestro servicio se podrían sintetizar en el intercambio de información sin comprometer la seguridad, el ahorro de recursos y la optimización de las comunicaciones. Permitiendo el uso de internet de forma segura, evitando los altos costos de los enlaces dedicados, y de la optimización del licenciamiento en seguridad (concentrando múltiples productos en este servicio).

Seguridad informática

HasarServicios

Resolviendo problemas comunes tales como

- Falta de recursos humanos para afrontar una adecuada gestión de la seguridad de la información.
- Recursos económicos para desarrollar una estrategia tecnológicas acorde a sus necesidades.
- Falta de experiencia que contribuyan a la prevención de eventos de seguridad.

GrupoHasar

HasarServicios

Por que contratar el servicio de seguridad informática?

01

► Porque mi empresa no cuenta con un área de seguridad informática, o personal técnico capacitado o con tiempos disponibles.

02

► Porque necesito saber qué está pasando con la red: entender por qué la red sigue lenta o saber a qué sitios están accediendo los usuarios y qué tipo de aplicaciones están usando.

03

► Porque la información es vital para mi negocio y no tengo una estrategia de Prevención, Detección y Mitigación de infecciones.

04

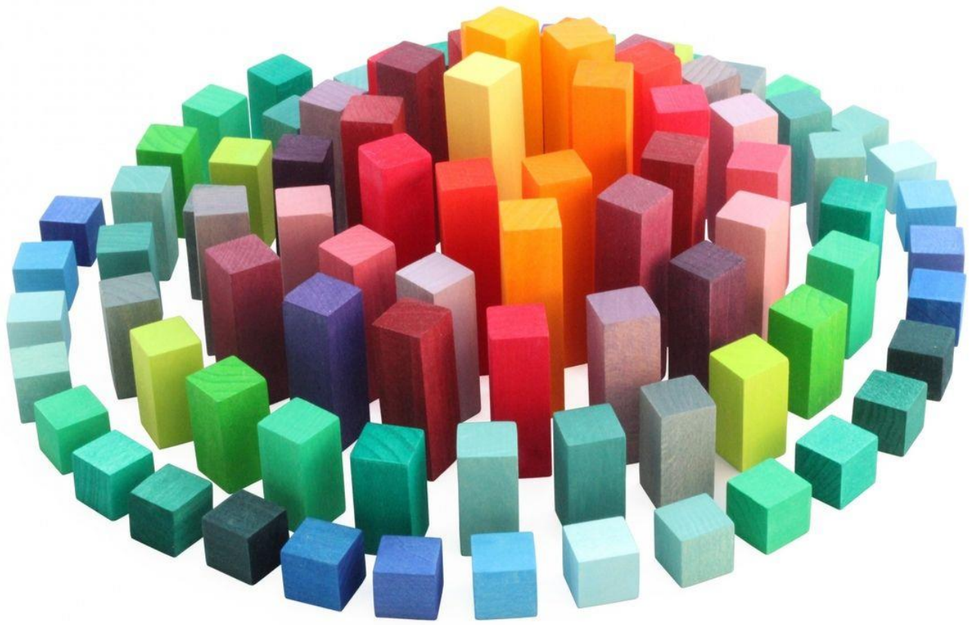
► Porque no cuento con mecanismos de prevención de fuga de información.

05

► Porque el enfoque tradicional de antivirus no detecta una amenaza persistente y avanzada, por lo que necesito de una tecnología que permita emular un sistema igual al que utilizo y detectar, por ejemplo, si una amenaza o no.

GrupoHasar

Componentes



- Equipamiento (en comodato con licenciamiento activo durante la vigencia del contrato).
- Soporte (reactivo, ver descripción en Anexo correspondiente).
- Administración (reactivo y proactivo, ver descripción en Anexo correspondiente).
- Monitoreo continuo (requiere “Dimensión”).
- Análisis de eventos de seguridad (requiere “Dimensión”).
- Diagnóstico de seguridad (requiere “Dimensión”).
- Reportes de gestión on-demand y “customizables” (requiere “Dimensión”).
- Reposición Inmediata en caso de falla del equipamiento.
- Protección de la inversión (posibilidad de reemplazo del equipamiento actual por uno acorde a los nuevos requerimientos de la empresa sustituyendo la cuota mensual por la correspondiente, previo pago de una cuota extra del valor del nuevo equipo).
- Opcional: Hosting de Dimensión.

Total security vs. Basic security

Basic security contiene

- **Servicio de Prevención de Intrusiones**

Ofrece protección integrada de las vulnerabilidades maliciosas, incluyendo los desbordamientos del búfer, inyecciones de código SQL y ataques de scripts entre sitios.

- **Control de aplicaciones**

Mantiene alejadas las aplicaciones improductivas, inadecuadas y peligrosas, y posibilita el filtrado granular dentro de las mismas (permitiendo determinadas funcionalidades dentro de una aplicación).

- **WebBlocker**

Controla el acceso a los sitios que alojan materiales cuestionables o representan riesgos de seguridad para la red.

- **SpamBlocker**

Ofrece una protección continua contra los correos electrónicos peligrosos y no deseados.

- **Gateway antivirus**

Analiza el trafico en todos los protocolos principales para detener amenazas.

- **Reputation enabled defense**

Garantiza una exploración web más rápida y segura con búsqueda basada en la nube.

- **Network discovery**

Brinda a los administradores la completa visibilidad de todos los dispositivos conectados.

Total security vs. Basic security

Total security AGREGA

- **Bloqueador de APT**

Usa un espacio aislado basado en la nube con emulación de todo el sistema para detectar y bloquear malware y ataques de tipo zero-day.

- **Prevención de pérdida de datos**

Inspecciona automáticamente los datos en movimiento para detectar infracciones de la política corporativa frente a robo o fuga de información.

- **Dimension command**

Es un conjunto de herramientas de gestión para que los profesionales no solo vean lo que está sucediendo en la red, sino que puedan tomar una acción inmediata desde el panel de control.

- **Servicio de detección y respuesta ante amenazas**

Correlaciona eventos de seguridad de la red y de extremos con inteligencia ante amenazas para detectar, priorizar y activar medidas inmediatas destinadas a detener los ataques de malware incluyendo un módulo específico contra *Ransomware*.

Visibilidad

Tanto el gerente que necesita saber en qué están utilizando su tiempo los usuarios cuando están en internet, como de los técnicos que proveen servicios y requieren de información para poder dar soporte, la visibilidad se ha vuelto particularmente importante. En cualquiera de las modalidades de licenciamiento, nuestro servicio incluye **Dimensión**, una solución de visibilidad de seguridad de red que brinda un conjunto de herramientas de generación de informes y visibilidad de grandes datos que identifica y extrae tendencias y problemas de seguridad claves al instante, brindando políticas importantes de seguridad en toda la red.

En síntesis, permitirá responder las siguientes preguntas

- ¿Por qué está lenta la red? ¿Necesito más ancho de banda o lo estoy malgastando?
- ¿Tengo un enlace caído o estoy distribuyendo la carga en los enlaces contratados?
- ¿Quién es el usuario o equipo que está consumiendo más ancho de banda?
- ¿De dónde provino la última infección/ataque?
- ¿Hay patrones de tráfico poco habituales?
- ¿Cuál es el sitio web más popular?
- ¿Qué aplicaciones está usando un usuario específico?

MUCHAS GRACIAS

HasarServicios

www.grupohasar.com/hasar-servicios

www.grupohasar.com

GrupoHasar