ESET Security Report

LATINOAMÉRICA 2012

- Argentina
- Bolivia
- Brasil
- Chile
- Colombia
- Costa Rica
- Ecuador
- El Salvador
- Guatemala
- Honduras
- México
- Nicaragua
- Panamá
- Paraguay
- Perú
- Rep.Dominicana
- Uruguay
- Venezuela

60%

Más del 60% de las empresas se preocupa por la fuga de información.

Todos los años ESET Latinoamérica participa en prestigiosos eventos en toda la región, entre ellos, el Technology Day que se realiza en países de Centroamérica como: Costa Rica, Guatemala, El Salvador, Nicaragua, Honduras, Panamá y República Dominicana. También en Segurinfo, un evento de similares características realizado para la región sudamericana en Argentina, Chile, Perú y Uruguay, además de participar en eventos en países de toda la región. En los mismos se realizan encuestas a ejecutivos de empresas relacionados con el área de la seguridad y tecnología de la información. Durante el 2011 participaron **3397 ejecutivos** de toda América Latina contribuyendo con sus opiniones y experiencias para poder recopilar la información utilizada para construir este informe.

Por tal motivo, a partir de los estudios realizados, se lleva adelante un análisis de la situación actual de la seguridad de la información en el mundo corporativo con el objetivo de identificar el comportamiento de las empresas frente a esta temática y marcar algunas tendencias en la región.

Antes de poder comenzar con el análisis de toda la información brindada por los gerentes a lo largo del año, es interesante tomar en cuenta algunos hechos que marcaron el año y su consecuencia para las empresas del mundo tecnológico. Es importante tener en cuenta este escenario al analizar algunas de las consultas que se realizaron a los ejecutivos para poder comprender mejor los resultados.

Para fines del 2010, ocurrieron una serie de hechos que tuvieron un impacto muy importante tanto en las empresas como en los usuarios finales durante todo el año siguiente. En noviembre de 2010 Wikileaks inició la publicación de 250.000 cables confidenciales que contenían la comunicación entre Estados Unidos y sus embajadas alrededor del mundo. Este hecho, generó un gran revés para la plataforma de archivos confidenciales ya que terminó perdiendo el apoyo de muchos organismos financieros que la sustentaban para poder mantener sus servicios operativos.

Debido a algunos bloqueos impuestos por entidades financieras a Wikileaks, surgió un grupo de hacktivistas que salió a apoyarlos. Los hacktivistas son grupos de personas que luchan por un ideal político o social realizando acciones de protesta digital, muchas veces ilícitas, sin manifestar deseos económicos. Este grupo, se identifica bajo el nombre de Anonymous y realizó diversos ataques de denegación de servicio, fugas de información, entre otras; a las compañías que se mostraban en contra a las publicaciones de Wikileaks. Esto generó una cierta incertidumbre en el ambiente corporativo ya que grandes compañías fueron afectadas a través de estos ataques. Debido a eso, muchas empresas han incrementado su preocupación por la fuga de información como se observa en el desarrollo de este informe.

Las preocupaciones de las empresas

De acuerdo a los datos relevados, se puede observar cuáles son las mayores preocupaciones por parte de los ejecutivos de las empresas de la región con respecto a la seguridad de la información. La mayoría de ellos coincide que hay tres factores de mayor relevancia para las empresas en Latinoamérica: El malware, la fuga de información y las vulnerabilidades en las aplicaciones.

Analizando los datos recopilados en mayor detalle, se puede observar en la siguiente gráfica, que la fuga de información o pérdida de datos es la mayor preocupación para más de un 60% de los encuestados:

>> Gráfico 1. ¿Cuáles son sus mayores preocupaciones en la SI?

A pesar de que el año pasado ya había una tendencia similar con respecto a esta amenaza, se puede observar que ahora existe mayor inquietud de forma generalizada con la fuga de información, ya que la preocupación se incrementó de **42.52% a 60.88%.** Lo que indica también que hay mayor necesidad de

18%

La preocupación por la fuga de información se incrementó en un 18% con relación al año anterior.

46%

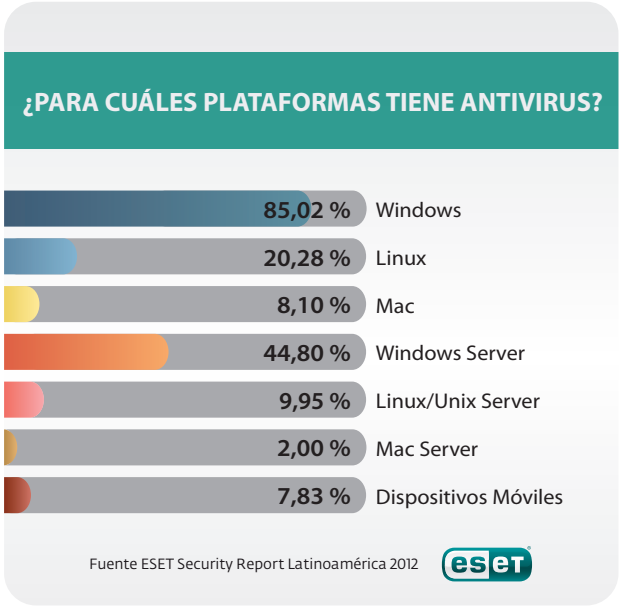
El malware afecta al 46% de las empresas en América Latina.

tomar acciones correctivas para mitigar estos casos. Para eso, la educación y concientización de los empleados es uno de los pilares fundamentales con el trato de la fuga de información.

>> Gráfico 2. ¿Ha sufrido incidentes de seguridad en los últimos 12 meses?

Con respecto a los incidentes sufridos el último año, los encuestados afirman con amplio margen sobre las demás opciones que el *malware* continúa a la vanguardia entre los incidentes que más afectan a las organizaciones en la región latinoamericana. Por otra parte, el robo de información, que representa la mayor preocupación para las empresas, afecta a menos del **10%** de ellas. Esto podría llevar a que muchas empresas no estén concentrando sus esfuerzos en la amenaza que más atenta contra sus organizaciones.

Otros números, sin embargo, no reflejan graves incidentes a pesar de la gran preocupación que representan para las empresas. Por ejemplo, el fraude interno y externo, es una preocupación que alcanza al **40 por ciento** de los encuestados, no obstante solo afecta al **6%** de ellos. En esta temática, muchos de los encuestados coinciden que el fraude interno es más nocivo, ya que es más difícil de prever y el impacto puede ser muchas veces mayor. Además, muchos ejecutivos manifiestan que se trata de empleados desleales a la organización y por lo tanto consideran que la falta de confianza agrava los hechos en una cuestión de esta índole.



>> Gráfico 3. ¿Para cuáles plataformas tiene antivirus?

Cuando los ejecutivos fueron preguntados acerca de cuáles plataformas en su empresa están protegidas, **menos del 8%** de ellos respondió afirmativamente con respecto a los dispositivos móviles. Lo que indica que muchas empresas que utilicen *smartphones* corporativos podrían ser vulnerables a alguna de las amenazas existentes. Es importante tener en cuenta que estos dispositivos normalmente son usados para leer el correo electrónico corporativo, utilizar redes sociales, navegar por Internet, entre otros; lo que implica el manejo de datos sensibles por parte del usuario tanto del punto de vista personal como corporativo. De no ser debidamente utilizado, esta información podría caer en manos de personas mal intencionadas y ocasionar serios daños a la empresa.

Además, a partir del año 2011, se ha observado la consolidación de los códigos maliciosos en los dispositivos móviles, mayoritariamente en Android. Con más de 400 millones de dispositivos en todo el mundo, Android posee el mayor *market share* del mercado lo cual vuelve a esta plataforma mucho más codiciada por los desarrolladores de malware. Esto trae aparejado que de los códigos maliciosos analizados para esta plataforma, cerca del **90%** aparecieron en el año pasado y solo el restante durante el 2010. Desde el punto de vista corporativo, es un hecho fundamental ya que, según los ejecutivos de la región, aproximadamente el **92%** de estos dispositivos móviles corporativos todavía no cuenta con una solución de seguridad que los proteja. Este se puede deber a que las empresas toda-

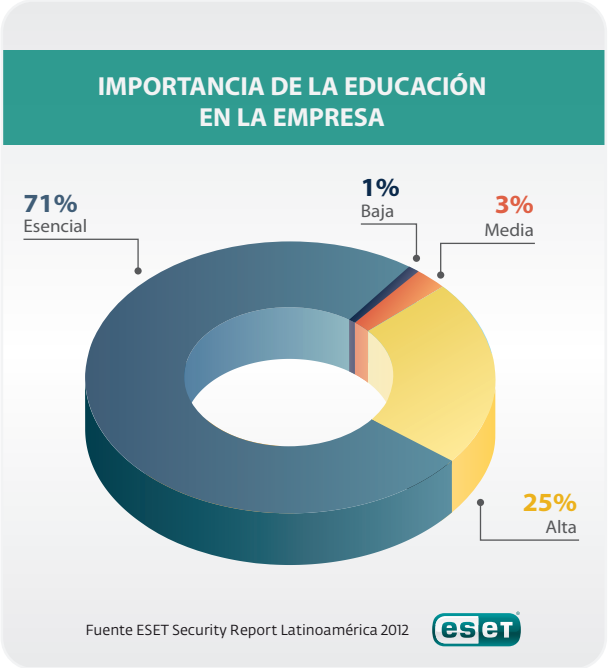
96%

El 96% de las empresas considera que la importancia de la educación es alta o esencial.

vía no adquieren conciencia de que en sus dispositivos móviles corporativos se utilizan correos corporativos, por ejemplo, así como otra información relevante. Por lo tanto, es necesario que estos teléfonos también sean protegidos como lo son sus computadoras debido a la sensibilidad de la información que contienen.

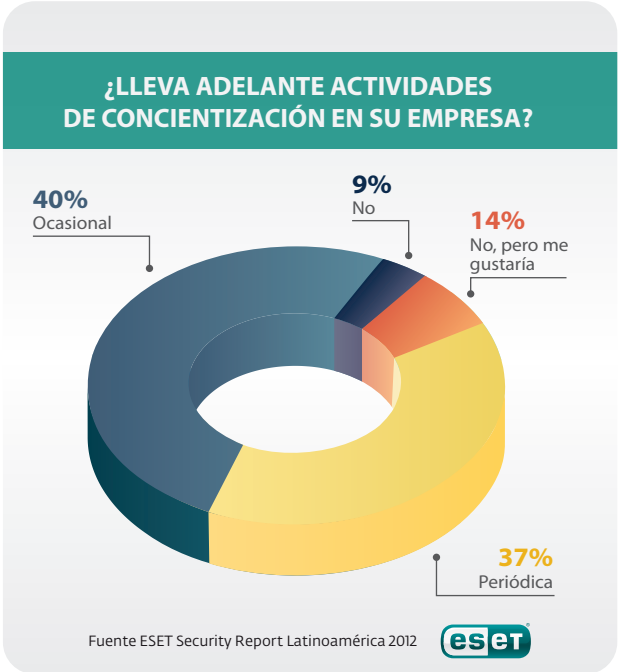
¿Considera realmente importante la educación?

Debido al desenlace de los hechos durante el año, se preguntó a los responsables de las distintas empresas de la región acerca de qué tan importante es la educación respecto a la seguridad de la información en el ambiente corporativo.



>> Gráfico 4. Importancia de la educación en la empresa

Como se puede observar en la figura anterior, **7 de cada 10 empresas** consideran que la educación de sus usuarios es un elemento esencial a tener en cuenta. De hecho, si se observa la cantidad de ejecutivos que calificaron de "esencial" o "alta" a la importancia de la educación en seguridad de la información, se puede observar que juntos representan un **96%** de los encuestados. Esto significa que casi la totalidad de ellos se muestran interesados en la temática. No obstante, a pesar de que los números reflejen un resultado positivo, la realidad es menos optimista, como se puede observar en la figura siguiente, son relativamente pocas las organizaciones que llevan adelante actividades de concientización periódicas en sus respectivas empresas.



>> Gráfico 5. ¿Lleva adelante actividades de concientización en su empresa?

Es decir, a pesar que prácticamente todas las personas consideran la educación como fundamental para su empresa, menos de **4 de cada 10** implementan medidas periódicas para educar a sus empleados. En una época donde la Ingeniería Social se mantiene como una de las herramientas esenciales para la propagación de amenazas, la educación es un arma eficaz para esos casos y debería ser tomada más en cuenta.

Vinculado con este tema, se preguntó a los ejecutivos de las empresas hasta qué nivel jerárquico consideran importante que se capaciten en seguridad de la información dentro de su empresa. Diego Marsili, quien encabeza el área de TI en Rapsodia, una empresa de indumentaria argentina; afirma: "Consideramos importante que se capaciten en todos los niveles. De hecho, lo estamos ejercitando desde las gerencias debido a que hacen uso de servicios electrónicos bancarios". Además de esto, diversos ejecutivos de la región manifiestan que toda la organización debe estar alineada con el proceso de seguridad y enfocan el interés en formalizar sus capacitaciones.

También fue preguntado a las empresas, cuáles consideraban que eran los mayores desafíos en seguridad informática para el próximo año. De acuerdo a los encuestados, existen múltiples

72%

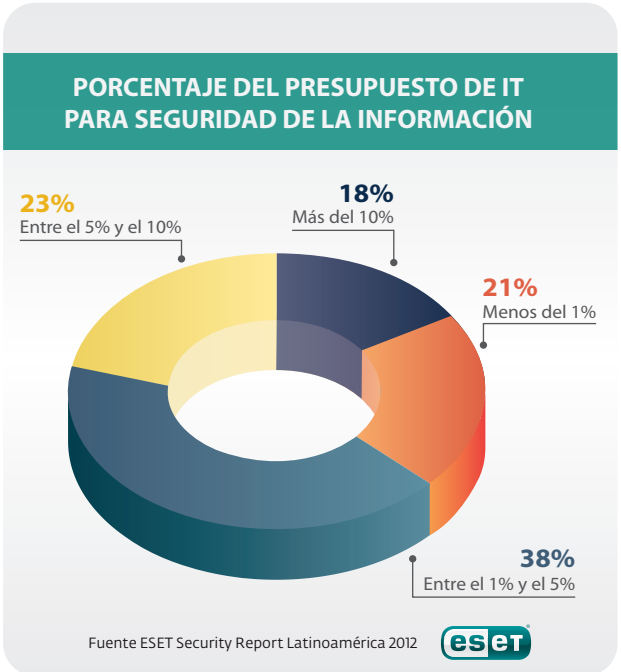
El 72% de las empresas afirma contar con políticas de seguridad.

desafíos a los que un ejecutivo de este área deberá afrontarse de aquí en delante y lo relacionan también con la educación. Por ejemplo, según Ricardo Celis, administrador de red de Derco Perú, es necesario: "Crear a nivel de los usuarios una cultura que se enfoque en los peligros que implica exponer información sensible de la organización, tanto para ellos como para la empresa. Las redes sociales son el primer foco de creación de perfiles sociológicos, la suplantación de identidad puede poner en riesgo datos de acceso a cuentas bancarias y demás información sensible de la empresa. Hay que hacer múltiples campañas de sensibilización con el tema".

Esa cultura a la que hacen referencia las empresas hoy en día, es producto de una transformación actitudinal de sus integrantes. Cuando los cambios en la educación se llevan a cabo de forma sostenida en el tiempo, es posible que se logren cambios culturales que mejorarán sustancialmente el rendimiento de la organización.

Gestión de la seguridad de la información

La seguridad de la información debe ser debidamente gestionada. En pos de conocer un poco más acerca de la realidad de esta gestión en las empresas latinoamericanas, se indagaron ciertos aspectos vinculados con la seguridad.



>> Gráfico 6. Porcentaje del presupuesto de IT para seguridad de la información

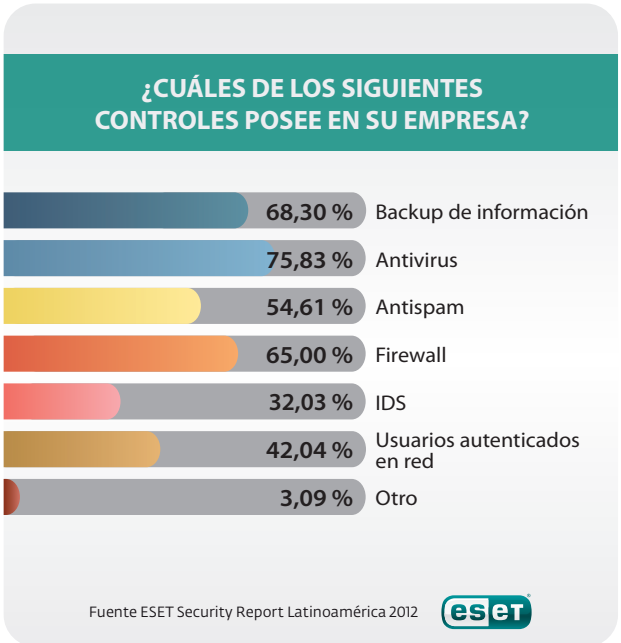
Presupuesto para el área de seguridad

Primero, se busca saber más acerca del compromiso de las empresas de la región de América Latina con la seguridad de sus datos. Para eso, los encuestados debían indicar cuál es el porcentaje del presupuesto de la organización que es designado exclusivamente para el área de seguridad.

Como se puede observar en la gráfica **N° 6**, la mayoría de los ejecutivos asegura que invierten entre el 1% y el 5% de su presupuesto. Por otro lado, es interesante la relación entre los que invierten más del 10% y los que invierten menos que el 1%, ya que ambos porcentajes son similares. Lo que significa que en América Latina casi el 20% de las empresas invierten un porcentaje considerable de su presupuesto en seguridad mientras que otro tanto, invierte menos del 1%. A pesar de que la cifra que refleja este porcentaje varíe de una organización a otra, sirve para detectar aquellos casos donde quizás se subestime a la seguridad para proteger convenientemente la información corporativa.

Controles de seguridad

Como se puede observar anteriormente, a pesar de que para más del **cincuenta por ciento** de las empresas el malware es una preocupación y que más del **45%** ya sufrieron una infección en los últimos 12 meses; sigue existiendo un número alto de empresas que no posee un antivirus.



>> Gráfico 7. ¿Cuáles de los siguientes controles posee en su empresa?

20%

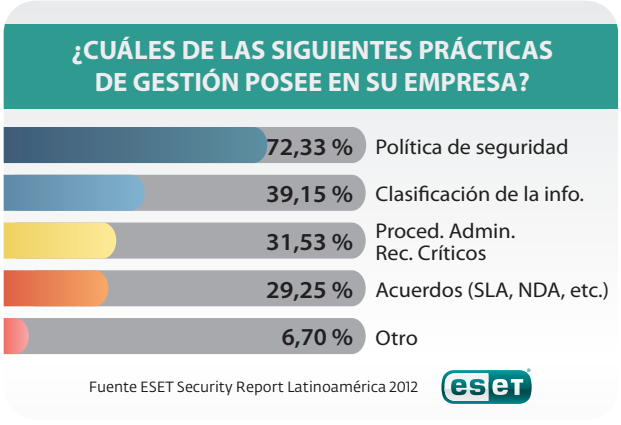
En el 2011 hubo un 20% más de infecciones que el año pasado.

Ese número refleja una realidad abrumadora ya que es difícil concebir el hecho de que **1 de cada 4 empresas no tiene un software antivirus instalado en sus computadoras.** Recuerden que una solución de seguridad es la principal herramienta que las empresas deben utilizar para poder prevenir, por ejemplo, los ataques masivos a los que pueden estar expuestas. Adicionalmente, esta herramienta contempla otros controles que las empresas también necesitan como: antispam, firewall, entre otros.

Sumado a eso, los demás datos que arroja la gráfica **N° 7** tampoco son muy alentadores. Solamente el **42%** de los encuestados afirman que su empresa utiliza usuarios autenticados en una red. Por otro lado, el **68%** de los ejecutivos informan que su empresa utiliza algún tipo de resguardo de información, mientras que para el **32%** restante la pregunta es cómo gestionan sus datos en caso de tener un incidente que provoque pérdida de información.

Prácticas de gestión de la seguridad

Se observa, además, que muchas empresas utilizan políticas de seguridad en la gestión de la seguridad de la información. Más del **70%** de las empresas encuestadas afirma estar siguiendo políticas, mientras que aproximadamente el **40%** invierte recursos en clasificar la información. Este último es un dato importante a tener en cuenta ya que existe un número importante de empresas que no está realizando una discriminación de la información en función de su confidencialidad. Asimismo, a pesar de que un 72,33% de las empresas lleva adelante políticas de seguridad, sin embargo el 31,7% de las empresas no considera el backup de la información en sus políticas de seguridad.



>> Gráfico 8. ¿Cuáles de las siguientes prácticas de gestión posee su empresa?

En algunos casos, esto puede representar una mala práctica de gestión de la seguridad ya que permitiría a un atacante acceder a información sensible y poner en compromiso la organización por una mala administración de los recursos.

Conclusión

Con respecto al año pasado, se observa que muchos valores se han incrementado y se mantiene la tendencia a invertir mayor cantidad de recursos en la concientización de los empleados en seguridad de la información. No obstante, no se puede afirmar que esta mayor atención a la temática se haya reflejado positivamente el estado actual de la seguridad corporativa de América Latina ya que, como se ve en este informe, la tasa de infección de malware en las empresas se ha incrementado en un **20%** entre el 2010 y el 2011 de acuerdo a lo respondido en las encuestas utilizadas para el armado de este informe.

Por otro lado, la preocupación de las empresas por la fuga de información ha aumentado en un **50%** respecto al año pasado. Esto puede estar ligado al impacto provocado por Anonymous con sus ataques de denegación de servicio a diferentes sitios de América Latina y el mundo. A pesar de que la mayoría de estos ataques han sido realizados a sitios gubernamentales, muchos de ellos fueron realizados sobre grandes empresas. Este escenario lleva a que muchas empresas de la región aumenten sus preocupaciones hacia este tipo de amenaza.

Las empresas han incrementado la utilización de los antivirus en sus sistemas. Si bien la mejora no supera el 10% con respecto al año pasado, es un dato no menor a tener en cuenta ya que la protección antivirus es un método muy eficaz a la hora de lidiar con amenazas, sobre todo masivas, que afectan a la organización. Lamentablemente, es una información que aproximadamente **1 de cada 4** empresas en Latinoamérica todavía no valora correctamente, debido a que no poseen una tecnología antivirus en sus equipos. Este dato puede estar fuertemente ligado al aumento en las infecciones que se han registrado de un año para el otro, ya que dichas amenazas no tienen otro mecanismo más eficiente que un antivirus para ser correctamente mitigadas.

También se considera importante que la seguridad de la información deje de ser subestimada en las organizaciones y que haya cada vez más educación a nivel organizacional respecto a esta temática. El desconocimiento de la amenaza puede ser tan dañino como la amenaza en sí misma. Por lo tanto, toda esta información debería ser debidamente procesada por las

empresas de la región para que los números reflejen en mejor medida el incremento de las protecciones y no tanto el de las preocupaciones por parte de los ejecutivos. De este modo, se podrían esperar cifras más positivas para el próximo reporte de seguridad.

Finalmente, reconocer la problemática es un gran paso sin embargo todavía no es suficiente. Que el **96%** de los encuestados considere que la importancia de la educación es alta o esencial para la empresa pero que **solo 4 de cada 10** lleve a cabo actividades de concientización de forma periódica es poco alentador. Las amenazas cambian constantemente y muchas veces se van volviendo más complejas buscando hacerse menos evidente para el usuario. Por lo tanto, se espera que la evolución tecnológica sea acompañada de la educación de los usuarios para que juntas puedan mitigar cada vez más las amenazas del cibercrimen.

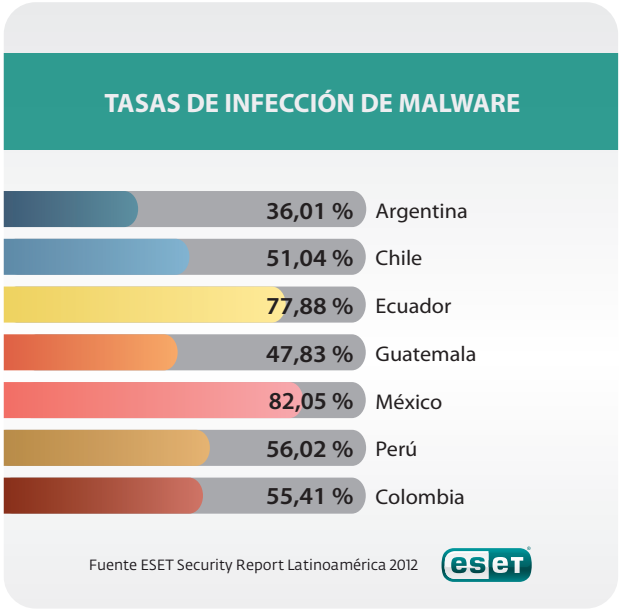
Anexos

El objetivo de este anexo es agregar información correspondiente a algunos países de la región para analizar las diferentes tendencias que reflejan las incidencias de malware entre un país y otro. Adicionalmente, se presenta una gráfica con las tasas de infección discriminadas por los siguientes países: **Argentina, Chile, Ecuador, Guatemala, México, Perú y Colombia.**

En Argentina las tasas de incidentes de *malware* son sensiblemente menores que en América Latina. Como se puede observar en la gráfica **N° 9**, únicamente el **36,01%** de los encuestados afirma haber tenido un incidente con malware en Argentina.

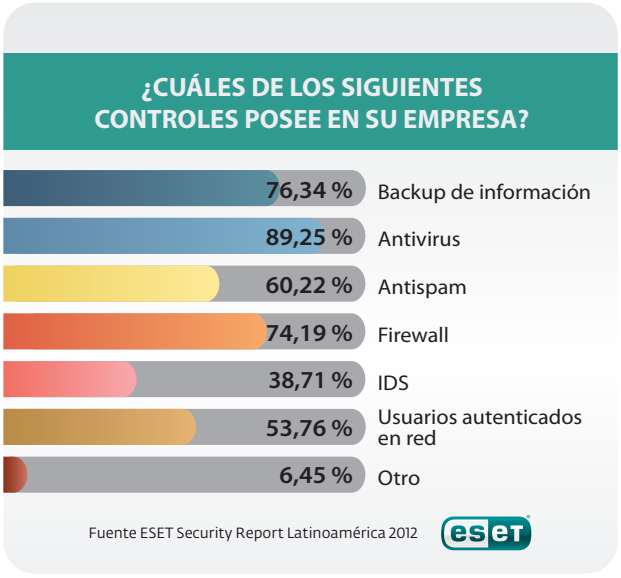
Este hecho puede estar vinculado con un mayor uso de controles en el país que en Latinoamérica como por ejemplo, aproximadamente el **80%** de las empresas afirman estar protegidas con una tecnología antivirus, así como también en el restante de los casos se registran cifras superiores a la región.

En el caso particular del Perú, se observa que existe mayor incidencia de **malware** dado que más de la mitad de las empresas afirma que tuvo algún incidente con esta amenaza y además un número menor de usuarios que la región indica utilizar una tecnología antivirus para contrarrestar estas amenazas. Además, el número de empresas que utiliza algún tipo de tecnología para respaldar su información es notablemente menor que el de América Latina, ya que representan un **48,35%** frente a un **68.30%** de la región.



>> Gráfico 9. Tasas de infección de malware

Colombia es una de las regiones en donde se ven mejores controles corporativos respecto a la seguridad de la información. Aproximadamente un **90%** de las organizaciones cuentan con una tecnología antivirus **¾ partes** de las empresas afirma utilizar tanto una herramienta de backup de la información como algún firewall para proteger la infraestructura de su compañía.



>> Gráfico 10. ¿Cuáles de los siguientes controles posee en su empresa?

No obstante, registran un mayor número de incidencias en explotación de vulnerabilidades que el resto de la región con un **17%** contra un **14%** en Latinoamérica.

Centroamérica, la zona comprendida por Panamá, Costa Rica, Nicaragua, Honduras, El Salvador, República Dominicana y Guatemala; también presenta algunas particularidades. Por ejemplo, es una región en donde las empresas se ven preocupadas con el *malware* y con la fuga de información casi en igual medida. No obstante, mientras las empresas de Guatemala registran un **47.83%** de incidencias de *malware*, países como Nicaragua alcanzan un **80%.**

>> Gráfico 11. ¿Cuáles son sus mayores preocupaciones en la SI?

No obstante, con respecto a los incidentes sufridos en el último año, la región centroamericana lidera en casos donde han surgido inconvenientes de malware con casi un **60%** de las empresas. Un **30%** más de incidencias que en los demás países de América Latina.

Finalmente, México es uno de los países donde sus empresas más se preocupan por el malware en toda América Latina. De hecho, es uno de los pocos en los que la preocupación de los ejecutivos está más orientada a los códigos maliciosos que a la fuga de información. Este comportamiento también tiene un porqué, dado que México también es una de las regiones con mayor tasa de incidencia de malware en América Latina con un **82,05%** de las compañías del país afectadas en el último año.

ESET Latinoamérica

Fundada en 1992, ESET es el fabricante de soluciones de seguridad de mayor crecimiento para usuarios corporativos y hogareños. ESET tiene oficinas en Eslovaquia, Estados Unidos, Polonia, República Checa, Inglaterra, Singapur, Argentina, Brasil y México; y es representada mundialmente por su canal de Partners en más de 180 países.

Av. Libertador 6250 - 6to. Piso - C1428 ARS Buenos Aires , Argentina
tel.: + 54 11 4788 9213 - fax.: +54 11 4788 9629
www.eset-la.com