Ciberseguridad 2026

Como adaptarse a la nueva era de la defensa autónoma

Checklist & autoevaluación

Heimdall

www.heimdallagency.com

2026: El año de la defensa autómata

El mundo de la ciberseguridad está entrando en una transformación profunda.

Los ataques ya no son manuales ni aislados: son automáticos, persistentes y masivos. Se propagan con IA, buscan debilidades sin intervención humana y se mueven con una velocidad imposible de seguir con métodos tradicionales.

Las empresas líderes globales (Microsoft, Google, CrowdStrike, Palo Alto, SentinelOne) ya comenzaron una transición hacia un nuevo modelo:
"Security Autopilot": Seguridad autónoma, visible y adaptativa.

¿Qué significa esta nueva era?

- **Los ataques no esperan:**
  - La detección debe ser continua y el análisis, inmediato.
- **El volumen supera al humano:**
  - La automatización dejará de ser un lujo, será el estándar mínimo.
- **La tecnología sola no alcanza:**
  - Quien no tenga procesos maduros y visibilidad real queda expuesto.
- **La regulación será más estricta:**
  - Europa, Estados Unidos y LATAM exigirán trazabilidad, respuesta documentada y madurez demostrable.
- **El ataque escala con IA:**
  - La defensa también debe escalar con IA, SOAR y análisis contextual.
- **La IA acelera. El criterio humano decide:**
  - La defensa moderna exige ambos.

En resumen:
2026 será el año donde las organizaciones necesitarán madurez, visibilidad total y capacidad de respuesta autónoma para sobrevivir en un ecosistema donde las amenazas ya no se gestionan manualmente.
Hoy no importa solo si tenés seguridad.
Importa si tu seguridad puede moverse más rápido que los ataques.

Heimdall

Preparate para esta nueva era con Heimdall

Heimdall está alineado desde sus inicios con el modelo de seguridad que recién ahora comienza a imponerse en el mundo.

01 vCISO: Madurez y dirección estratégica

Nuestro servicio de vCISO ayuda a las empresas a migrar del modelo tradicional hacia un modelo moderno basado en:

- Madurez operativa real
- Roadmap estratégico 2026
- Zero Trust práctico
- Gobernanza clara y medible
- Procesos que fortalecen la autonomía de defensa

El vCISO traduce la complejidad técnica en decisiones simples que la dirección puede entender y aprobar.

02 SOC 24x7: Visibilidad y respuesta inteligente

Nuestro SOC está construido sobre la misma arquitectura conceptual de las grandes plataformas globales, pero adaptado a LATAM y a costos accesibles:

- Detección continua
- Correlación inteligente de eventos
- Investigación automatizada
- Playbooks SOAR
- Threat hunting proactivo
- Gestión de incidentes con trazabilidad total

03 Cultura y personas: La otra mitad de la ecuación

La tendencia global muestra que más del 80% de los ataques exitosos ocurren por un error humano.
Por eso incluimos:

- Simulaciones de phishing
- Formación práctica
- Evaluación del riesgo humano
- Microaprendizajes continuos

Porque la defensa autónoma no es solo tecnología:
Es personas + procesos + inteligencia + automatización.

Heimdall

CHECKLIST 2026

12 Controles escenciales para un 2026 seguro, visible y preparado para la nueva era

- [ ] **Estrategia de Ciberseguridad 2026 (Plan + Prioridades)**
  ¿Tu empresa sabe qué proteger primero y por qué? Definí prioridades mínimas: qué riesgos son críticos, qué iniciativas no pueden postergarse y cómo se medirá el avance.
- [ ] **Visibilidad real de tu infraestructura**
  No se puede defender lo que no se ve. Firewalls, servidores, usuarios, nube: todo debe generar registros y estar monitoreado de manera continua y centralizada
- [ ] **Detección continua y alertas tempranas**
  La pregunta clave no es qué herramienta tenés sino qué tan rápido te enterás cuando algo anda mal.
  Activá alertas críticas o implementá monitoreo especializado (SOC).
- [ ] **Gestión de usuarios y accesos (Zero Trust práctico)**
  El principio 2026: nadie accede a más de lo que necesita.
  Eliminá cuentas inactivas, revisá permisos, activá MFA y restringí accesos privilegiados.
- [ ] **Análisis y corrección de vulnerabilidades**
  Detectar sin corregir es igual a no tener seguridad.
  Ejecutá escaneos mensuales o continuos y corregí según criticidad real, no según cantidad.
- [ ] **Cultura de ciberseguridad y factor humano**
  La automatización es clave, pero el criterio humano sigue siendo la diferencia.
  Capacitación breve, simulaciones de phishing y concientización periódica es la clave.
- [ ] **Clasificación y protección de información**
  No todos los datos valen lo mismo.
  Identificá lo crítico, protegelo con cifrado y controlá dónde se almacena.
- [ ] **Copias de seguridad seguras y probadas**
  No alcanza con tener backups: tenés que poder restaurarlos.
  Ejecutá al menos una prueba trimestral de restauración + copias en entornos aislados.
- [ ] **Plan de respuesta ante incidentes**
  Un incidente sin plan puede terminar peor.
  Definí roles, contactos, pasos y responsabilidades.
- [ ] **Seguridad en redes e internet**
  Los errores de red siguen siendo la puerta de entrada favorita.
  Revisá puertos abiertos, configuraciones inseguras, accesos remotos y contraseñas por defecto.
- [ ] **Automatización y procesos repetibles (SOAR o flujos manuales)**
  2026 exige velocidad y consistencia.
  Automatizá tareas recurrentes y documentá procesos para que no dependan de una sola persona.
- [ ] **Integración entre seguridad, IT y negocio**
  La ciberseguridad no puede estar aislada. Programá reuniones mensuales para definir prioridades compartidas y establecer KPIs que hablen el lenguaje del negocio.

Heimdall

Autoevaluación

Medí el nivel de preparación de tu empresa para enfrentar la nueva era de ciberseguridad

Cómo usar esta hoja

Para cada uno de los 12 controles del checklist, marcá en qué nivel se encuentra tu empresa:

0 = No planificado
1 = Planificado
2 = En implementación
3 = Implementado

Al finalizar, sumá el puntaje total para conocer tu nivel de riesgo actual y un plan de acción recomendado.

Control evaluado	0	1	2	3
1. Estrategia de ciberseguridad 2026	☐	☐	☐	☐
2. Visibilidad real de tu infraestructura	☐	☐	☐	☐
3. Detección continua y alertas tempranas	☐	☐	☐	☐
4. Gestión de usuarios y accesos (Zero Trust)	☐	☐	☐	☐
5. Análisis y corrección de vulnerabilidades	☐	☐	☐	☐
6. Cultura de ciberseguridad y factor humano	☐	☐	☐	☐
7. Clasificación y protección de información	☐	☐	☐	☐
8. Copias de seguridad seguras y probadas	☐	☐	☐	☐
9. Plan de respuesta ante incidentes	☐	☐	☐	☐
10. Seguridad en redes e internet	☐	☐	☐	☐
11. Automatización y procesos repetibles	☐	☐	☐	☐
12. Integración entre seguridad, IT y negocio	☐	☐	☐	☐

Heimdall

Interpretá tu puntaje

Sumá todos los valores

🔴 **Riesgo Crítico (0 a 12 puntos)**
Tu organización está altamente expuesta.
No hay visibilidad, no hay capacidad de respuesta y los controles básicos no están funcionando.
Plan de acción prioritario:

- Implementar proceso de revisión periódica de logs urgente
- Activar MFA al menos en accesos críticos
- Ejecución inmediata de un escaneo de vulnerabilidades
- Crear un plan de respuesta ante incidentes
- Construir el roadmap 2026 basado en prioridades

🟠 **Riesgo Alto (13 a 24 puntos)**
Existen esfuerzos aislados, pero no hay madurez ni articulación real.
La probabilidad de sufrir un incidente significativo es muy alta.
Plan de acción prioritario:

- Centralizar visibilidad y activar alertas de interés
- Establecer procesos mínimos y políticas formales
- Relevar accesos y aplicar Zero Trust básico
- Realizar simulaciones de phishing y capacitaciones periódicas
- Integrar un proceso de monitoreo básico de logs

🟡 **Riesgo Medio (25 a 30 puntos)**
Hay una base sólida, pero faltan automatización, estandarización y capacidad de respuesta rápida.
Plan de acción prioritario:

- Automatizar tareas repetitivas y alertas manuales
- Definir procesos formales IT y documentarlos
- Validar backups y pruebas de restauración trimestrales
- Avanzar hacia detección basada en comportamiento
- Actualizar roadmap en base a prioridades

🟢 **Riesgo Bajo (31 a 36 puntos)**
Tu empresa tiene una base madura y está bien encaminada hacia la nueva era de seguridad.
El siguiente paso es lograr autonomía operativa.
Plan de acción prioritario:

- Incorporar SOAR y automatizaciones avanzadas
- Ejecutar threat hunting regular
- Revisar Zero Trust y accesos privilegiados
- Integrar métricas de resiliencia (MTTD, MTTR, tiempo de impacto evitado)
- Realizar auditorías internas trimestrales

Heimdall

Evaluarse es el primer paso
Mejorar es una decisión

Si querés que nuestro equipo revise tu resultado y te prepare un plan de acción personalizado para 2026 contactanos!.

¿Querés seguir fortaleciendo tu estrategia?
Accedé a todos nuestros manuales gratuitos para que tu empresa esté realmente preparada:

Todo lo que necesitás para anticiparte a la nueva era de ciberseguridad, en un solo lugar.

Contacto

Descargas

Contactanos

ARG: +54 11 5235 2388
USA: +1 3074 151 037
info@heimdallagency.com
www.heimdallagency.com

Heimdall