ESET Security Report 2013 | Argentina

Situación de la seguridad corporativa en América Latina

CONTENIDO

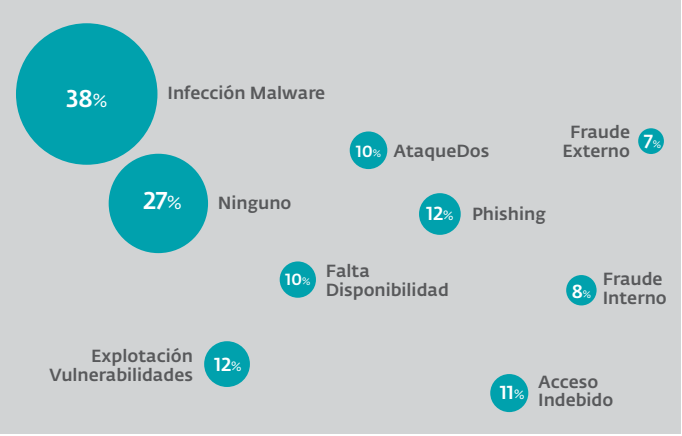
38% Son los usuarios que han sido afectados por los códigos maliciosos

Durante 2012, ESET Latinoamérica participó en diversos eventos de la región relacionados con el área de la Seguridad de la Información. Particularmente, se puede destacar en Argentina el caso de Segurinfo y además el ESET Security Day, el ciclo de eventos gratuitos para empresas organizado por ESET Latinoamérica. Más de 650 personas de diferentes empresas asistieron a los eventos y respondieron una encuesta relacionada con la Seguridad de la Información. Con los datos recopilados se ha podido construir un panorama de la seguridad en las empresas y organizaciones argentinas.

Para este análisis se tuvieron en cuenta los principales incidentes de seguridad que afectaron a las empresas argentinas durante 2012, comparando la situación con el resto de Latinoamérica. Además, este análisis se complementa con una comparación entre la situación de las empresas argentinas con respecto a las demás empresas de la región en lo que respecta al uso de controles y la inversión para gestionar la seguridad de la información, y los esfuerzos en materia de educación para lograr la reducción de incidentes.

Incidentes de seguridad en empresas argentinas

01 *Niveles de incidentes de seguridad en Argentina*

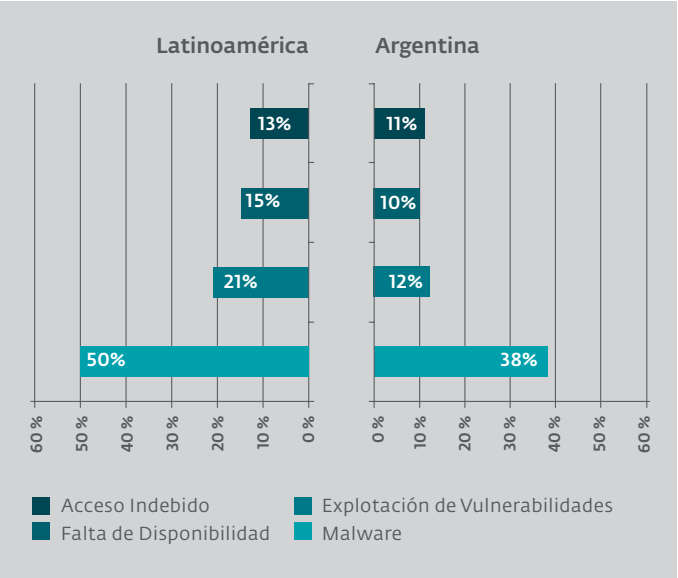


Fuente: *ESET Security Report 2013 | Argentina*

Luego de preguntarle a los ejecutivos cuáles fueron los incidentes de seguridad que más los afectaron durante 2012, los que resultaron en primer lugar fueron los códigos maliciosos, ya que el **38%** de los encuestados declaró haber sufrido este tipo de incidente. Además, otras amenazas como la explotación de vulnerabilidades, la falta de disponibilidad y los ataques de DoS tuvieron un comportamiento similar al de 2011 y se posicionaron cerca del **10%**. El phishing y el acceso indebido a información sensible continúan de cerca con el **12%**, y los casos de fraude con el **8%**. Asimismo, aproximadamente uno de cada cuatro usuarios señaló no haber tenido ningún incidente de seguridad en el último año.

Si bien los porcentajes de incidentes en las empresas de Argentina no superan el **50%**, es interesante comparar estos valores con los del resto de Latinoamérica para tener un punto de referencia más preciso.

02 *Comparación de niveles de incidentes de seguridad*



Fuente: *ESET Security Report 2013 | Argentina*

Cabe destacar que a pesar de que menos empresas encuestadas hayan sufrido algún incidente relacionado con malwa-

82% De las empresas argentinas participantes afirmó contar con una solución antivirus

re, no necesariamente indica que sean menos vulnerables. Es importante tener en cuenta, tal como se resaltó en el informe de tendencias en materia de seguridad de la información para el 2013 de ESET Latinoamérica[1] , que los atacantes buscan nuevas alternativas para propagar malware. A raíz de esto, los equipos de seguridad de las diferentes empresas se enfrentan a nuevos vectores de propagación de códigos maliciosos enfocados en aprovechar servicios vulnerables en Internet para afectar más usuarios.

Implementación de Controles y Gestión

Controles basados en tecnología

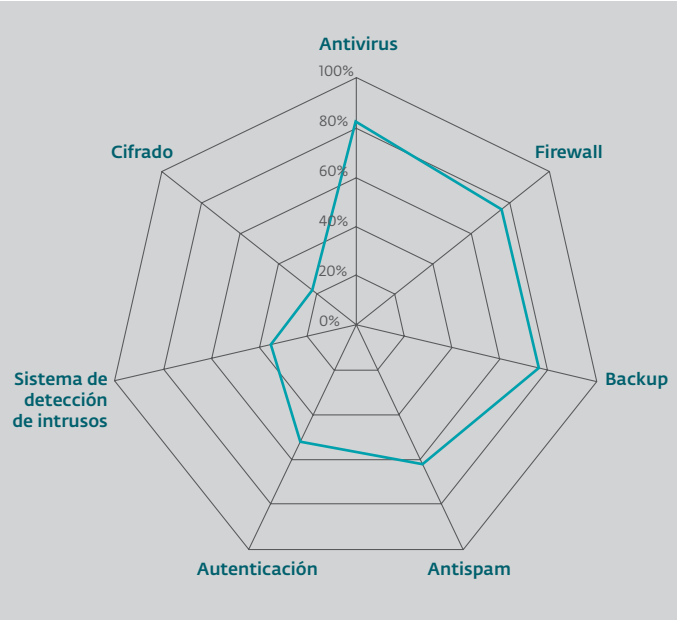
Cuando se trata de la implementación de controles, las empresas deben considerar aquellos que ayuden a disminuir la posibilidad de ocurrencia de un incidente, es decir, los controles preventivos. Además, como muchas veces no es posible evitar el incidente, es necesario contar con controles que reduzcan el impacto al momento de presentarse un incidente. Esta segunda categoría se conoce como "controles correctivos".

Entre los ejecutivos de las empresas argentinas que participaron de nuestras encuestas, el **82%** afirmó contar con una solución antivirus. Otro control tecnológico preventivo, el Firewall, es utilizado por **75%** de las empresas encuestadas siendo el segundo control más utilizado de este tipo. Dentro de esta misma categoría, también resaltan los sistemas de autenticación y los controles Antispam.

Por otra parte, entre los controles correctivos se destacó la realización de backups, ya que el **76%** de los usuarios confirmaron la utilización de una herramienta para realizar respaldos.

El uso de los tres controles (Antivirus, Firewall y Antispam) resultan ser las soluciones básicas para garantizar la seguridad en cualquier empresa. A pesar de esta consideración, y que en el mercado existen soluciones que integran estas tres características como ESET Endpoint Security, apenas el **51%** de las empresas argentinas encuestadas cuenta con los tres controles, contra el **55%** de las empresas del resto de Latinoamérica.

03 *Implementación de controles basados en tecnología*



Fuente: *ESET Security Report 2013 | Argentina*

Por otro lado, la autenticación está implementada en el **52%** de las empresas argentinas, apenas un **2%** por encima de la media latinoamericana.

Vale destacar que este es el principal mecanismo para mantener la confidencialidad de la información y, además es la manera de llevar adelante una investigación en caso de necesitar esclarecer algún acceso indebido a un sistema.

Otros controles, como el cifrado, mantienen la tendencia de poco uso en Argentina. Es importante resaltar que los dispositivos portátiles son cada vez más populares, por lo que los riesgos de pérdida de los mismos con la información almacenada se incrementan y dan lugar a la necesidad de incorporar controles que mitiguen el impacto de estos eventos.

1. En nuestro Centro de Amenazas pueden encontrar el artículo de ***Tendencias 2013: Vertiginoso crecimiento de malware para móviles***

76% Los usuarios confirmaron la utilización de una herramienta para realizar respaldos

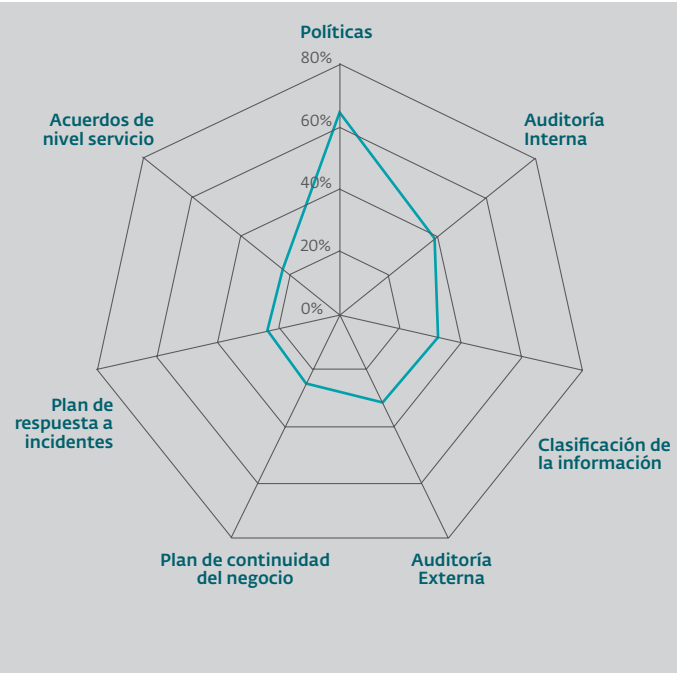
Controles basados en gestión

En cuanto a los controles de gestión, es interesante observar que cerca del **64%** de los encuestados afirmó contar con una política de seguridad definida, sin embargo, las respuestas en los controles restantes están por debajo del **40%.**

Medidas de control como los Planes de Respuesta a Incidentes (PRI) y Planes de Continuidad del Negocio (PCN), están implementadas por una cuarta parte de las empresas encuestadas. Esto indica que el **75%** de las empresas argentinas encuestadas no tiene debidamente escritos y definidos los procedimientos de acción ante un incidente.

Este punto probablemente se traduzca en acciones improvisadas, que pueden derivar en malas decisiones y gastos adicionales de dinero.

04 *Implementación de controles basados en gestión*

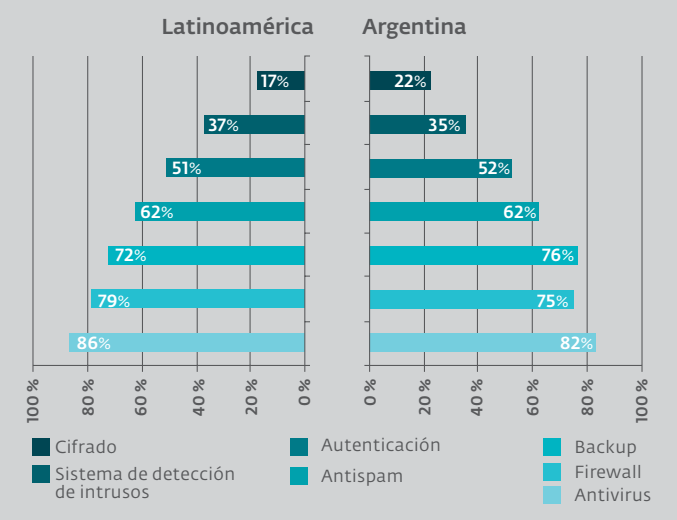


Fuente: *ESET Security Report 2013 | Argentina*

Uso de controles y gestión en empresas argentinas con respecto a la región

En términos generales, la adopción de controles tecnológicos en las empresas encuestadas en Argentina es similar al resto de las empresas encuestadas en la región. Básicamente, se concentran en: Antivirus, Firewall y Antispam; como controles preventivos, y el backup en lo referido a controles correctivos.

05 *Comparación entre los porcentajes de implementación de controles basados en tecnología*



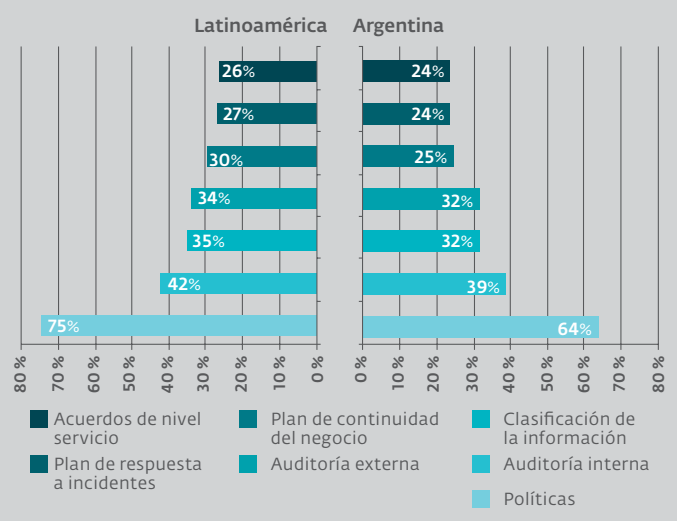
Fuente: *ESET Security Report 2013 | Argentina*

Si bien los niveles de implementación de controles como la autenticación o el cifrado son levemente mayores en las empresas argentinas, resultan ser bastante bajos dadas las nuevas tendencias de movilidad y portabilidad de la información, lo que hace necesario que se tomen medidas adicionales para garantizar la seguridad de la información en los dispositivos móviles. No solo es importante contar con tecnología para tratar de mitigar el impacto o la ocurrencia de incidentes de seguridad, también es necesario definir controles basados en gestión para garantizar la seguridad de la información. Para las empresas argentinas encuestadas, los controles basados en gestión tienen un comportamiento similar al resto de

52% Son las empresas argentinas con un control preventivo como la autenticación

empresas en Latinoamérica, que comprenden la redacción de políticas como el control más relevante y, por tanto, implementado aunque en menor proporción, como se puede observar a continuación:

06 *Comparación entre los porcentajes de implementación de controles basados en gestión*



Fuente: *ESET Security Report 2013 | Argentina*

De acuerdo a la información anterior, vale la pena resaltar que los esfuerzos de las compañías en Argentina parecen estar más enfocados en los controles tecnológicos que en los de gestión, siguiendo la tendencia en toda la región. Es necesario tener en cuenta entonces, que la implementación de controles tecnológicos puede ser más costosa en comparación a los de gestión, la mejor alternativa.

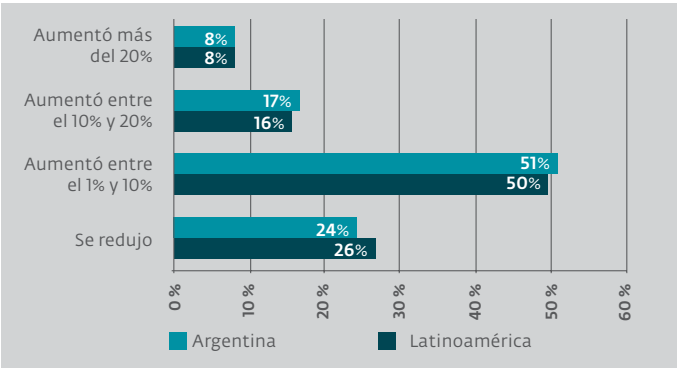
Una de las diferencias entre estos tipos de controles radica en la demanda de tiempo que requieren para su implementación. Aunque al principio, los controles de gestión pueden requerir más tiempo (por ejemplo para la clasificación de información o la creación del Plan de Continuidad del Negocio), en el mediano y/o largo plazo pueden representar una diferencia importante para garantizar la seguridad de la información. Si bien los porcentajes de incidentes son menores en las empresas argentinas, se puede observar que el comportamiento en la implementación de controles es bastante similar al de la región, e incluso en algunos aspectos es peor. Este hecho plantea el interrogante de cuáles son los factores que generan esta diferencia. A continuación, se profundizará la influencia de otros factores como la inversión en seguridad y tener un área exclusiva que se encargue de la seguridad y la educación.

Diferencias en la gestión de la seguridad de la información entre Argentina y Latinoamérica

Inversión en seguridad

La inversión en seguridad es uno de los principales desafíos con los que se debe enfrentar una compañía a la hora de gestionar la seguridad de su información. Asimismo, otro factor que la complejiza, es la medición del retorno de la inversión (ROI o ROSI para seguridad), ya que se percibe a largo plazo. Pero tal como se presenta en el siguiente gráfico, para el caso de Argentina la inversión en materia de seguridad aumentó en comparación con el resto de las empresas encuestadas en la región. De esta manera, hubo menos empresas que redujeron la inversión y fueron más las que la incrementaron.

07 *Variación del presupuesto de 2011 a 2012 en las empresas de Argentina comparadas con las empresas de Latinoamérica*



Fuente: *ESET Security Report 2013 | Argentina*

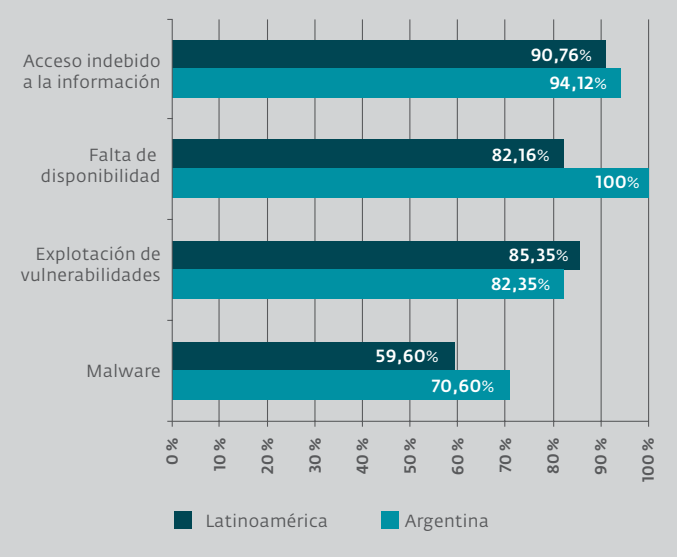
64% Afirmaron contar con una política de seguridad definida

En este sentido, es importante recordar el buen uso de estos recursos a nivel corporativo, ya que en muchas ocasiones el presupuesto asignado para las áreas de seguridad es insuficiente y sin embargo, se compran productos que no son utilizados o debidamente aprovechados.

La importancia de un área dedicada a la Seguridad de la Información

En muchos casos, tener más recursos al realizar una tarea no es necesariamente la forma correcta de lograr mejores resultados. Sin embargo, para las empresas que tienen un área específica dedicada a la gestión de la Seguridad de la Información, la proporción de incidentes es significativamente menor, como se puede observar a continuación:

08 *Porcentaje de empresas que no tuvieron incidentes teniendo un área de seguridad implementada*



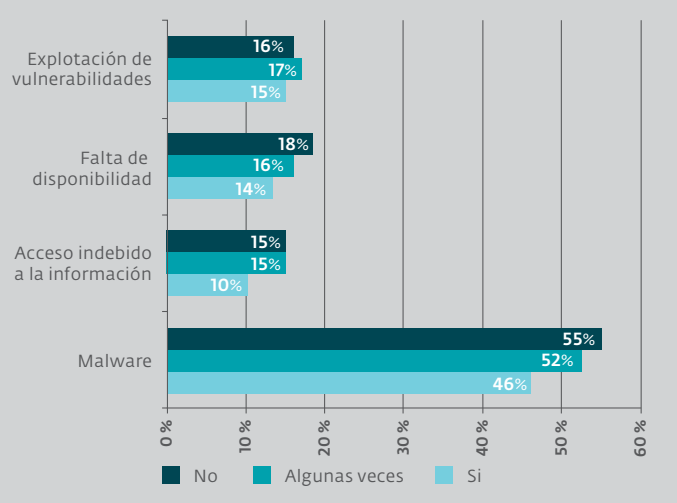
Fuente: *ESET Security Report 2013 | Argentina*

En el caso de las empresas argentinas, se puede ver que el hecho de tener un área de seguridad incrementa los niveles de la seguridad de la información. De esta forma, al contar con un área de seguridad que trabaja independientemente monitoreando los procesos críticos de la compañía, se logra tener un mejor manejo de los incidentes de seguridad que se puedan presentar.

Influencia de las actividades de educación

Cabe resaltar la importancia de las actividades de capacitación para afianzar una cultura de manejo seguro de la información en las compañías. De acuerdo a la información brindada por los ejecutivos encuestados, hay una tendencia a que el porcentaje de incidentes se incremente cuando no se desarrollan actividades de educación en las organizaciones. A continuación, se puede observar un gráfico que compara los porcentajes de incidentes en función de las actividades de concientización brindadas:

09 *La educación y los niveles de ocurrencia de incidentes de seguridad*



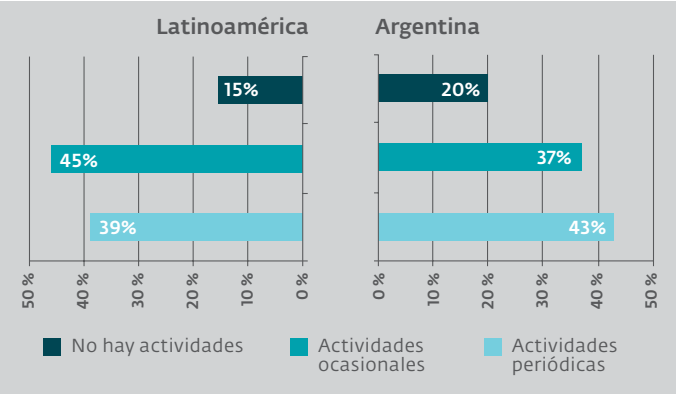
Fuente: *ESET Security Report 2013 | Argentina*

Inclusive, se puede apreciar que la diferencia entre la realización de actividades de capacitación esporádicas y la ausencia de las mismas, es mínima. Esto refleja lo importante que es para las empresas mantener un programa constante de educación, sobre actividades esporádicas. Estas acciones ayudan a que los empleados puedan saber cuáles son las amenazas

más frecuentes a las que pueden enfrentar, además de conocer las mejores prácticas para no verse afectados.

En este sentido, se puede observar entonces cómo las empresas de Argentina tuvieron proporcionalmente mejores niveles en la ejecución de actividades periódicas de concientización.

10 *Porcentaje de empresas que llevan a cabo actividades de educación*



Fuente: *ESET Security Report 2013 | Argentina*

Conclusiones

Para prevenir incidentes con códigos maliciosos y explotación de vulnerabilidades, resulta muy útil la adopción de controles tecnológicos como Antivirus, Firewall, IDS o IPS (Sistema de detección / prevención de intrusos).; aunque de acuerdo a lo presentado, estos últimos son de menor adopción. Asimismo, para prevenir el fraude son apropiados los sistemas de autenticación, que también presentan niveles de uso muy bajos. Además, es recomendable complementarlos con controles de gestión preventivos (como las auditorías) y de carácter correctivo (como los planes de respuesta a incidentes). Cabe destacar que estos controles de gestión tienen muy bajo nivel de aceptación en las empresas de América Latina y las empresas argentinas no son la excepción.

Si bien es importante tener en cuenta que la implementación de controles de seguridad debe ser acorde a la realidad de la empresa, es aconsejable contar con las precauciones necesarias antes de que ocurran los incidentes y no hacerlo de forma reactiva. Si cuando ocurre un incidente se enfocan los esfuerzos únicamente en solucionar el problema a nivel funcional, se descuidarían otros aspectos de la seguridad de la información que podrían comprometer seriamente a la compañía.

Asimismo, es importante destacar que la educación juega un papel importante en la seguridad de la información; y más allá de tener capacitaciones esporádicas, lo que realmente disminuye la ocurrencia de incidentes son los programas continuos de capacitación a los empleados.

Particularmente en las empresas encuestadas de Argentina, sobresale el hecho que indica que los niveles de ocurrencia relacionados con incidentes de tecnología están por debajo del resto de empresas en Latinoamérica. Esto puede ser, en parte, consecuencia de tener una mayor cantidad de empresas con áreas de seguridad dedicadas, mayores aumentos de presupuesto y actividades de educación periódicas. Todo esto refleja una diferencia, pero los porcentajes siguen dando un margen que indica que aún hay bastante por mejorar.

En este sentido, uno de los retos principales para las empresas es que a pesar de que adopten controles para prevenir los incidentes, estos seguirán ocurriendo dado que la información es un activo muy valioso para muchos cibercriminales. Lo cual plantea la necesidad de fortalecer los controles a través del análisis de la situación particular de cada empresa.

Por otra parte, si bien los porcentajes de incidentes son menores en Argentina, seguir reduciendo estos valores dependerá de que las empresas dejen de estar centradas únicamente en el componente tecnológico y se combinen con educación y gestión, formando tres pilares fundamentales. De este modo, se logrará un mejor equilibrio en la Seguridad de la Información y por lo tanto incrementará la protección de las empresas ya que, como se pudo observar, no es solamente la implementación de controles basados en tecnología lo que garantiza una mayor protección.

ESET Latinoamérica

Con 25 años de trayectoria en la industria de la seguridad de la información, ESET es una compañía global de soluciones de software de seguridad, creadora del legendario ESET NOD32 Antivirus y orientada a proveer protección de última generación contra amenazas informáticas. Actualmente cuenta con oficinas centrales en Bratislava (Eslovaquia) y de Coordinación en San Diego (Estados Unidos) Buenos Aires (Argentina) y Singapur. Además, posee otras sedes en Londres (Reino Unido), Praga (República Checa), Cracovia (Polonia), Jena (Alemania) San Pablo (Brasil) y México DF (México).

Desde el 2004, ESET opera para la región de América Latina en Buenos Aires, Argentina, donde dispone de un equipo de profesionales capacitados para responder a las demandas del mercado en forma concisa e inmediata y un Laboratorio de Investigación focalizado en el descubrimiento proactivo de variadas amenazas informáticas.

Juan Díaz de Solïs 1270 - 2do. Piso - C.P 1638 - Buenos Aires, Argentina
Tel.: + 54 11 5171 ESET (3738) - Fax.: +54 11 5171-3739 - www.eset-la.com

ESET Security Report 2013 | Argentina

Situación de la seguridad corporativa en América Latina