



# Informe sobre amenazas

McAfee Labs

## Robo de información

Los qué, cómo y quiénes de las fugas de datos.



**El 53 %**

de los ataques a la seguridad los descubre alguien ajeno a la organización atacada.



**El 62 %**

de los ataques a la seguridad afectan a los datos personales de clientes o empleados.



**Casi el 40 %**

de las pérdidas de datos incluyen algún tipo de soporte físico.



**El 68 %**

de los ataques a la seguridad comportan pérdidas de datos que por normativa exigen generar un informe al respecto.



**Más del 25 %**

de las empresas no vigilan el acceso a la información de empleados o clientes.



**Solo el 37 %**

de las empresas supervisan los endpoints, incluida la actividad de usuarios y soportes físicos.

## Crisis en Urgencias

El ransomware infecta los hospitales.

Los autores de ransomware atacan hospitales porque



**Sistemas heredados**

Utilizan sistemas heredados con seguridad insuficiente.



**Dispositivos médicos**

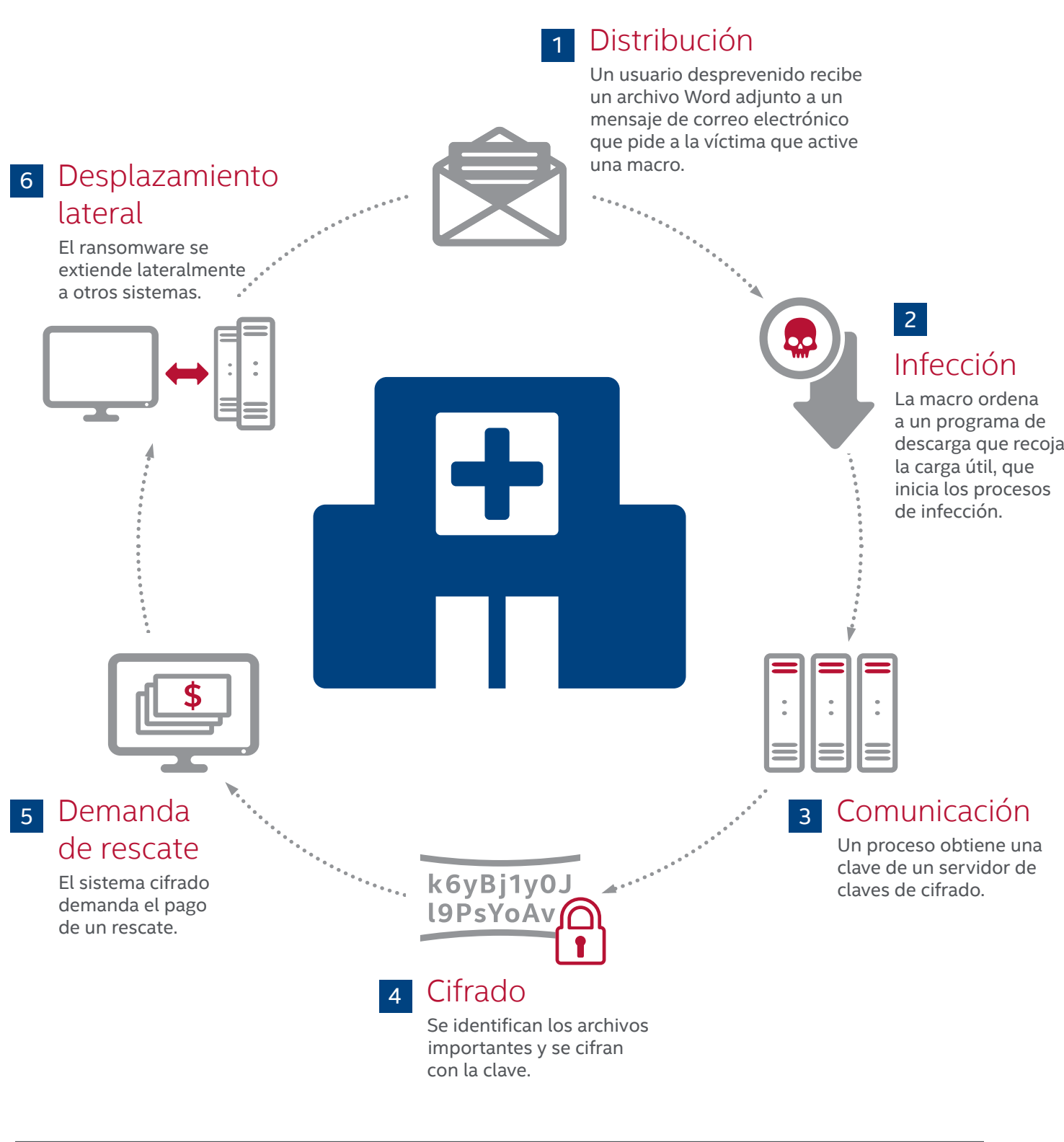
Emplean dispositivos médicos con seguridad insuficiente o inexistente.



**Atención al paciente**

Necesitan acceso inmediato a la información para prestar el mejor servicio posible de atención al paciente.

Fases de un ataque de ransomware a un hospital



**19 hospitales**

Al menos 19 hospitales fueron infectados por ransomware durante el 1.º y el 2.º trimestre.



**17 000 \$**

En el 1.º trimestre, un hospital de California pagó 17 000 \$ para recuperar sus archivos y sistemas después de cinco días laborables de inactividad.



**100 000 \$**

Intel Security descubrió que, durante el 1.º trimestre, un grupo relacionado de ataques selectivos a hospitales generó unos 100 000 \$ en pagos de rescates.

## Análisis

Uso del aprendizaje automático para detener a los agresores.

El aprendizaje automático es la acción de automatizar los análisis que utilizan ordenadores para aprender con el tiempo.



**Análisis preceptivo**

"Se recomienda esto porque ocurrirá esto otro"



**Análisis descriptivo**

"¿Qué ha ocurrido?"



**Análisis predictivo**

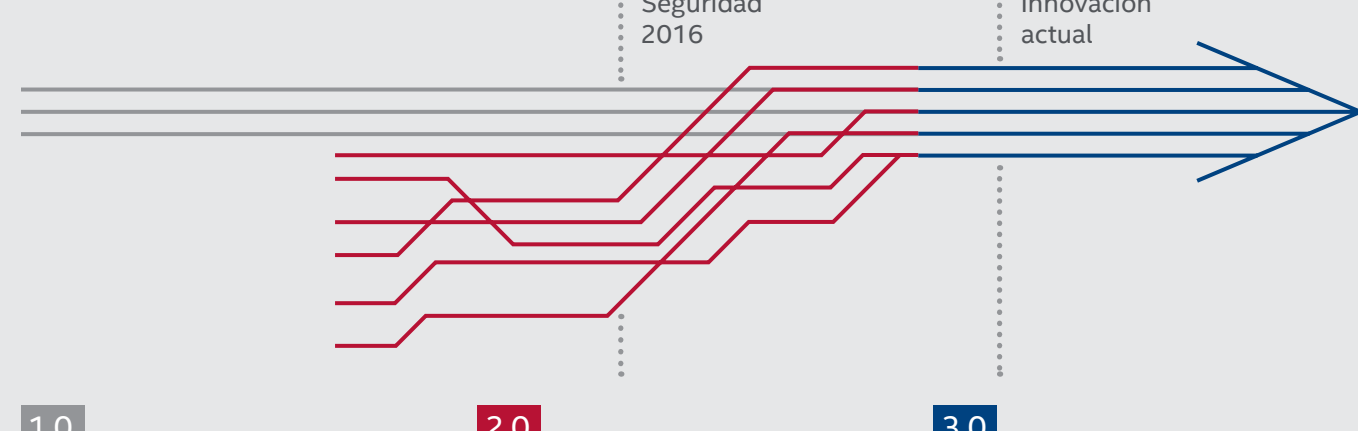
"¿Qué ocurrirá?"



**Análisis de diagnóstico**

"¿Por qué ha ocurrido?"

La evolución de los análisis



**1.0**

**Análisis 1.0**

- Conjuntos de datos estructurados de fuentes internas
- Análisis descriptivos y de diagnóstico
- Reactivos pero útiles

**2.0**

**Análisis 2.0**

- Big Data: grandes volúmenes de datos complejos y sin estructurar
- Datos de fuentes internas y externas

**3.0**

**Análisis 3.0**

- Uso de aprendizaje automático con Big Data, aprendizaje profundo y computación en la nube
- Detección e información rápidas y proactivas

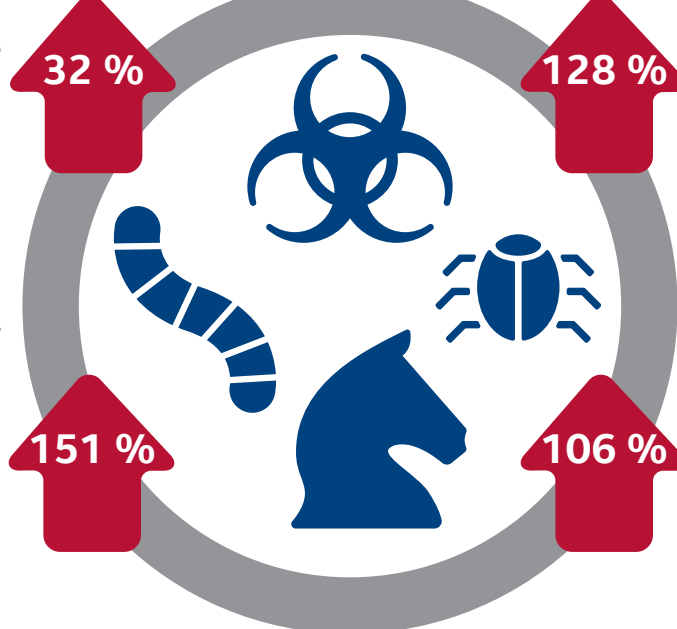
Fuente: adaptada del International Institute for Analytics.

## Estadísticas sobre amenazas

Hay 316 amenazas nuevas cada minuto, o más de 5 cada segundo.

**Malware**

El número de muestras nuevas de malware registrado en el 2.º trimestre —41 millones— es el segundo más alto jamás contabilizado. Durante el pasado año, el "zoo" de malware de McAfee Labs creció un 32 % hasta superar los 600 millones de muestras.



**Ransomware**

El número de muestras nuevas de ransomware —más de 1,3 millones— fue el más alto jamás registrado en el 2.º trimestre. El año pasado, el total de ransomware creció un 128 %.

**Malware para móviles**

El número de muestras nuevas de malware para móviles —casi 2 millones— fue el más alto jamás registrado en el 2.º trimestre. El año pasado, el total de malware para móviles creció un 151 %.

**Malware basado en macros**

Los nuevos trojanos de descarga son responsables del incremento de más de un 200 % de nuevo malware basado en macros en el 2.º trimestre. El año pasado, el total de malware basado en macros creció un 106 %.

## McAfee Global Threat Intelligence

McAfee GTI recibió de media 48,6 millones de consultas al día.



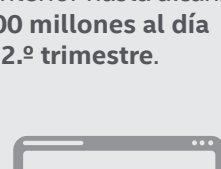
**100 millones**

Las protecciones de McAfee GTI contra URLs maliciosas crecieron ligeramente con respecto al año anterior hasta alcanzar los 100 millones al día en el 2.º trimestre.



**30 millones**

Las protecciones de McAfee GTI contra programas potencialmente no deseados bajaron un 83 % con respecto al año anterior hasta alcanzar los 30 millones al día en el 2.º trimestre.



**104 millones**

Las protecciones de McAfee GTI contra archivos maliciosos bajaron un 77 % con respecto al año anterior hasta alcanzar los 104 millones al día en el 2.º trimestre.



**29 millones**

Las protecciones de McAfee GTI contra direcciones IP peligrosas muestran el mayor aumento en los dos últimos años, 29 millones al día, lo que supone un incremento del 128 % con respecto al trimestre anterior.



Informe de McAfee Labs sobre amenazas

Septiembre de 2016

Visite [www.mcafee.com/September2016ThreatsReport](http://www.mcafee.com/September2016ThreatsReport) para ver el informe completo.

