# ESET SECURITY REPORT
## LATINOAMÉRICA 2013

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

# CONTENIDO


Situación de la seguridad en pequeñas y grandes empresas 3

Incidentes de Seguridad que afectan a las empresas durante 2012 3

Percepción de la seguridad en las empresas 4

Implementación de Controles y Gestión 4

Uso de controles y gestión 5

Principales amenazas en los países de Latinoamérica 6

- Malware 6
- Explotación de Vulnerabilidades 6
- Falta de disponibilidad 7
- Acceso indebido 7

Más educación menos incidentes de seguridad 7

Invertir en seguridad para reducir los incidentes 8

La importancia de un área dedicada a la Seguridad de la Información 9

- Reducción de incidentes 9
- Más actividades de educación 10

Las actividades de educación disminuyen 10

Evolución de la seguridad en los últimos tres años 10

- Incidentes más recurrentes 10
- Uso de controles basados en tecnología 11
- Uso de controles basados en gestión 11

Conclusiones 12

**50%** Son los usuarios que declaran haber sufrido incidentes por códigos maliciosos

Durante 2012, ESET Latinoamérica participó en diversos eventos en la región relacionados con el área de la Seguridad de la Información. Entre los que se puede destacar, se encuentran: Technology Day, que se realiza en países de Centroamérica como Costa Rica, Guatemala, El Salvador, Nicaragua, Honduras, Panamá y República Dominicana; y Segurinfo, un evento similar al anterior pero realizado en Sudamérica, particularmente en Argentina, Chile, Perú, Colombia y Uruguay. En estos eventos se realizan encuestas a ejecutivos de empresas relacionados con la seguridad y tecnología de la información. Vale la pena destacar que, se contó con la participación de más de 3500 ejecutivos de toda América Latina, quienes aportaron información clave, parte de la cual fue necesaria para construir este reporte. La información recopilada fue utilizada para poder realizar un análisis exhaustivo y presentar un panorama representativo de la Seguridad de la Información en la región

El siguiente informe comienza con un análisis sobre la forma en la cual los ejecutivos clasificaron sus preocupaciones en materia de seguridad de la información durante el 2012, teniendo en cuenta el tamaño de cada empresa. Seguidamente, se analizan los principales incidentes de seguridad que afectaron a las empresas durante los últimos doce meses, considerando las preocupaciones y el uso de los controles, con el fin de determinar la percepción de seguridad, las principales medidas de protección utilizadas y la forma en la que fueron empleadas. Luego, se expone cómo los principales incidentes de seguridad afectan a los países de Latinoamérica.

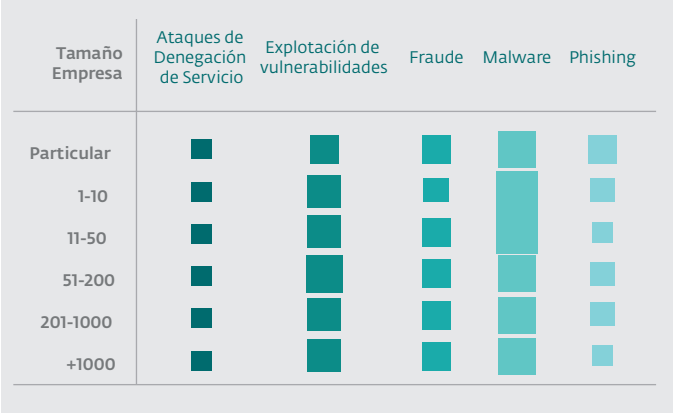
Este informe se complementa con el análisis de la incidencia de la educación y la inversión en Seguridad de la Información respecto a la ocurrencia de incidentes en las empresas. Finalmente, se hace un recuento del comportamiento de los principales incidentes de seguridad y el uso de los controles tecnológicos y de gestión durante los últimos tres años.

## Situación de la seguridad en pequeñas y grandes empresas

En el siguiente gráfico, el área de la figura representa la magnitud del porcentaje de usuarios que respondieron sobre cuál era su mayor preocupación en términos de seguridad de la información. La explotación de vulnerabilidades y los ataques de phishing cuentan con las mayores variaciones, es decir que mientras para particulares y empresas pequeñas es más preocupante el phishing, las empresas grandes se preocupan más por la explotación de vulnerabilidades.

El malware, si bien tiene los mayores porcentajes para las empresas pequeñas, representa también la mayor preocupación para las empresas más grandes.

*| Gráfico Nº 1 |*
*Fuente ESET Security Report | Latinoamérica 2013*




Si bien hay algunas diferencias entre cómo las empresas conciben los incidentes de seguridad, es importante destacar la coincidencia en la preocupación frente al malware. Cabe recordar, que una infección con algún tipo de código malicioso puede tener consecuencias que van desde la interrupción de las operaciones del negocio hasta el robo de información. Otro incidente en el que coinciden las empresas grandes y pequeñas, es en el caso de la explotación de vulnerabilidades. Esto se puede explicar en gran medida por el hecho de que los ciberdelincuentes no distinguen entre empresas grandes, medianas o chicas al momento de vulnerar un servidor, simplemente aprovechan aquellos que tengan alguna debilidad para explotar.

Es importante destacar, además, que independientemente del tamaño de la empresa, se hace necesaria la gestión de la seguridad de la información, por lo que se cae el mito que sostenía que una empresa pequeña no tiene mayores preocupaciones en materia de seguridad, frente a los que pueden tenerlas más grandes. Nuevamente, los incidentes de seguridad no distinguen el tamaño de la empresa.

## Incidentes de Seguridad que afectaron a las empresas durante 2012

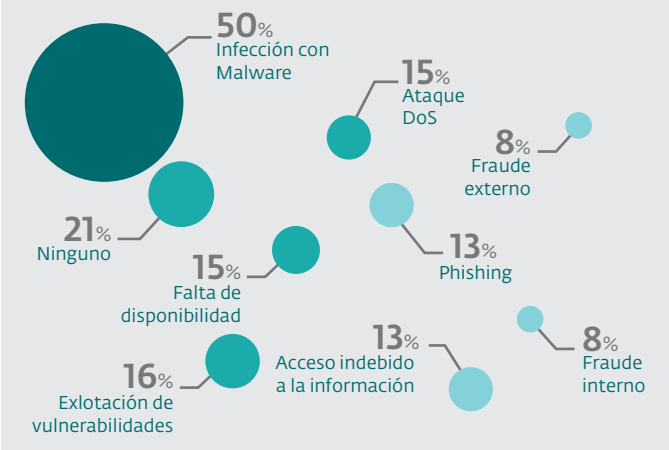
Luego de preguntarle a los ejecutivos cuáles fueron los incidentes de seguridad que más los afectaron durante 2012, los incidentes que resultaron en el primer lugar fueron los códigos maliciosos, ya que la mitad de los encuestados declararon haber sufrido este tipo de incidente.

Otras amenazas, como la explotación de vulnerabilidades, la falta de disponibilidad y los ataques de DoS tuvieron un comportamiento bastante similar durante el último año, donde cerca del 15% de los usuarios dijo haber sufrido alguno de estos.

**27%** Son las empresas donde su mayor preocupación es la infección con códigos maliciosos

El phishing y el acceso indebido a información sensible continúan de cerca con el 13%, y los casos de fraude con el 8%. Además, uno de cada cinco usuarios señaló no haber tenido ningún incidente de seguridad en el último año.

*| Gráfico Nº 2 |*
*Fuente ESET Security Report | Latinoamérica 2013*




El hecho de que la mitad de las empresas encuestadas sufrieran algún incidente relacionado con malware se puede explicar a partir del hecho que los atacantes están buscando continuamente nuevas alternativas para propagar malware. Tal como indica el informe de tendencias para el 2013 de ESET Latinoamérica en materia de seguridad de la información, los vectores de propagación de códigos maliciosos se están enfocando cada vez más en aprovechar servicios vulnerables en Internet para afectar mayores cantidades de usuarios. Por lo tanto, no sorprende que los principales incidentes ocurridos durante 2012 giren alrededor del malware y la explotación de vulnerabilidades.

## Percepción de la seguridad en las empresas

A continuación, se expondrá cómo las preocupaciones de los ejecutivos de las empresas que respondieron a nuestras encuestas se relacionan con los incidentes que se presentaron en el último año.

Se le pidió a los participantes que organizaran cinco amenazas (las infecciones con códigos maliciosos, la explotación de vulnerabilidades, los casos de fraude, el phishing y los ataques de denegación de servicios) de mayor a menor grado de preocupación de acuerdo a la situación de cada empresa.

Resultó que para el 27% de empresas de la región la infección con códigos maliciosos fue la mayor preocupación, y al menos la mitad de estas empresas sufrieron una infección con malware.

En el caso de la explotación de vulnerabilidades, para el 21% de los ejecutivos fue la mayor preocupación, lo cual se aproxima al 16% de las empresas que manifestaron haber experimentado este tipo de incidentes.

Por otro lado, los casos de fraude representan la segunda preocupación para el 29% de las empresas, que si se compara con el hecho de que al menos el 8% de las empresas sufrieron algún tipo de fraude (interno o externo), resulta ser mucho mayor y por lo tanto se sobredimensiona el incidente.

A partir de esta información se puede ver que la percepción en materia de amenazas en las empresas no se encuentra totalmente alineada con el tipo de incidentes que realmente se presentan. Si se toma como referencia el caso del malware, se puede observar que ha afectado al menos a la mitad de las empresas encuestadas, sin embargo, no es claramente la mayor preocupación al momento de la gestión. En una situación similar pero opuesta se encuentran los casos de fraude, que si bien aparecen como una de las principales preocupaciones, no son los incidentes que ocurren con mayor frecuencia.

Cabe preguntarse, entonces, si los esfuerzos que se están haciendo en materia de seguridad informática están enfocados en lo que realmente sucede o si están de acuerdo a una percepción no tan representativa de la realidad.Esto no implica que existan amenazas menos importantes, sino que las preocupaciones deberían estar acorde a lo que las empresas enfrentan diariamente.

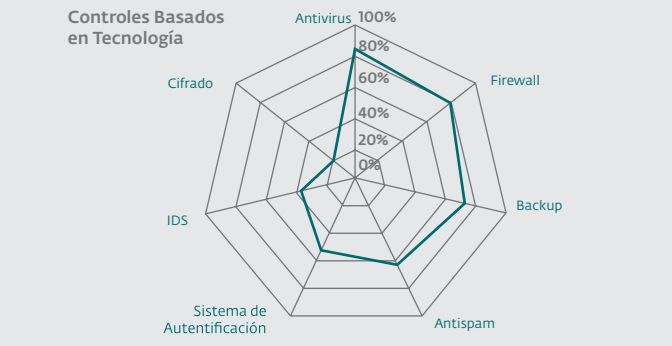
## Implementación de Controles y Gestión

Entre los ejecutivos de las empresas que participaron de los eventos de ESET Latinoamérica, el 86% afirmó contar con una solución antivirus en las compañías donde trabajan. Otro control tecnológico preventivo como el Firewall alcanzó el 80% dentro de las medidas más utilizadas.

Dentro de esta misma categoría resaltan los sistemas de autenticación y los controles Antispam. Por otra parte, entre las soluciones de carácter correctivo se destacó la realización de backups, ya que el 78% de usuarios confirmaron la utilización de una herramienta para realizar respaldos.
Queda en evidencia, entonces, que la combinación de Antivirus, Firewall y Antispam son los controles elementales más populares con los cuales cuentan la mayoría de las empresas en Latinoamérica. A pesar de esta consideración, y de que en el mercado existen soluciones que integran estas tres características, apenas el 55% de las empresas encuestadas cuentan con los tres controles.

**78%** De usuarios confirmaron la utilización de una herramienta para realizar respaldos.

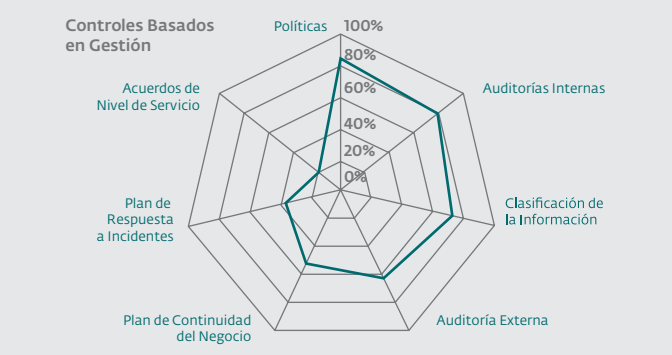
*| Gráfico Nº 3 |*
*Fuente ESET Security Report | Latinoamérica 2013*




Por otro lado, sorprende que un control preventivo básico como la autenticación, esté implementado en apenas el 50% de las empresas. Teniendo en cuenta que este es el principal mecanismos 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.En este sentido, también es destacable el hecho de que el cifrado de la información tenga tan poca relevancia dentro de los controles utilizados. Si bien es un control correctivo, puede ser la única forma que tengan las empresas para evitar que información sensible caiga en manos equivocadas. Además, teniendo en cuenta que los dispositivos portátiles son cada vez más populares, los riesgos se incrementan y la necesidad de incorporar controles resulta fundamental.

En cuanto a los controles de gestión, es interesante observar que casi el 80% de los encuestados afirmaron contar con una política de seguridad definida, sin embargo, las respuestas en los controles restantes no alcanzan siquiera el 50%. Puede tomarse como ejemplo, el caso de los Planes de Respuesta a Incidentes (PRI) y los Planes de Continuidad del Negocio (PCN), ya que son medidas que aplican solo el 26% de las empresas encuestadas. Nuevamente, queda en evidencia que casi tres de cada cuatro empresas en Latinoamérica no tienen claramente definido un plan de acción en caso de que se presente un incidente.

*| Gráfico Nº 4 |*
*Fuente ESET Security Report | Latinoamérica 2013*




De acuerdo a la información anterior, vale la pena resaltar que los esfuerzos de las compañías en la región parecen estar más enfocados en los controles tecnológicos que en los de gestión. Es necesario tener en cuenta, entonces, que la implementación de controles tecnológicos pueden ser más costosos que de gestión.

Una de las diferencias entre los controles tecnológicos y los de gestión 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 el levantamiento del Plan de Continuidad del Negocio) en el mediano o largo plazo pueden representar una diferencia importante para garantizar la seguridad de la información.

## Uso de controles y gestión

Para garantizar niveles óptimos en la protección de la información en una compañía, es claro que no se puede tener implementado solamente un control; la combinación de varios es el factor que va a dar mejores resultados. De la información recolectada, se puede observar que el 70% de las empresas que tiene implementado algún tipo de respaldo, no tienen un Plan de Respuesta a Incidentes documentado y el 64,36% no cuenta con un Plan de Continuidad del Negocio.

Resulta de vital importancia marcar esto, porque si bien tienen su información respaldada no existen procedimientos y guías de cómo recuperarla en el tiempo y la forma necesaria para garantizar la operación del negocio, lo cual se logra a través de la implementación y prueba de un Plan de Continuidad de Negocio.

El control de gestión que tiene mayores niveles de implementación es la política de seguridad. Sin embargo, tres de cada cinco usuarios que tienen redactadas y publicadas las políticas de seguridad de la información, no han realizado una clasificación de su información, lo cual podría indicar que las políticas están redactadas con poca profundidad sin tener en cuenta todos los activos de información con los que cuenta la compañía.

Lo que es más crítico aún, es que uno de cada cinco usuarios no cuenta con una política de seguridad establecida ni clasifica su información, a pesar de contar con controles de tipo tecnológico como antivirus, firewall, backup, etc.

La pérdida o robo de la información a través del fraude, es una de las mayores preocupaciones para las empresas, ya que al menos una de cada cuatro empresas la eligieron por detrás del malware. A pesar de esto, apenas el 20% de ellas cuentan con políticas de seguridad definidas y una solución de autenticación, las alternativas de control

**86%** el 86% afirmó contar con una solución antivirus en las compañías donde trabajan

más viables para prevenir incidentes de fraude.

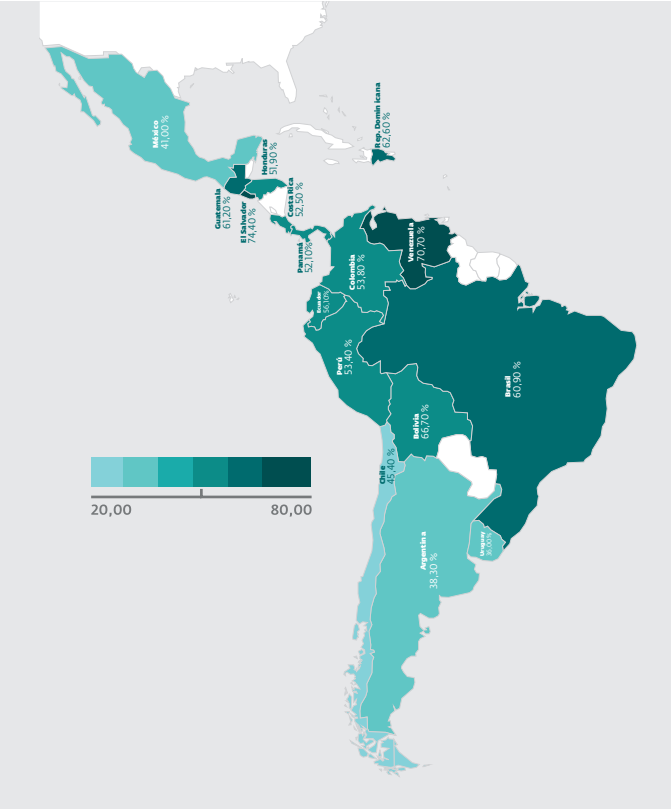
Es llamativo el hecho de que un 6% de las empresas en Latinoamérica no tiene una solución de seguridad para proteger sus equipos ni cuentan con políticas de seguridad. A pesar de que el número no parece tan relevante, es grave que algunas empresas no consideren las amenazas que existen en Internet y no se protejan ni con las herramientas básicas.

Por otro lado, el 80% de las empresas de América Latina que sí poseen una solución de seguridad no tienen ninguna política de seguridad definida. Es importante recordar que en el ámbito corporativo la gestión es tan importante como el uso de las tecnologías

## Principales amenazas en los países de Latinoamérica

### ■ Malware

*| Gráfico Nº 5|*
*Fuente ESET Security Report | Latinoamérica 2013*

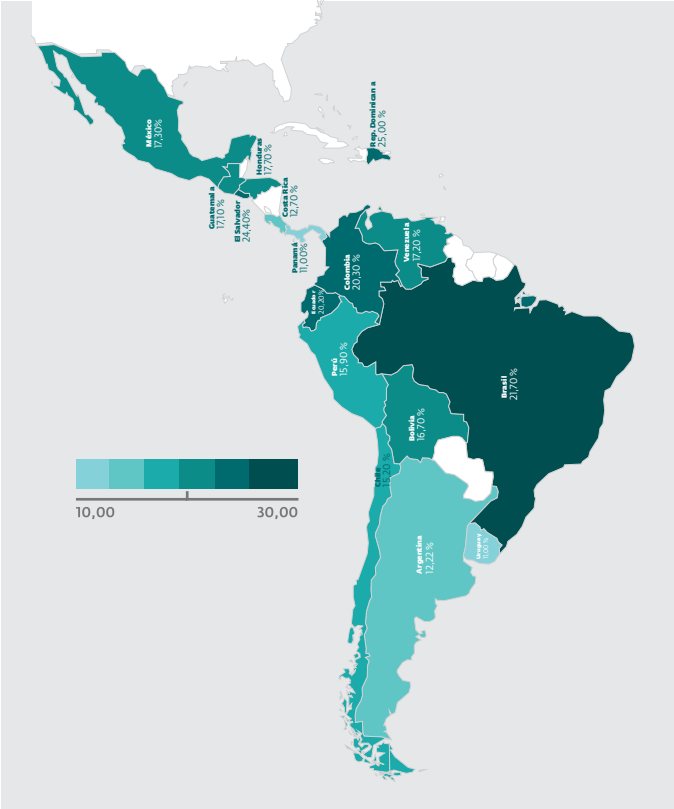



A raíz del hecho que el malware fue la amenaza que más afectó a las organizaciones en Latinoamérica durante el 2012, en el siguiente mapa se exponen los porcentajes de las empresas de cada país que tuvieron incidentes de este tipo.

Cabe destacar que, los países de Centro América, Colombia, Brasil, Ecuador, Perú, Venezuela y Bolivia estuvieron por encima del promedio de la región, es decir que más del 50% de las empresas encuestadas en estos países sufrieron un incidente relacionado con malware en los últimos doce meses. Solamente México, Chile, Uruguay y Argentina estuvieron por debajo del 50%.

### ■ Explotación de Vulnerabilidades

*| Gráfico Nº 6|*
*Fuente ESET Security Report | Latinoamérica 2013*




En cuanto a la explotación de vulnerabilidades, el segundo incidente de mayor ocurrencia durante el último año, se puede observar como en El Salvador y República Dominicana cerca de una cuarta parte de las empresas que participaron de la encuesta afirmaron haber sufrido al menos un incidente de estas características.

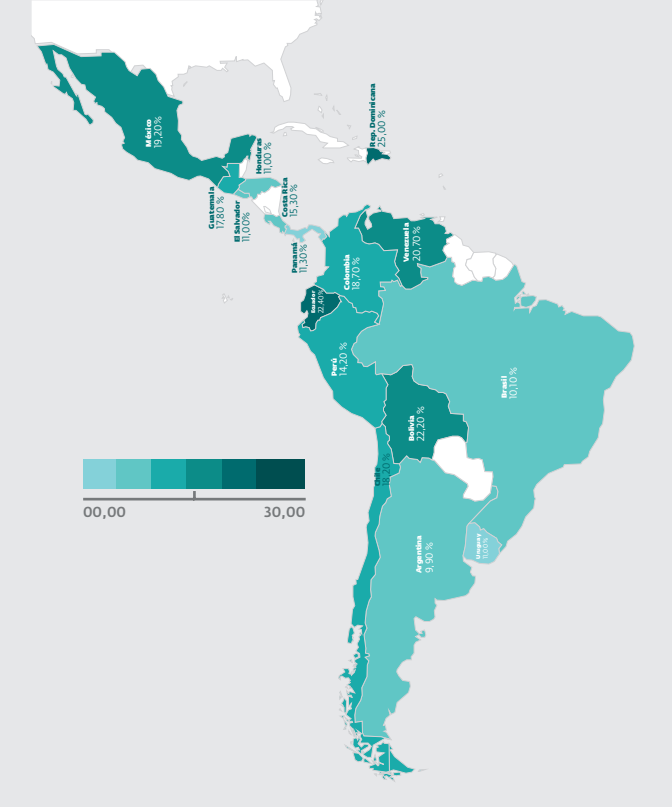
Otros países como Colombia, Ecuador y Brasil tienen porcentajes

**50%** Son las que empresas estan implementando un control preventivo básico

cercanos al 20% de empresas que también estuvieron afectadas. Estos valores, si bien no son la mayoría dentro las empresas encuestadas en cada país, están alejados del porcentaje de empresas en toda la región, y más en comparación con los demás países cuyos porcentajes son similares o están por debajo.

## ■ Falta de disponibilidad

*| Gráfico Nº 7|*
*Fuente ESET Security Report | Latinoamérica 2013*



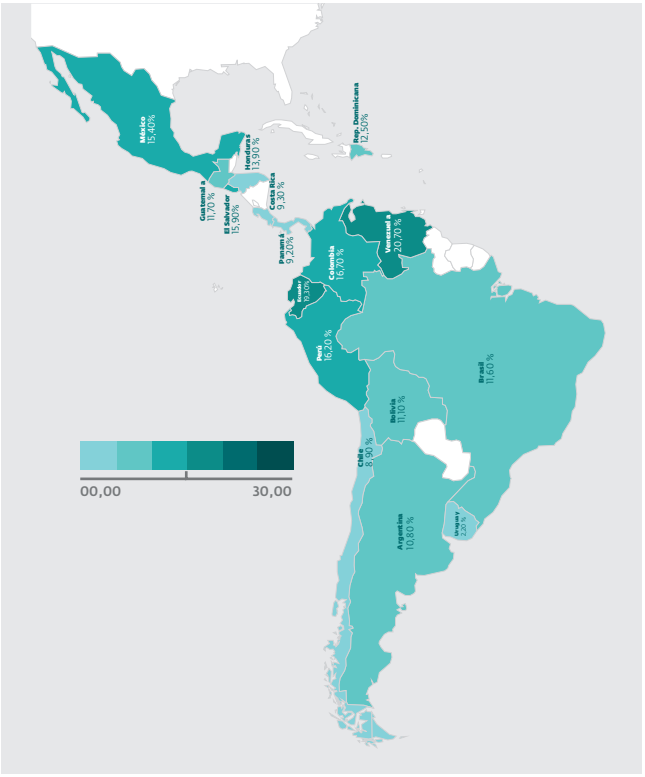

Los incidentes de falta de disponibilidad fueron más comunes en empresas de países como Bolivia (22.4%), Ecuador (22.2%), Venezuela (20.7%) y República Dominicana (25%).

Mientras que otros, como México (19.2%), Colombia (18.7%) y Guatemala (17,8%) estuvieron igualmente por encima del porcentaje de empresas afectadas por estos incidentes en la región (15%).

## ■ Acceso indebido

En el caso de los incidentes asociados al acceso indebido de la información, fueron seis los países que estuvieron por encima del

*| Gráfico Nº8|*
*Fuente ESET Security Report | Latinoamérica 2013*




porcentaje de empresas afectadas en toda la región (13%), siendo Ecuador (19.3%) y Venezuela (20,7%) los que presentaron mayores proporciones de afección. Los restantes países: Colombia (16,7%), Perú (16,2%), El Salvador (15,9%) y México (15,4%) están un poco menos alejados de este promedio.

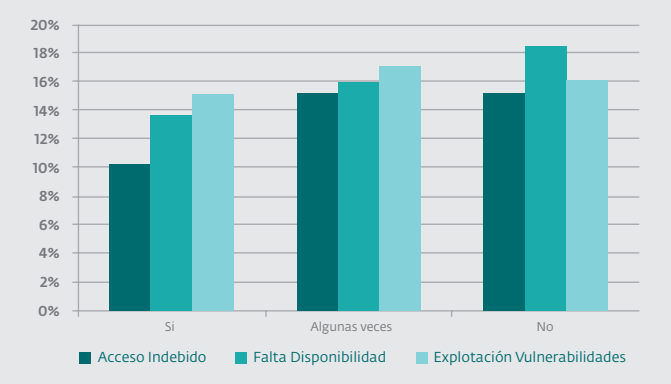
## Más educación, menos incidentes de seguridad

Cabe resaltar la importancia de las actividades de capacitación en las empresas para afianzar una cultura de manejo seguro de la información en la compañía. De acuerdo a la información brindada por los ejecutivos encuestados, hay una tendencia a que el porcentaje de incidentes incremente, cuando no se llevan a cabo actividades de educación en las organizaciones.

A continuación, se puede observar un gráfico que compara los porcentajes de ocurrencia de diferentes incidentes que se materializan en una empresa en función de las actividades de concientización brindadas a sus empleados:

**20%** De las empresas cuentan con políticas de seguridad definidas

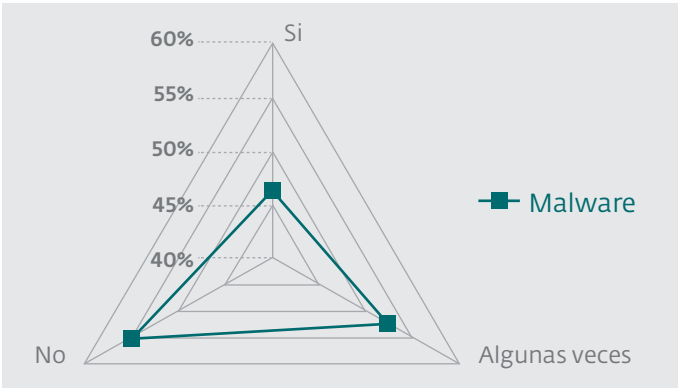
*| Gráfico Nº9|*
*Fuente ESET Security Report | Latinoamérica 2013*




Inclusive, se puede apreciar que la diferencia entre la realización de actividades de capacitación esporádicas y la ausencia de las mismas, es mínima.

Asimismo, si se realiza el mismo tipo de análisis pero solamente para los incidentes relacionados con códigos maliciosos, se puede observar un comportamiento similar al obtenido para el resto de las amenazas.

*| Gráfico Nº10|*
*Fuente ESET Security Report | Latinoamérica 2013*

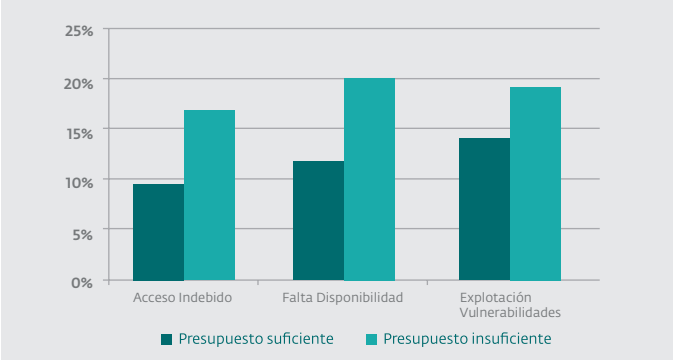



Puntualmente, para los incidentes relacionados con malware, se puede ver que en el caso de las organizaciones que tienen un plan de capacitación establecido, la cantidad de incidentes es 10% menor. Además, se mantiene la tendencia vinculada con las actividades de educación eventuales o la ausencia de las mismas.

## Invertir en seguridad para reducir los incidentes

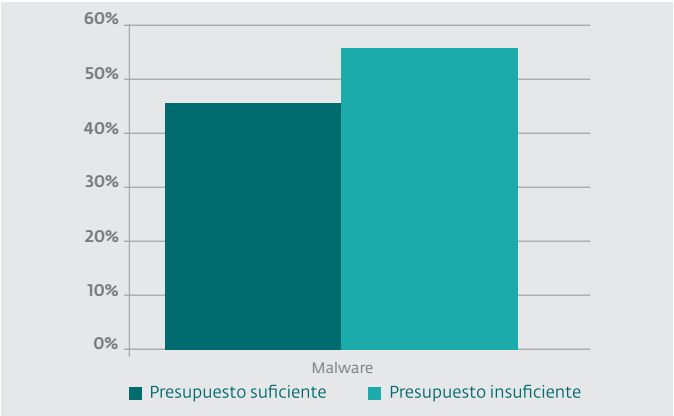
La inversión es uno de los principales desafíos con los que se debe enfrentar una compañía, a la hora de establecer la gestión de la seguridad de su información. Asimismo, otro factor que la complejiza es la medición del retorno de la inversión, ya que se percibe a largo plazo. Pero tal como se presenta en el siguiente gráfico, cuando el presupuesto invertido en Seguridad de la Información es considerado como "suficiente", se logra observar que el porcentaje de incidentes es sensiblemente menor.

*| Gráfico Nº11|*
*Fuente ESET Security Report | Latinoamérica 2013*




En el caso del malware, se da la misma tendencia: si el presupuesto es "suficiente" para el área de seguridad, la cantidad de incidentes es menor. En este sentido, es importante recordar el buen uso de estos recursos a nivel corporativo, ya que muchas veces el presupuesto asignado para las áreas de seguridad es insuficiente y, sin embargo, se compran productos que no son utilizados o debidamente aprovechados.

*| Gráfico Nº12|*
*Fuente ESET Security Report | Latinoamérica 2013*

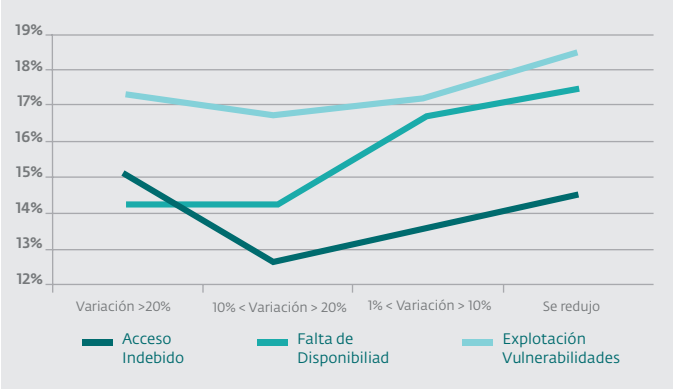



De manera similar, se puede observar como la cantidad de incidentes se redujo en las empresas que aumentaron el presupuesto destinado al área de seguridad en el último año.

**80%** Son las empresas de América Latina que sí poseen una solución de seguridad

*| Gráfico Nº13|*

*Fuente ESET Security Report | Latinoamérica 2013*




En el caso de los tres incidentes de seguridad representados en el gráfico anterior, los aumentos de al menos el 10% en el presupuesto tienen relación directa con la ocurrencia de menos incidentes durante el último año.

En cuanto a los incidentes de malware, se da un comportamiento similar en aquellas empresas donde aumentó el presupuesto para el área de seguridad de la información, tal como se nota en el siguiente gráfico. En el caso de las compañías que aumentaron menos del 10%, la cantidad de incidentes fue menor que para aquellas que redujeron el presupuesto.

*| Gráfico Nº14|*

*Fuente ESET Security Report | Latinoamérica 2013*

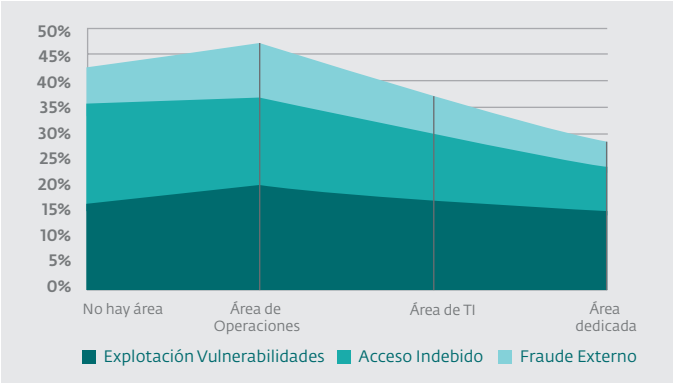

## La importancia de un área dedicada a la Seguridad de la Información

### ■ Reducción de incidentes

En muchos casos, tener más recursos al realizar una tarea no es necesariamente la forma correcta de lograr mejores resultados. Sin embargo, a raíz del siguiente gráfico, se puede observar que para las empresas que tienen un área específica dedicada a la gestión de la seguridad de la información, la cantidad de incidentes es significativamente menor.

*| Gráfico Nº15|*

*Fuente ESET Security Report | Latinoamérica 2013*

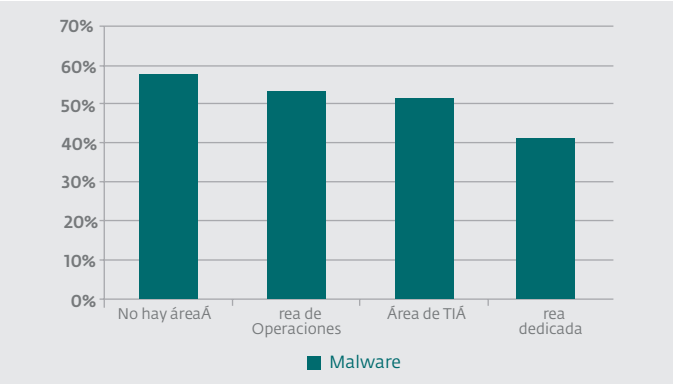



La gestión de la seguridad de la información, dado que es una cuestión transversal a todas las actividades de una empresa, debería tener un área encargada e independiente. Con esto se logra, por una parte, no mezclarse con el negocio y, por la otra, servir eficientemente al cumplimiento de los objetivos corporativos. Además, el hecho de que se traten como áreas diferentes evita los conflictos de intereses que se pueden generar. Incluso hay diferencias entre tener un área exclusiva y tener delegada la seguridad de la información en áreas que presten servicios críticos el negocio.

Tal como en los casos anteriores, el comportamiento en cuanto a la reducción de incidentes relacionados con infecciones con códigos maliciosos tiene un comportamiento similar al resto de incidentes. En este caso, tener un área dedicada a la gestión de la seguridad de la información resulta un factor clave, y es responsable directo de porcentajes menores de incidentes.

*| Gráfico Nº16|*

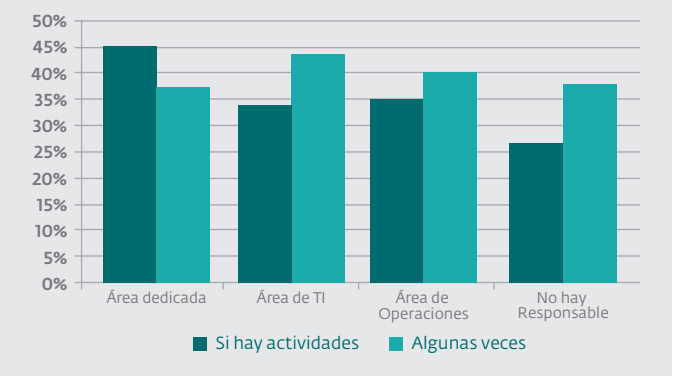
*Fuente ESET Security Report | Latinoamérica 2013*



**10%** Es 10% menor la cantidad de incidentes en las organizaciones que tienen un plan de capacitación

Como se mencionó anteriormente, realizar actividades de educación en temas de seguridad de la información disminuyó los niveles de incidentes. Además, se observa una interesante relación entre las actividades de concientización y el hecho de contar con un área de seguridad de la información: las empresas en América Latina que tienen un área formalmente definida por lo general son las que más esfuerzos dedican a llevar adelante planes de concientización para sus empleados.

*| Gráfico Nº17|*
*Fuente ESET Security Report | Latinoamérica 2013*



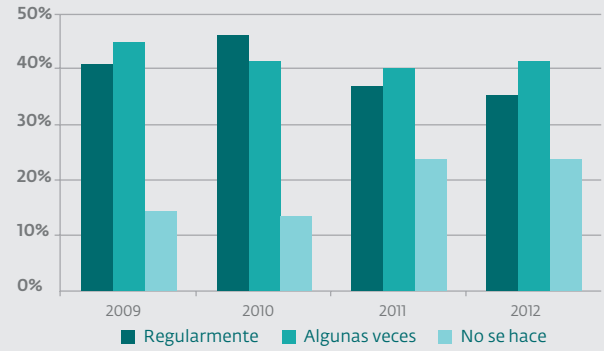

## Las actividades de educación disminuyen

Pero a pesar de que la información recopilada muestra que a medida que se incrementan las actividades de educación, disminuyen los incidentes; al hacer un análisis comparativo de los últimos cuatro años, se observa que el porcentaje de empresas que realizan regularmente actividades de concientización ha disminuido casi un 10% en los últimos años, mientras que se han mantenido las actividades ocasionales.

Por otro lado, se nota un aumento de las empresas que directamente no realizan actividades de capacitación. En relación al año pasado, el 25% de empresas que no realizan este tipo de actividades se mantiene, pero ha aumentado con relación a 2010 en un 10%.

Esto significa que, anualmente, mientras el número de empresas que realizan capacitaciones regularmente va disminuyendo, crecen las empresas que no hacen este tipo de actividades o las hacen de forma esporádica.

*| Gráfico Nº18|*
*Fuente ESET Security Report | Latinoamérica 2013*




La situación anterior se ve respaldada en el gráfico, ya que la intención de realizar actividades de concientización disminuyó en un 30%. Durante el 2011 el 14.2% de los encuestados, a pesar de no realizar actividades de concientización, lo consideraba como una posibilidad. Sin embargo, solo el 9.8% de los encuestados en 2012 considera realizar actividades de este tipo.

## Evolución de la seguridad en los últimos tres años

A partir de la información que se ha podido recolectar durante los eventos en los que año a año participa ESET Latinoamérica, se presenta a continuación cómo ha sido la evolución de los incidentes y la adopción de los controles para su mitigación.

### ■ Incidentes más recurrentes

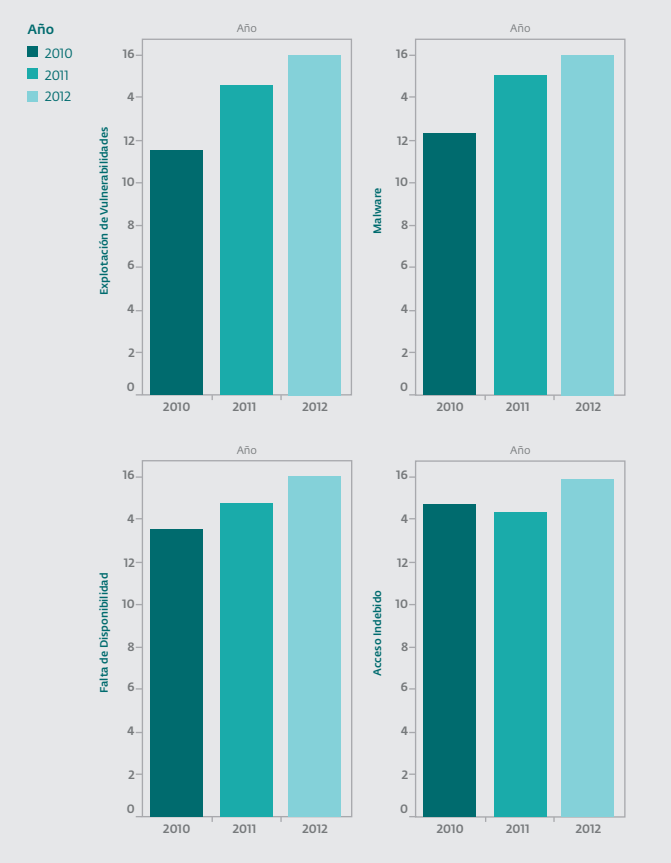
Los niveles de incidentes que afectan la seguridad de las empresas en los últimos tres años han aumentado. Solamente en el caso del Acceso Indebido a la Información se había notado un decrecimiento leve durante el 2011. Pero para 2012, el porcentaje de víctimas de este tipo de incidentes se incrementó nuevamente.

Este comportamiento pone en evidencia que el enfoque de la seguridad no debe estar ligado únicamente a la gestión de un tipo de incidente.

Se puede ver que la materialización de los diferentes incidentes de seguridad es creciente, lo cual refleja el hecho de que cada vez es más común ver ataques donde se mezclan diferentes tipos de acciones maliciosas.

**10%** Las empresas que realizan regularmente actividades de concientización ha disminuido

*| Gráfico Nº19|*
*Fuente ESET Security Report | Latinoamérica 2013*

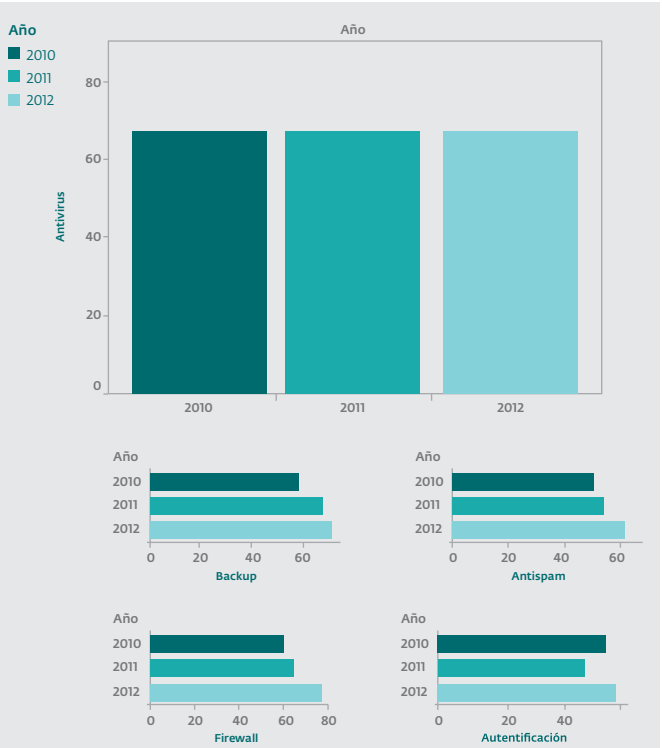



## ■ Uso de controles basados en tecnología

Los controles basados en tecnología han tenido un crecimiento semejante en los últimos tres años, a excepción de las soluciones de backup y de autenticación que tuvieron comportamientos diferentes.Para el caso del backup, de 2010 a 2011 los controles aumentaron en casi el 10%, frente el 3% que crecieron de 2011 a 2012.
Las soluciones de autenticación, en cambio, tuvieron en el período 2010 a 2011 una disminución de casi 6% en su implementación. Durante el 2012 el crecimiento de estas soluciones fue de casi el 8%.

En resumen, se puede observar que cada vez más empresas utilizan una solución de seguridad en su empresa, no obstante todavía hay más de un 10% que no tiene ninguna herramienta para prevenir sus sistemas de cualquier código malicioso en Internet y casi 30 de cada 100 no realizan respaldo de su información. Esto representa un riesgo para esas empresas en caso que su información se pierda o sufra algún tipo de daño.

*| Gráfico Nº20|*
*Fuente ESET Security Report | Latinoamérica 2013*




## ■ Uso de controles basados en gestión

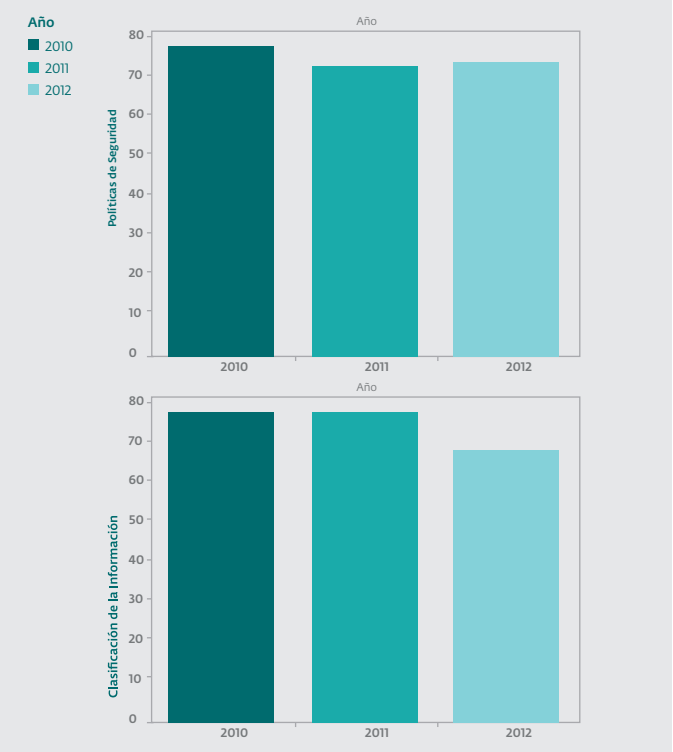
La evolución en la adopción de los controles asociados en la gestión es muy diferente a la de aquellos que se basan en la tecnología.Solamente analizando la implementación de Políticas de Seguridad y la Clasificación de la información, se puede ver que los mayores esfuerzos se centran en los controles de tipo tecnológico.

La implementación de políticas de seguridad, que si bien está bastante extendida ya que cerca del 80% de las empresas la tienen, en los últimos tres años ha tenido un estancamiento, dado que más del 20% de las empresas no tienen claramente definido cómo gestionar la seguridad de la información.

Anteriormente, se ha mencionado que medidas como la clasificación de la información ayudan a que una empresa enfoque sus esfuerzos en aquellos activos de infomación que sean realmente críticos para el negocio. Por lo tanto, resulta interesante observar que menos del 40% de empresas en la región tengan presente llevar adelante este tipo de actividades e, incluso, que este porcentaje se vea disminuido en el transcurso de los últimos años.
Esto puede dar indicios de que quizás los esfuerzos para garantizar la seguridad de la información se están destinando a las acciones equivocadas.

**9,8%** solo el 9.8% de los encuestados en 2012 considera realizar actividades de concientización

*| Gráfico Nº21|*
*Fuente ESET Security Report | Latinoamérica 2013*




## Conclusiones

Al momento de preguntarle a las empresas sobre cuáles son sus mayores preocupaciones en materia de seguridad de la información, siguen apareciendo en primer lugar los ataques con códigos maliciosos seguidos de la explotación de vulnerabilidades y los fraudes.
En el caso de la explotación de vulnerabilidades, es importante resaltar la variedad de aplicaciones a las que se les han descubierto fallas en el último año, y que pueden poner en riesgo la integridad de la información corporativa. Dentro de estas aplicaciones, se destacan Java y Flash Player, con el componente adicional que la infección es totalmente independiente del sistema operativo.

Para prevenir incidentes con códigos maliciosos y explotación de vulnerabilidades, resulta muy útil la adopción de controles tecnológicos como antivirus, firewall o IDS, aunque de acuerdo a lo presentado este último es el de menor adopción. Por otro lado, para prevenir los incidentes de fraude resultan útiles los sistemas de autenticación, que presentan niveles de uso muy bajos. Además, se recomienda complementarlos con controles de gestión preventivos, como las auditorías, y de carácter correctivo, como los planes de respuesta a incidentes. Cabe destacar en este sentido, que estos controles de gestión tienen muy bajo nivel de aceptación en las empresas de América Latina.
La ocurrencia de incidentes es el principal catalizador para la adopción de soluciones de seguridad, lo cual da muestras de un comportamiento reactivo más que preventivo. Tal es el caso de los incidentes de acceso indebido a la Información y los controles de autenticación. Para el periodo entre 2010 y 2011 los niveles de estos incidentes se redujeron, pero entre 2011 y 2012 tuvieron un crecimiento mayor a lo que había disminuido. Conscientes de lo complejo que pueden ser este tipo de incidentes y las consecuencias que pueden traer para una empresa, aumentó la adopción de controles de autenticación en el periodo de 2011 y 2012, en detrimento de la disminución que se había dado de 2010 a 2011.

Si bien es importante tener en cuenta que la implementación de controles de seguridad debe ir de acuerdo a la realidad de la empresa, es mejor contar con las precauciones necesarias antes de que ocurran los incidentes y no hacerlo de forma reactiva. Prestar atención a las amenazas más frecuentes en el momento del incidente, puede dejar un agujero importante en la seguridad que podría comprometer seriamente a la compañía.

Además, se pudo notar que la educación juega un papel fundamental en la seguridad de la información. Y más allá de tener capacitaciones no periódicas, lo que realmente disminuye la ocurrencia de incidentes son los programas continuos de capacitación a los empleados. A pesar de que se ve que la educación reduce estos niveles fehacientemente, en los últimos tres años estas actividades se han reducido en las empresas de América Latina, lo cual marca una debilidad importante del punto de vista corporativo a nivel mundial.
Resulta interesante destacar que los incidentes de malware han incrementado anualmente, pero el crecimiento entre los años 2011 y 2012 (3%) fue menos de la mitad del período entre los años inmediatamente anteriores (8.5%). Esto, a su vez, va acompañado del crecimiento en la adopción de controles de seguridad como antivirus, Antispam y Firewall. Lo importante en este punto, es que el menor incremento en los incidentes de malware se nota de la misma forma para los restantes tipos de incidentes.

Finalmente, es importante resaltar que si bien las empresas adoptan controles para prevenir la ocurrencia de incidentes, estos siguen ocurriendo e incluso presentan una tendencia creciente. Lejos de que esto signifique que los controles no sirven, demuestra que el reto para las empresas está más relacionado con analizar si los mismos se están aplicando eficazmente.

En la medida que los esfuerzos de las empresas dejen de estar centrados únicamente en el componente tecnológico y se combinen con la educación y la gestión, formando tres pilares fundamentales, se logrará un mejor equilibrio en la seguridad de la información y, por lo tanto, incrementará la protección de las empresas en América Latina.

## 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.

Juan Díaz de Solis 1270 - 2do. Piso - B1638DBB, Vicente López,
Buenos Aires , Argentina
tel.: +54 11 5171-3738 (ESET) - fax.: +54 11 5171-3739