ESET Security Report
Latinoamérica 2015

Argentina • Chile • Colombia • Costa Rica • Ecuador
El Salvador • Guatemala • Honduras • México
Nicaragua • Panamá • Paraguay • Perú • Venezuela

ENJOY SAFER TECHNOLOGY™

CONTENIDO

01 / Introducción

Como parte de las actividades desarrolladas por el Laboratorio de Investigación de ESET Latinoamérica, durante 2014 participamos en diversos eventos relacionados con la industria de la Seguridad Informática a lo largo de toda la región. Para ESET es muy importante conocer el estado de la Seguridad de la Información de empresas y gobiernos, de modo que aprovechamos estos eventos y encuentros para realizar encuestas a los participantes que, cabe destacar, pertenecen a múltiples industrias, negocios y rubros por lo que el universo de las encuestas es muy extenso y variado. En 2014 contamos con la participación de más de 3980 ejecutivos de toda América Latina, quienes aportaron la información necesaria para construir este reporte.

Con los datos recopilados podemos dar un panorama sobre cuál es la forma en que los ejecutivos abordan los problemas relacionados con la seguridad en sus empresas. Además, nos permite hacer un análisis sobre el comportamiento de las amenazas y la manera en que se abordan las medidas de control para enfrentarlas.

Como dijimos anteriormente, el desarrollo de este informe está enfocado en responder cuatro preguntas que nos van a permitir tener un panorama acerca de cuál es el estado de la Seguridad Informática en las empresas de la región. Primero nos ocuparemos de conocer alrededor de qué amenazas giran las preocupaciones de las empresas, llegando incluso a compararlas de acuerdo al tamaño de la empresa para encontrar semejanzas y diferencias.

En 2014 contamos con la participación de **3980** ejecutivos

Conocer las preocupaciones de las empresas nos servirá de punto de partida para compararlas con lo que ocurre en la realidad, es decir, las preocupaciones contra los incidentes reales. Esto nos permitirá saber si los esfuerzos para asegurar la información de una compañía están bien enfocados o no, ya que en ocasiones se invierte dinero teniendo en cuentas las preocupaciones y no los incidentes que suceden realmente.

Si bien se le presta atención a los incidentes ocurridos, es igualmente importante conocer qué hacen las empresas para protegerse. En este sentido, veremos qué tipo de controles tecnológicos y de gestión adoptan, las actividades de concientización que realizan y la variación de presupuesto en materia de seguridad que hay en las diferentes empresas encuestadas.

Finalmente, haremos un análisis retrospectivo de los últimos cinco años sobre algunos de los incidentes que han tenido mayores cambios en cuanto a la cantidad de empresas afectadas. Además, observaremos cómo la materialización de estas amenazas pareciera no estar asociada con la adopción de nuevos paradigmas de control que permitirían reducir los incidentes.

02 / ¿Cuáles son las preocupaciones de las empresas en Latinoamérica?

Una de las cuestiones que resulta interesante conocer para determinar en qué se enfocan las empresas cuando se trata de la Seguridad de la Información, son aquellas preocupaciones por las cuales invierten recursos para evitar problemas.

Además de conocer solamente las preocupaciones, es interesante analizar cómo cambian de acuerdo al tamaño de la empresa. Tal como se puede observar en el ***Gráfico 1,*** resulta que la mayor preocupación para cerca del 70% de las empresas encuestadas en Latinoamérica son las **vulnerabilidades de *software* y sus sistemas.** Esta preocupación se mantiene en el primer lugar independiente del tamaño de la empresa, seguida por la infección con códigos maliciosos. En este caso, cabe resaltar que la infección con *malware* tiene más impacto como preocupación entre las pequeñas y medianas empresas en comparación con las grandes.

El top 3 de las amenazas lo completan los incidentes asociados con fraude interno o externo. Un aspecto a destacar es que los incidentes de *phishing* sean una preocupación para alrededor del 40% de las empresas, independientemente de su tamaño. Si bien es una de las amenazas más simples desde el punto de vista técnico, en nuestro informe **"Tendencias 2015: El mundo corporativo en la mira"** [1] resaltamos que es uno de los medios para propagar las **APTs (*Advanced Persistent Threat* o Amenazas Avanzadas y Persistentes).** Los cibercriminales saben que el usuario promedio es bastante propenso a abrir adjuntos de correos desconocidos, lo que es utilizado no sólo en APTs sino en otros incidentes como el malware que secuestra información y luego pide rescate, conocido como Ransomware. El ejemplo más reciente de esto último fueron las campañas mundiales de CTB-Locker, detectado por ESET como *Win32/FileCoder.DA*.

Preocupaciones relacionadas con la seguridad de la información en las empresas encuestadas en Latam, clasificadas por tamaño de empresa

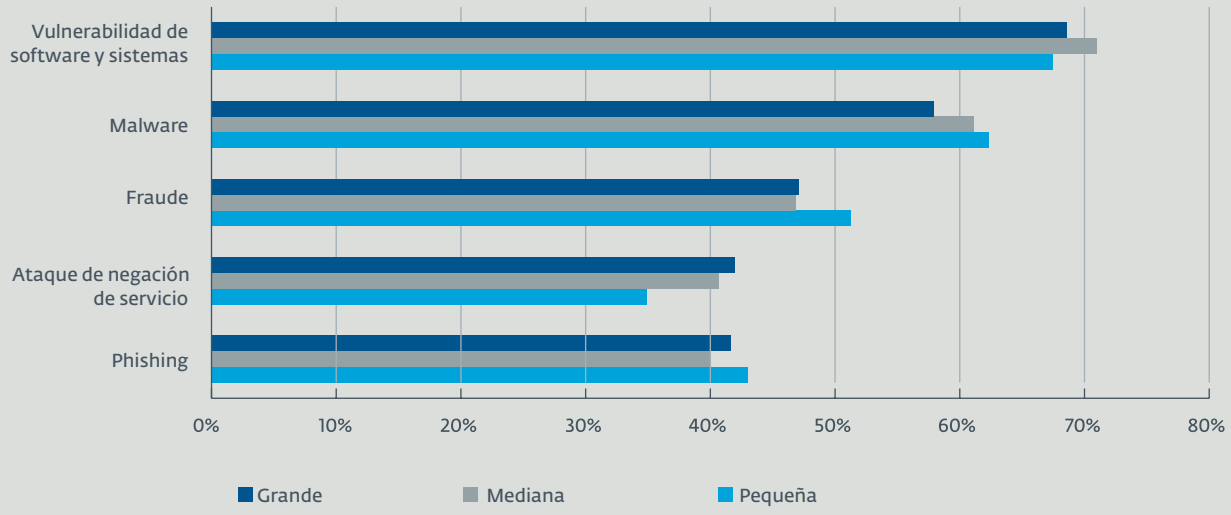


GRÁFICO 1 / Preocupaciones de la Seguridad de la Información de las empresas de acuerdo de su tamaño

1 **Laboratorio de Investigación ESET Latinoamérica. WeLiveSecurity en Español.** http://www.welivesecurity.com/wp-content/uploads/2015/01/tendencias_2015_eset_mundo_corporativo.pd

Por otra parte, hay un aspecto adicional muy interesante que se desprende del análisis de las preocupaciones, pero que se evidencia agrupando por tipo de industria al que pertenece cada empresa. Es así que para las empresas del sector financiero, más allá de los códigos maliciosos o las vulnerabilidades, sus preocupaciones se enfocan en las posibilidades de ser víctimas de un fraude.

En el caso del rubro de la salud y de gobierno, la mayor preocupación se vincula con las vulnerabilidades o agujeros de seguridad. Es así como en el 60% de las empresas de estos sectores considera que el mayor peligro proviene de la infección con códigos maliciosos; esto se relaciona con los casos que vemos desde hace varios años en los cuales sitios gubernamentales son víctimas de ataques de ciberdelincuentes[2].

Luego de analizar estas cuestiones, concluimos que las preocupaciones en materia de seguridad se mantienen alineadas a lo largo de todas las empresas y más allá de su tamaño el comportamiento es muy semejante, por lo cual los esfuerzos de las áreas de seguridad deberían enfocarse en tratar los riesgos como acontecimientos que realmente pueden ocurrir. En las próximas secciones del ESET Security Report, develaremos cuáles de estas preocupaciones se materializaron en incidentes a lo largo del año pasado.

60%

De las empresas considera que el mayor peligro proviene de la infección con códigos maliciosos

2 **WeLiveSecurity. Cuenta oficial de Twitter del presidente de Venezuela comprometida.** http://www.welivesecurity.com/la-es/2013/04/15/cuenta-oficial-twitter-presidente-venezuela-comprometida/

Phishing alojado en página del gobierno peruano. http://www.welivesecurity.com/la-es/2010/11/18/phishing-alojado-en-pagina-del-gobierno-peruano/

WeLiveSecurity. Gobierno de Brasil sufre ciberataque a pocos días del Mundial. http://www.welivesecurity.com/la-es/2014/05/30/gobierno-brasil-sufre-ciberataque-pocos-dias-mundial/

México, Brasil y Perú con más sitios educativos y de gobierno infectados. http://www.welivesecurity.com/la-es/2013/07/19/mexico-brasil-y-peru-con-mas-sitios-educativos-y-de-gobierno-infectados/

Operación Medre: ¿espionaje industrial en Latinoamérica?. http://www.welivesecurity.com/la-es/2012/06/21/operacion-medre-espionaje-industrial-latinoamerica/

Sitio web del gobierno Ecuatoriano comprometido con ataque. http://www.welivesecurity.com/la-es/2010/06/08/sitio-gobierno-ecuatoriano-comprometido-ataque/

03 / ¿Qué incidentes sufrieron las empresas durante 2014?

Ahora que conocemos cuáles son las preocupaciones de las empresas, lo siguiente es saber cuáles fueron realmente los incidentes; esto nos dará una idea de si los esfuerzos para contrarrestarlos están bien orientados.

Tal como vemos en el ***Gráfico 2*** la distribución de los incidentes es muy similar independiente del tamaño de la organización, sobre todo para los incidentes más recurrentes como los **accesos indebidos**, la **infección con malware** y los **ataques de denegación de servicio** (DoS).

Esta tendencia demuestra que a un ciberdelincuente no le interesa el tamaño de la empresa siempre y cuando pueda obtener algún tipo de ganancia económica; es crucial que los responsables de la seguridad de las compañías conozcan esto y no pase inadvertido en ninguna reunión de planificación e implementación de planes de seguridad.

Un caso interesante y que vale la pena resaltar está relacionado con los incidentes asociados al *phishing*. Lo veíamos en el ***Gráfico 1*** como el tipo de amenaza que menos preocupa a las empresas, y particularmente a las de mayor tamaño como el incidente que menos reportan como parte de sus principales preocupaciones. Sin embargo, en el ***Gráfico 2*** vemos como casi el 20% de empresas grandes sufrieron algún incidente de *phishing* que, vale la pena recordar, afectan directamente a la información que manejan los empleados y que puede exponer de forma crítica datos sensibles.

Ya que tenemos un panorama de cómo se dieron los incidentes de seguridad en las empresas a nivel general en Latinoamérica; ahora es importante ver la tendencia de incidentes país por país.

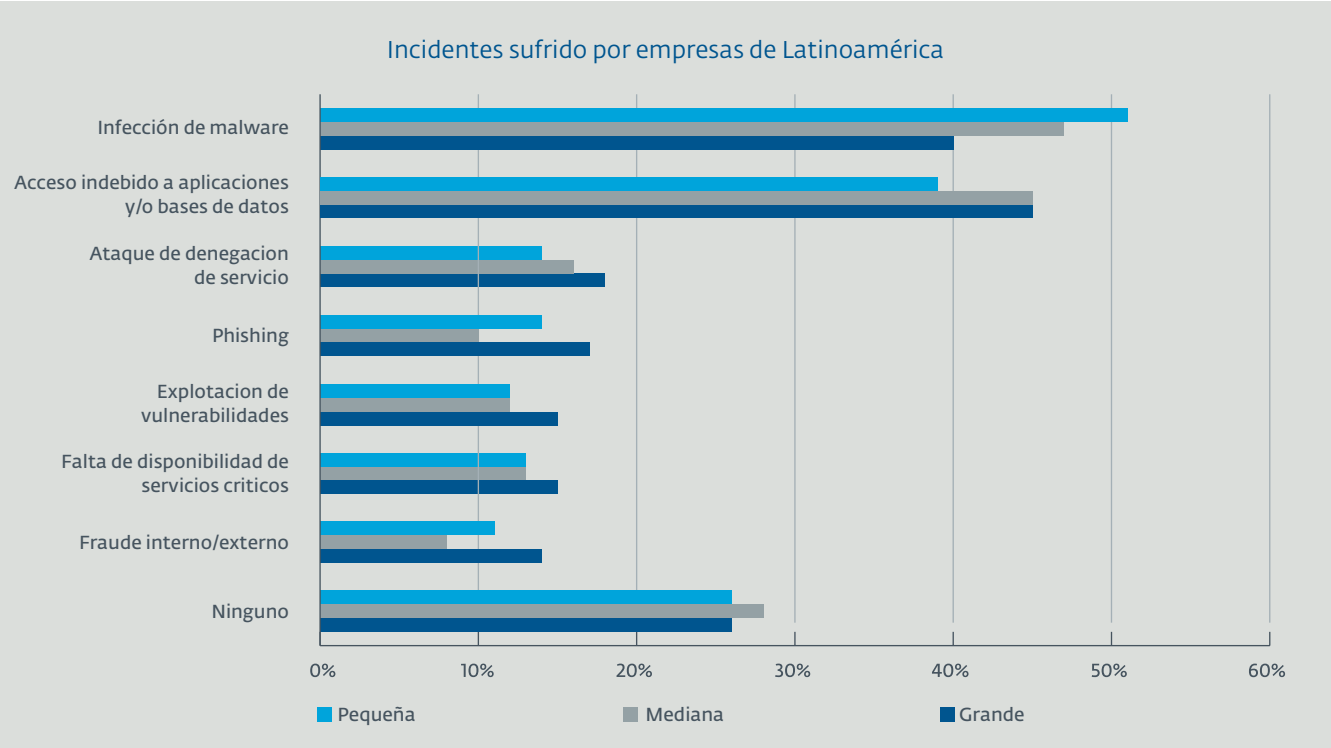


GRÁFICO 2 / Incidentes sufridos en empresas de Latam.

Malware

A nivel regional, las empresas encuestadas en Colombia, Venezuela, Ecuador, Perú y Nicaragua son la que reportaron mayores niveles de infecciones con códigos maliciosos.

Esto no es una sorpresa cuando observamos que, por ejemplo, en Colombia las detecciones de *botnets* crecieron un 10% durante 2014, y en países como Ecuador y Venezuela encontramos variantes de códigos maliciosos que no son los más comunes comparados con el resto de Latinoamérica[3].

En el caso de Perú, vemos que es uno de los países de la región con más detecciones de uno de los gusanos más propagados en la región, *VBS/Agent.NDH*[4]. Tanto esta amenaza como *JS/Bondat* han causado un dolor de cabeza a más de una empresa.

10%

Crecieron las amenazas de Botnes en Colombia durante el 2014

Porcentaje de empresas, por país, que sufrieron un incidente relacionado con infecciones de códigos maliciosos

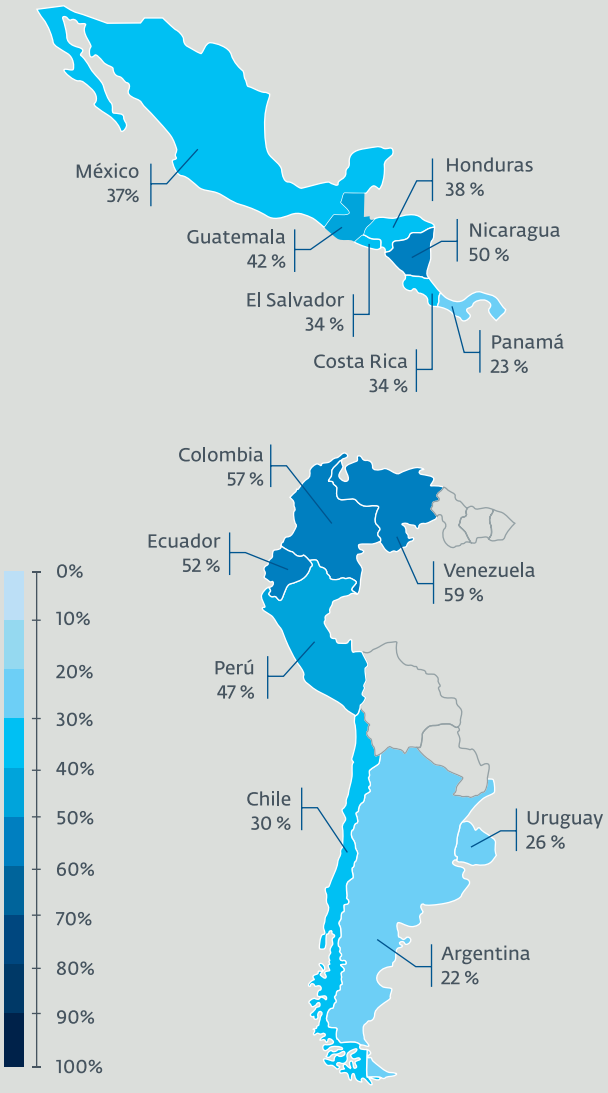


GRÁFICO 3 / Infecciones con malware por país.

3 **Zombis en Colombia, Ecuador y Venezuela: botnets a la orden del día.** http://www.welivesecurity.com/la-es/2014/10/23/zombis-colombia-ecuador-venezuela-botnets/

4 **Conoce al gusano más propagado en Latinoamérica.** http://www.welivesecurity.com/la-es/2014/09/17/gusano-mas-propagado-latinoamerica/

Acceso indebido

A diferencia de lo ocurrido en años anteriores, los incidentes relacionados con accesos indebidos a la información fueron los más reportados por las empresas de la región. De hecho, tan solo fueron 5 de los 14 países encuestados en los que menos de la mitad de las empresas tuvieron algún incidente de este tipo. En los 9 países restantes, más de la mitad de las empresas declararon haber tenido un incidente de este tipo.

Encontrar este incidente en la primera posición en todos los países de Latinoamérica es el reflejo de lo que se vio durante todo el año. Casos como los de Sony[5], Home Depot[6] , eBay[7] o Target[8] dejaron en evidencia lo que sucede con la información si no se toman los recaudos de seguridad adecuados.

La pérdida y exposición de información confidencial no es el único problema de un incidente de este tipo sino que también supone un problema para la reputación de la empresa, y una probable disminución de la confianza por parte de los clientes. De todas maneras, más allá de esto, cuando ocurre un incidente de seguridad -*ya sea detectado de manera interna o a través de algún agente externo a la compañía*- es notificado, las empresas deben relevar a qué información confidencial se tuvo acceso y cómo es que los cibercriminales o atacantes lograron poner sus manos sobre esos datos.

Asimismo, estos incidentes pueden darse cuando no existen controles o perfiles correctos en las redes de las empresas, y permiten que personal de otras áreas o sectores logren acceder a planes confidenciales de la gerencia, administración, recursos humanos y demás.

Porcentaje de empresas, por país, que sufrieron un incidente relacionado con acceso indebido a aplicaciones y/o bases de datos

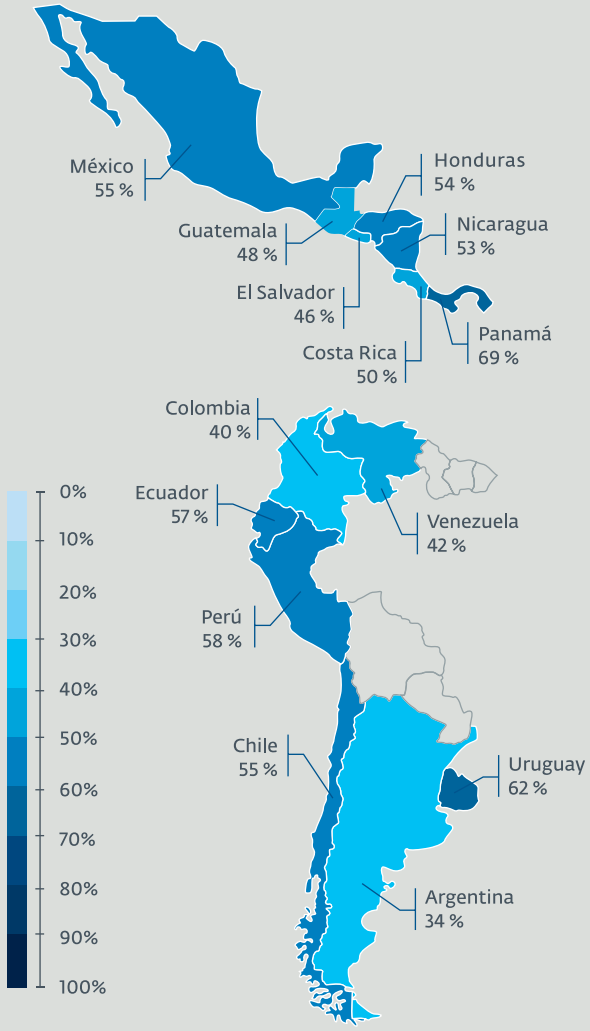


GRÁFICO 4 / Acceso indebido por país.

5 Intrusión a Sony Pictures y supuesta fuga de datos confidenciales. http://www.welivesecurity.com/la-es/2014/11/25/sony-pictures-fuga-de-datos-confidenciales/

6 Home Depot y los ataques al retail: cómo proteger el negocio. http://www.welivesecurity.com/la-es/2014/09/11/home-depot-ataques-retail-como-proteger-negocio/

7 eBay confirma brecha de seguridad y recomienda cambiar contraseñas. http://www.welivesecurity.com/la-es/2014/05/21/ebay-confirma-brecha-seguridad-recomienda-cambiar-contrasenas/

8 Renuncia el CEO de Target tras la grave falla en sus sistemas. http://www.welivesecurity.com/la-es/2014/05/05/renuncia-ceo-target-tras-grave-falla-sistemas/

Explotación de Vulnerabilidades

La explotación de vulnerabilidades es uno de los incidentes de mayor ocurrencia en las empresas grandes. En promedio 1 de cada 5 empresas de cada país sufrió la explotación de vulnerabilidades.

No obstante, esto tampoco es sorpresivo, especialmente cuando vemos casos como Poodle, que afectaba a SSL 3.0[9], Shellshock una grave vulnerabilidad en Bash[10], Heartbleed relacionado con una falla de seguridad en OpenSSL[11] e incluso vulnerabilidades en Smart TV[12]. Todo esto es la clara evidencia de por qué este tipo de incidentes entra en la categoría de los más ocurridos.

Además de estas vulnerabilidades tan reconocidas, hemos visto algunas campañas de ataques dirigidos en Europa o incluso en algunos países de la región, donde los cibercriminales decidieron utilizar exploits relacionados a documentos de ofimática, como archivos de Word, PDF y vulnerabilidades en Flash.

Para los equipos de seguridad de las empresas, es importante prestar atención a las detecciones que ocurren dentro de la red, con el fin de identificar patrones y tendencias que puedan traer a la luz el motivo de tales intentos de explotación.

Porcentaje de empresas, por país, que sufrieron un incidente relacionado con Explotación de Vulnerabilidades

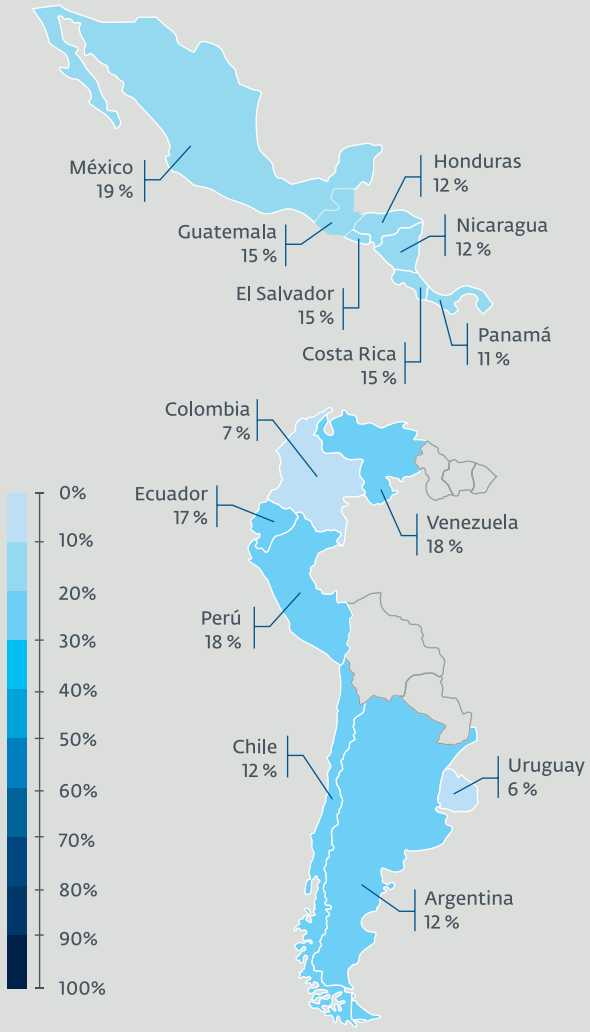


GRÁFICO 5 / Explotación de vulnerabilidades por país.

9 Poodle, la vulnerabilidad en SSL 3.0 y cómo te podría afectar. http://www.welivesecurity.com/la-es/2014/10/15/poodle-vulnerabilidad-ssl-3/

10 Shellshock, la grave vulnerabilidad en Bash -y todo lo que debes saber. http://www.welivesecurity.com/la-es/2014/09/26/shellshock-grave-vulnerabilidad-bash/

11 5 cosas que debes saber sobre Heartbleed. http://www.welivesecurity.com/la-es/2014/04/09/5-cosas-debes-saber-sobre-heartbleed/

12 Peligro para los Smart TV: una vulnerabilidad permitiría ataques en masa. http://www.welivesecurity.com/la-es/2014/06/10/peligro-smart-tv-vulnerabilidad-ataques-en-masa/

04 / ¿Cómo se están protegiendo las empresas de Latinoamérica?

En este momento, ya contamos con un panorama de las preocupaciones de los encargados de la Seguridad de la Información en las empresas de Latinoamérica y aquellos incidentes con los cuales tuvieron que lidiar durante los últimos doce meses. Ahora vale la pena analizar cómo se organizan las empresas para enfrentar estos incidentes y qué controles y/o acciones llevan a cabo para hacerlo.

Encargados de la gestión

Una de las preguntas más habituales dentro de las organizaciones está relacionada con la responsabilidad de la gestión de la seguridad. Resulta interesante ver que cerca del 60% de las empresas encuestadas delega la responsabilidad de gestionar la Seguridad de la Información al área de TI, lo cual puede generar conflictos de operación, o incluso de implementación y seguimiento, ya que también dependería de la misma área.

Tal vez para las empresas más pequeñas resulta difícil contar con un área que se encargue de la gestión de la seguridad. De hecho, cerca del 20% de las empresas pequeñas en la región aún no cuentan con un área que se encargue de gestionar la seguridad, y en aquellas donde sí la hay la misma está relacionada con la Gerencia General. Sin embargo, que casi un 25% de las pequeñas empresas siga esta tendencia no está del todo mal ya que al menos separan la gestión de la parte operativa. Lo que sí resulta importante es vincular otras áreas al proceso para que el seguimiento y la implementación se ajusten a las necesidades reales de la organización.

Para las empresas más grandes es más habitual que la tarea de gestionar la seguridad esté en áreas específicas de seguridad, de Gestión de Riesgo o incluso áreas tan diversas como puede ser una Gerencia Financiera. Más allá de la ubicación dentro del mapa organizacional, lo más relevante es que la gestión tenga los suficientes recursos para poder realizar las implementaciones necesarias a fin de garantizar la Seguridad de la Información.

Distribución del presupuesto

Cuando se pregunta si se considera suficiente la asignación de presupuesto para la gestión de la Seguridad de la Información, cerca del 57% de las empresas encuestadas coinciden en que no lo es, lo cual sigue estando de acuerdo a lo que se vio en años anteriores.

Si bien es claro que las amenazas siguen presentándose, además de que se van diversificando e incluso aumentando, esto no se ve acompañado de un crecimiento fuerte en el presupuesto asignado para seguridad, tal como se puede ver en el crecimiento de la asignación de presupuesto mostrado en el ***Gráfico 6.***

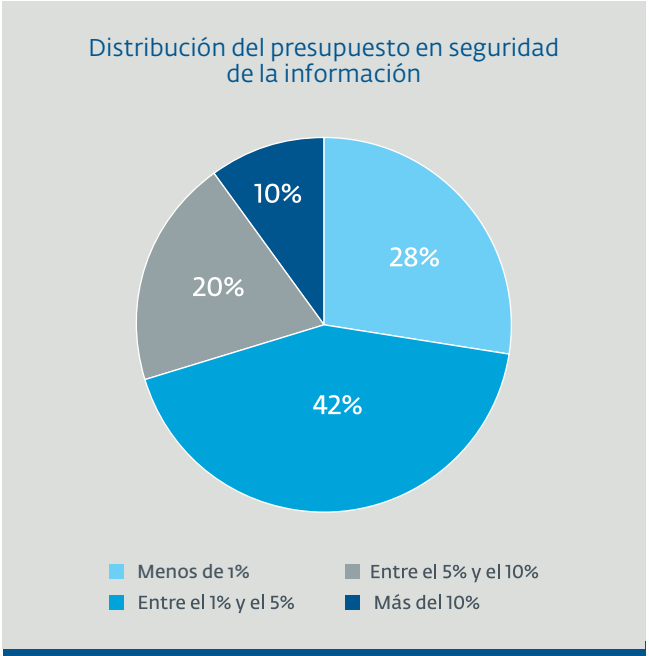


GRÁFICO 6 / Distribución del presupuesto para la Seguridad de la Información.

Está claro que la cantidad de dinero que se invierte en seguridad no determina si una gestión será exitosa o no. Sin embargo, es importante que se destine la cantidad de dinero adecuado para garantizar que los controles a implementar sean los que realmente se necesitan. No siempre tener

lo último en tecnología garantiza la mejor protección; hay otros factores como la gestión y la educación que son igualmente importantes y que seguramente no impliquen los mismos niveles de inversión.

Actividades de concientización

Cuando se trata de garantizar la Seguridad de la Información en una organización el factor humano cuenta con un lugar más que relevante y los programas de concientización son el principal y más efectivo control que se pueda implementar para asegurarlo.

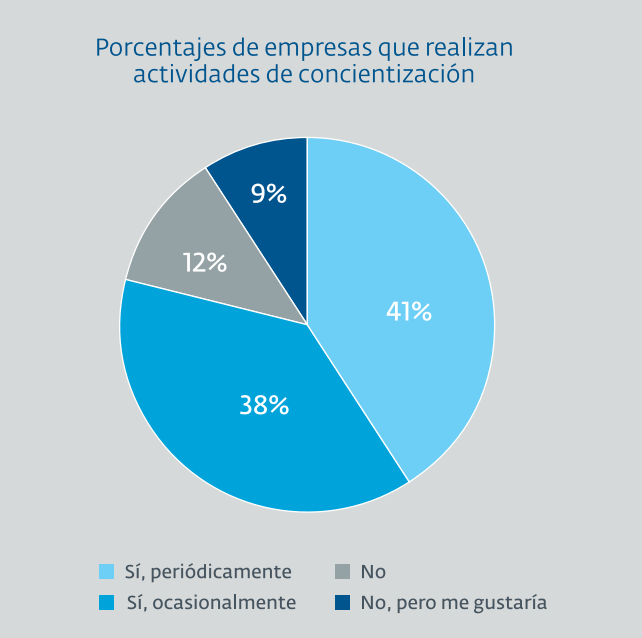


GRÁFICO 7 / Actividades de educación en las empresas.

Sin embargo, el 20% de las empresas todavía no realiza actividades de este tipo. Además, la educación a los empleados debe ser un proceso constante, y de las empresas encuestadas el 38% lo hace de forma ocasional, lo cual si bien es un paso importante, no es suficiente para garantizar realmente la adopción de las mejores prácticas.

Hace tiempo que vemos que incidentes de *phishing* son utilizados en campañas de APTs, de modo que incrementar los esfuerzos en la concientización se convierte en una actividad casi imperativa, ya que la educación es una de las principales barreras ante este tipo de ataques. De esta forma en lugar de recargar toda la responsabilidad de protección en la tecnología, se evita la infección de raíz gracias a contar con un usuario educado[13].

Controles tecnológicos

Los mayores esfuerzos para tratar de garantizar la Seguridad de la Información en una empresa giran alrededor de la tecnología. Si analizamos el ***Gráfico 8,*** que surge de preguntar por los niveles de implementación de las medidas de control más usuales en el mercado, vemos que hay una tendencia bastante marcada hacia cierto tipo de soluciones.

En el caso de los controles preventivos, vemos que el 92% usa software antivirus y el 85%, *firewalls*. En el caso de los controles correctivos, el *backup* es utilizado en el 74% de empresas, y si bien es aceptable, se esperaría que fuera mucho más cercano al 100% dada la importancia que representa contar con respaldos de información, más aun dado el crecimiento de amenazas como el ransomware[14].

13 Desde el Laboratorio de ESET Latinoamérica sabemos la importancia que tiene la educación en los planes de la Seguridad Informática y que en muchas ocasiones las empresas necesitan de cursos accesibles y orientados a sus empleados. Es dentro de este marco que la Plataforma Educativa de ESET (https://edu.eset-la.com/) cuenta con material libre y gratuito para que las empresas puedan capacitar a sus colaboradores.

14 Resumen de amenazas 2014: ¿cómo vivimos la seguridad este año?. http://www.welivesecurity.com/la-es/2014/12/30/resumen-de-amenazas-2014-seguridad/

Porcentaje de empresas encuestadas en Latam que tiene implementados controles basados en tecnología

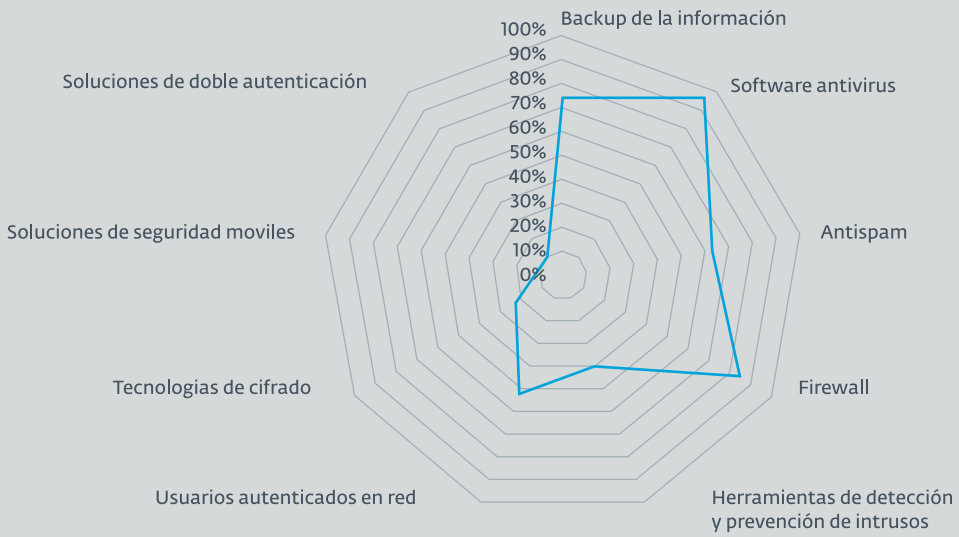


GRÁFICO 8 / Implementación de controles tecnológicos.

Sin embargo, hay controles que sorprenden por sus bajos niveles de implementación. Por ejemplo, apenas un 11% cuenta con una solución de seguridad en dispositivos móviles. Teniendo en cuenta que tendencias como **BYOD (Bring Your Own Device)** y el uso de smartphones y tablets se consolida cada vez más dentro de las organizaciones, y tal como mencionamos desde nuestro informe **"Tendencias 2013: Vertiginoso crecimiento de malware para móviles",** estamos frente rápido crecimiento de malware y amenazas para estos dispositivos[15], de modo que las empresas deberían aumentar considerablemente los controles para los equipos portables.

Además, incidentes como el acceso indebido a la información, que ha sido uno de los que más se presentó en los últimos doce meses, pueden ser controladoa con medidas como el **cifrado de la información** o la implementación de un **doble factor de autenticación.** En este sentido, se da una parajoda: existen las medidas de control adecuadas para contrarrestar muchos de los incidentes que más se presentan en las empresas de Latinoamérica, pero aún no se da el paso a su implementación, lo que da lugar a que información sensible pueda quedar expuesta.

La gestión de la Seguridad de la Información

Como ya mencionamos, contar con controles tecnológicos no es suficiente para tener la información protegida. En cuanto a los controles de gestión, se destaca solamente que casi el 90% de los encuestados afirman contar con una política de seguridad definida. Por otro lado, los restantes controles de gestión no alcanzan siquiera el 50% implementación.

15 **Laboratorio de Investigación ESET Latinoamérica. Tendencias 2013: Vertiginoso crecimiento de malware para móviles.** http://www.welivesecurity.com/wp-content/uploads/2014/02/tendencias_2013_vertiginoso_crecimiento_malware_moviles.pdf

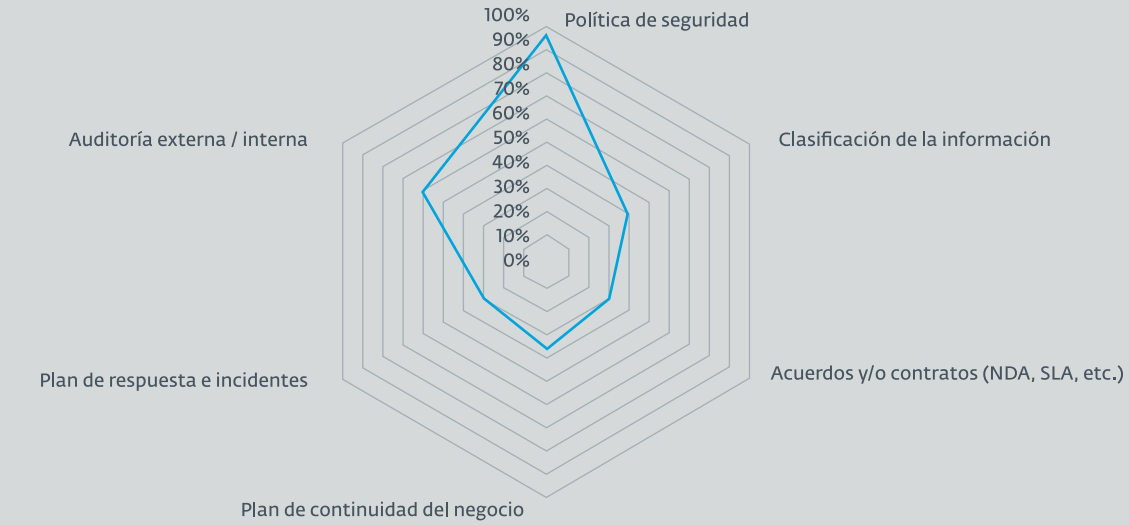


GRÁFICO 9 / Implementación de prácticas de gestión de la Seguridad de la Información.

El hecho de que apenas un 36% de las empresas tengan implementado un Plan de Continuidad del Negocio, y un porcentaje aún más bajo, el 29%, un Plan de Respuesta a Incidentes no se condice con las preocupaciones que hay al interior de las áreas de seguridad. Las preocupaciones tienen que ir acompañadas de un plan de acción. Tal vez lo más peligroso para la información sea seguir pensando que no se va a sufrir un incidente de seguridad y que, por lo tanto, no se necesita un plan de acción.

De acuerdo a la información anterior, vale la pena resaltar que los esfuerzos de las compañías en la región, de acuerdo a los ejecutivos encuestados, parecen estar más enfocados en los controles tecnológicos que en los de gestión. Es necesario tener en cuenta que la implementación de controles tecnológicos puede ser más costosa que de gestión, mientras que estos últimos pueden demandar más tiempo al principio, pero, en el mediano o largo plazo pueden representar una diferencia importante para garantizar la Seguridad de la Información.

29%

De las empresas encuestadas cuentan con un plan de respuesta a incidentes

05 / Cinco años de evolución del estado de la Seguridad Informática

A partir de la información que se ha podido recolectar durante los eventos en los que participamos año a año, a continuación presentamos la evolución de los incidentes y la adopción de los controles para su mitigación.

Aumento de las infecciones con códigos maliciosos

Uno de los incidentes que se mantiene dentro de los de mayor ocurrencia en las empresas de Latinoamérica es la infección con códigos maliciosos. Basándonos particularmente en las encuestas realizadas durante los eventos del año pasado este porcentaje creció, llegando a un 44%. Este dato no es menor, más teniendo en cuenta que el año pasado había tenido un decrecimiento importante.

Incidentes relacionados con seguridad informática para las empresas encuestadas en Latam-Malware

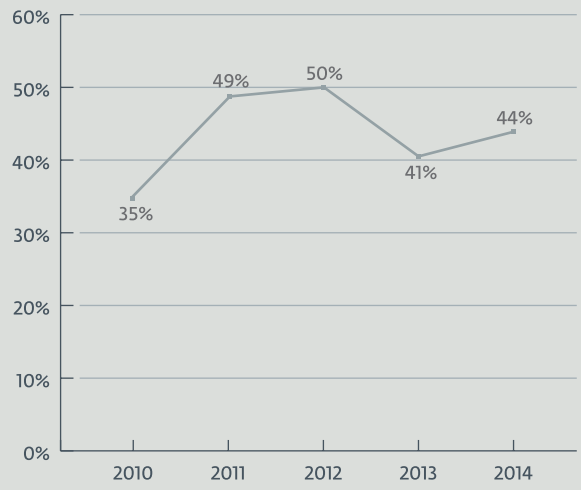


GRÁFICO 10 / Infecciones con malware durante 2014.

Estamos ante un crecimiento de las amenazas, incluso tal como se refleja en el informe del equipo de seguridad de HP[16] la cantidad de muestras relacionadas con códigos maliciosos siguen aumentando a un ritmo exponencial. No es una sorpresa que este tipo de comportamientos sea visto como una tendencia en materia de Seguridad de la Información, y de ahí la importancia de contar con las medidas de seguridad adecuadas que permitan garantizar los niveles de seguridad para que el negocio pueda funcionar correctamente.

Acceso indebido: lo que más creció

El incidente que más crecimiento tuvo dentro las empresas encuestadas en la región fue el acceso indebido a información, triplicando su ocurrencia al pasar de un 13% durante 2013 a un 44% en 2014. De hecho, es un comportamiento generalizado para todos los países de Latinoamérica.

Incidentes relacionados con seguridad informática para las empresas encuestadas en Latam-Acceso Indebido de la información

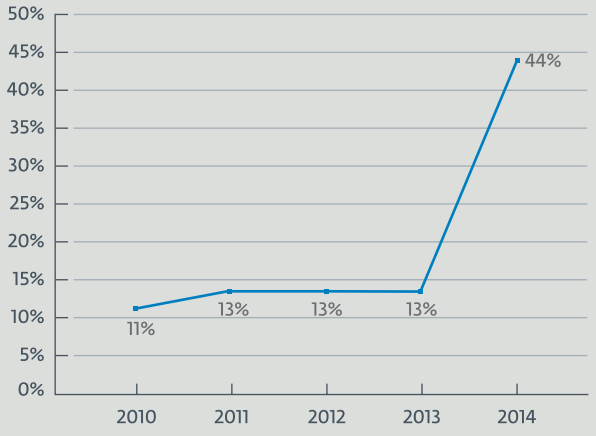


GRÁFICO 11 / Accesos indebidos durante 2014.

16 **HP Security Research. Cyber Risk Report 2015.** http://www8.hp.com/us/en/software-solutions/cyber-risk-report-security-vulnerability/

Si bien este incidente puede tener sus orígenes en muchas otras amenazas, refleja el interés creciente de los atacantes por información sensible de la que puedan obtener algún rédito económico.

Campañas como Windigo[17] son un ejemplo claro de cómo aparecen iniciativas enfocadas en robar información y que no están concentradas en una plataforma específica. De hecho, ya desde 2013 había información sobre códigos maliciosos que afectaban Linux; tal es el caso de ***Linux/Ebury*** un backdoor para ***OpenSSH*** utilizado para controlar los servidores y robar credenciales y ***Linux/Cdorked*** otro backdoor pero para HTTP utilizado para redirigir el tráfico web de los servidores afectados[18].

44%

Porcentaje de incidentes por infección de códigos maliciosos en las empresas de Latinoamérica

Crecimiento sostenido de los casos de fraude

A pesar de las normativas y la adopción de nuevas y mejores prácticas de gestión, los incidentes relacionados con el fraude externo o interno han tenido un crecimiento sostenido en los últimos años, pasando de un 4% de empresas que los reportaron en 2011 a un 12% en 2014. Es importante aclarar que para que un incidente sea considerado como fraude debe estar involucrado por lo menos algún empleado. En este sentido hay dos aspectos sobre los cuales es necesario trabajar. En primer lugar, adoptar controles tecnológicos que reduzcan la posibilidad de que por mala fe de un empleado la información de la compañía se vea en riesgo. De esta manera si limitamos los niveles de acceso a la información con controles como un doble factor de autenticación o el cifrado de los datos, va a ser mucho más difícil que personas que no estén autorizadas tengan acceso a datos privilegiados.

Incidentes relacionados con seguridad informática para las empresas encuestadas en Latam-Casos relacionados con fraude interno o externo

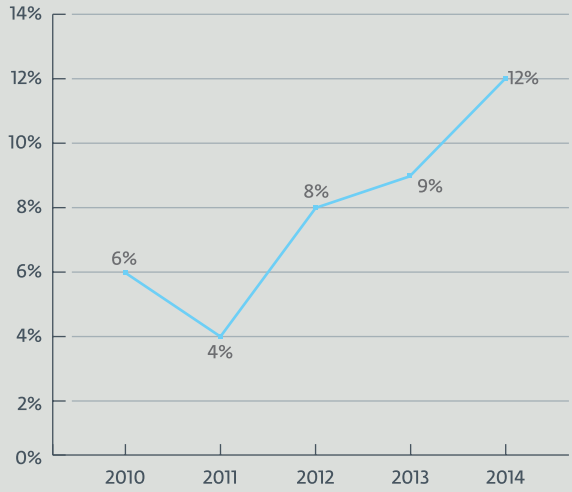


GRÁFICO 12 / Fraudes internos o externos durante 2014.

En segundo lugar, la gestión correcta de la información se convierte en el otro pilar necesario para reducir este tipo de incidentes. Si se mejoran aspectos sencillos como la clasificación de los activos de información, se podrán evaluar realmente cuáles son los riesgos que más exponen los datos importantes de la empresa.

17 WeLiveSecurity. Operación Windigo: Análisis de una gran campaña de malware que roba credenciales desde servidores Linux. http://www.welivesecurity.com/wp-content/uploads/2014/03/Operaci%C3%B3n-Windigo-ESET-Espa%C3%B1ol.pdf

18 Operación Windigo: malware utilizado para atacar más de 500.000 computadoras. http://www.welivesecurity.com/la-es/2014/03/18/operacion-windigo-malware-utilizado-para-atacar-mas-500-000-computadoras/

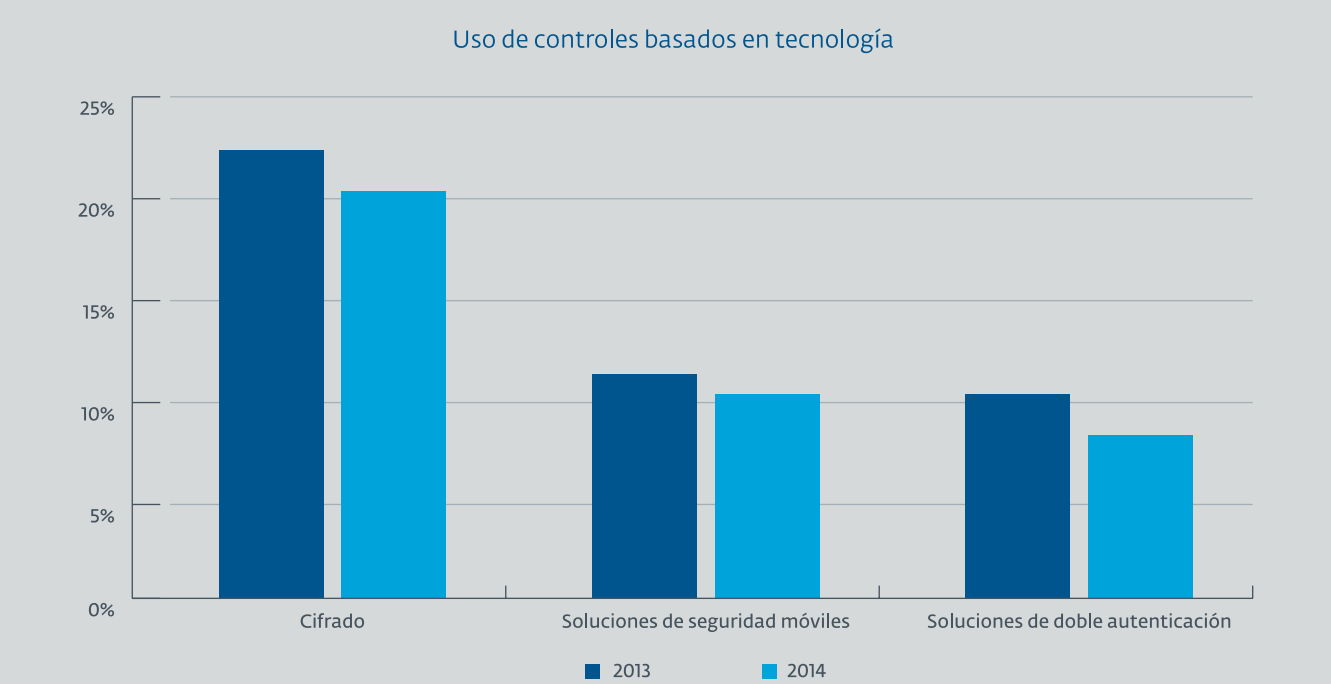


GRÁFICO 13 / Uso de controles tecnológicos durante 2013 y 2014.

Adopción de controles

Ya se mencionó que controles como el cifrado, la doble autenticación y las soluciones de seguridad en dispositivos móviles tienen los menores índices de adopción en las empresas de Latinoamérica. Pero lo que resulta aún más preocupante es que estos niveles decrecieron con respecto a 2013. De hecho, en ninguno de los tres controles se superaron los niveles de implementación que recolectamos durante 2013.

Ante un escenario que plantea amenazas cada más masivas y complejas, con una diversificación importante entre plataformas, resulta sorprendente que la implementación de estos controles no crezca. Si bien implementar una medida tecnológica no es la solución para reducir los incidentes de seguridad, es un primer paso fundamental.

Por lo tanto, es necesario que los encargados de la Seguridad de la Información en las empresas evalúen los riesgos y las consecuencias asociadas a su ocurrencia y, de esta forma, considerar implementar estas medidas de control.

Manejo de incidentes: el control que menos creció

Lo ideal dentro de una empresa sería estar libre de incidentes y que, por lo tanto, la información y la continuidad de las operaciones no se viera nunca en riesgo. Ya vimos que, en promedio, el 20% de las empresas en la región contaron con esta fortuna, pero la realidad indica que es difícil no sufrir ningún tipo de ataque (sea neutralizado o no) por lo tanto es necesario estar preparados por si un incidente de seguridad se presenta.

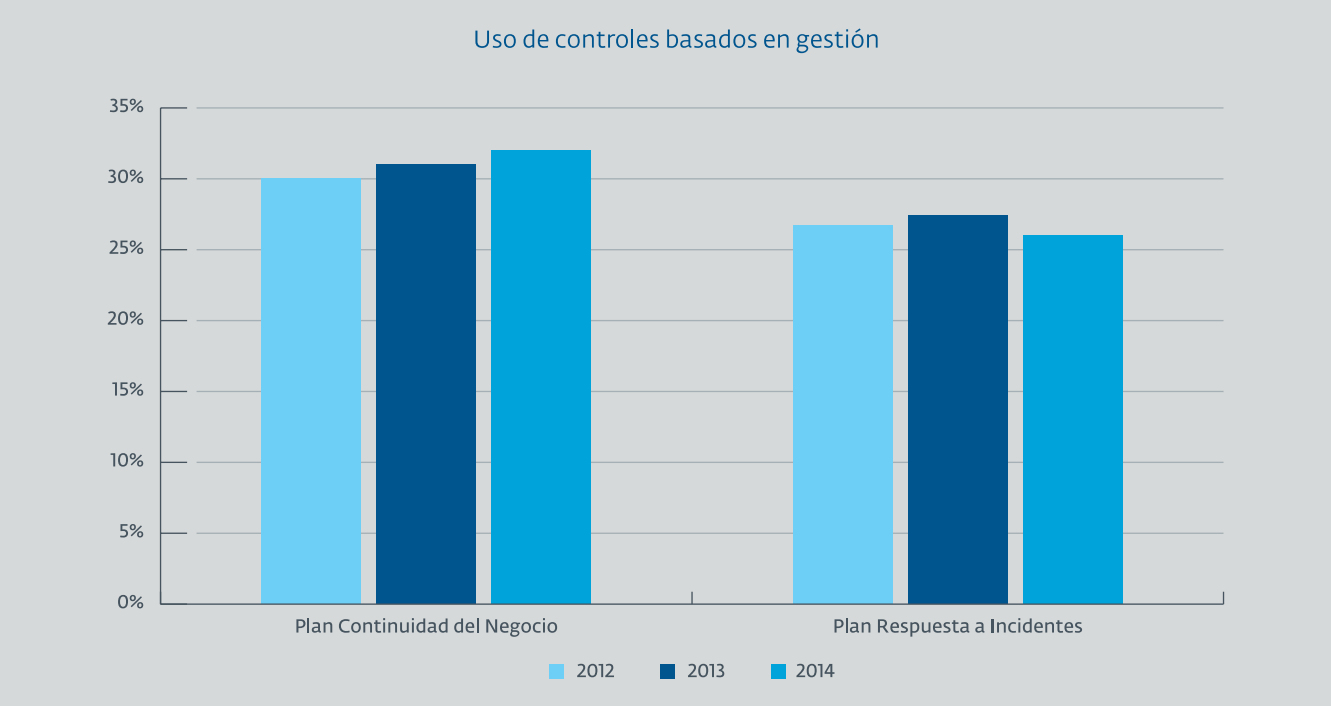


GRÁFICO 14 / Controles de gestión durante 2014.

Los procedimientos de recuperación, estrategias de comunicación y documentación de lecciones aprendidas son algunos de los puntos a tenerse en cuenta dentro de un Plan de Continuidad del Negocio y de un Plan de Respuesta a Incidentes.

Lo que resulta preocupante es que en Latinoamérica este tipo de controles basados en gestión no han tenido un crecimiento significativo en cuanto a su implementación en los últimos tres años. Considerar este tipo de planes ofrece una ventaja al momento de responder de forma planeada ante una crisis y minimizar su impacto en contra de los objetivos y misión de la empresa de manera proactiva.

20%

De las empresas en la región contaron con la fortuna de estar libres de incidentes

06 / Conclusiones

Cuando se habla de gestionar la seguridad dentro de una organización, hay por lo menos dos factores que resultan determinantes al momento de hacer alguna implementación o llevar a cabo un proyecto que implique invertir en seguridad. Por un lado, está la percepción que se tenga de las amenazas que pueden llegar a ocurrir y, por el otro, los incidentes que en algún momento hayan ocurrido.

Si bien es cierto que pueden existir otros factores, como las disposiciones legales, la competencia o el nivel de conocimiento dentro del equipo de seguridad que influyen en la manera de tratar la seguridad, la percepción y la historia marcan los hitos más relevantes.

Dentro de estos dos aspectos, muchas veces se cree que el tamaño de la organización va a ser determinante para enfocar las medidas de control. Pero después de analizar las opiniones de más de 3900 ejecutivos que trabajan en seguridad en diversas empresas de Latinoamérica, encontramos que la percepción de seguridad no cambia mucho entre tamaño de empresas, al igual que los incidentes que pueden sufrir.

Esta tesis nos sirve para derribar el mito de que los atacantes se centran únicamente en las empresas más grandes. De esta manera, es muy importante que todos los equipos de seguridad de las empresas hagan un análisis juicioso de sus estados y si realmente están teniendo en cuenta las diversas posibilidades que puede aprovechar un atacante para acceder a información valiosa.

Seguramente casos como Shellshock, Heartbleed o Poodle han abierto los ojos de muchos equipos de seguridad para considerar lo vulnerables que pueden llegar a estar si no se hace una adecuada gestión de los controles de seguridad que están implementados. Además, con el tiempo nos dimos cuenta de que las APTs son cada vez más utilizadas, lo que implica que debemos pasar de la preocupación a la acción para garantizar el nivel de seguridad que nuestra información requiere.

En este sentido, la implementación de controles sigue estando muy sesgada hacia las medidas más clásicas relacionadas con la tecnología. Y si bien es claro que deben seguir existiendo, si se las acompaña con una adecuada gestión serán incluso más efectivas como la primera barrera de protección contra las amenazas informáticas. No obstante, no se debe olvidar que ya se han incorporado nuevas tendencias en los lugares de trabajo, como BYOD, y que las amenazas se han diversificado para extender su capacidad de acción.

El uso de dispositivos móviles en las empresas es una realidad para la cual muchas aún no han tomado las medidas adecuadas. Vemos que el uso de soluciones de seguridad en este tipo de dispositivos sigue teniendo un nivel de implementación muy bajo, pero que el uso de *smartphones y tablets* cada vez crece más.

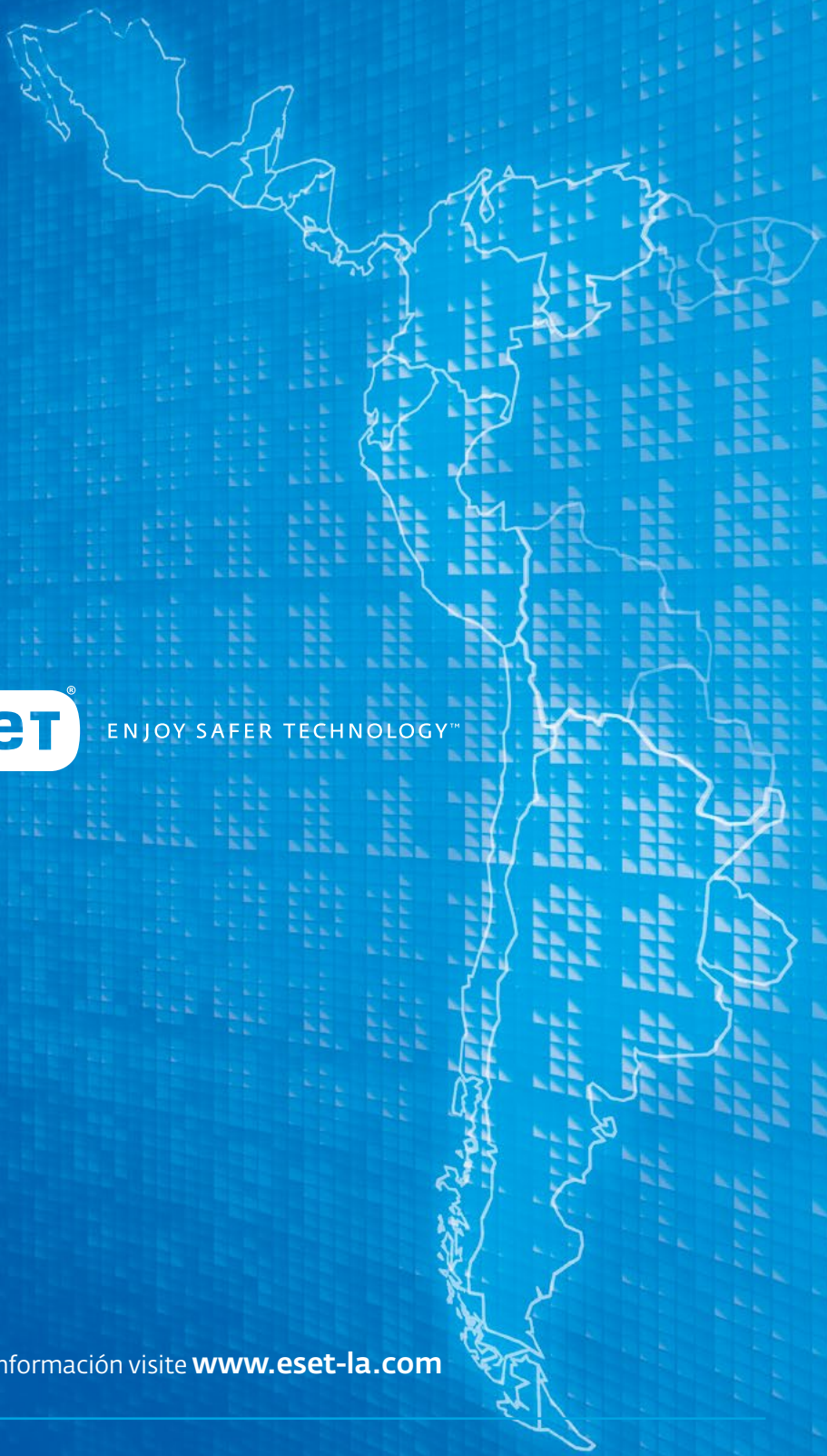
Tal vez es el momento más adecuado para que las empresas de la región comiencen a pensar en la gestión de la seguridad con una visión holística, como siempre debió hacerse. No solamente con tener un antivirus, un *firewall* y políticas de seguridad va a alcanzar para garantizar la Seguridad de la Información de forma más general. Es necesario expandir el análisis incluyendo nuevas tecnologías, no desconocer la diversidad de amenazas y, sobre todo, que todo el recurso humano de la empresa esté al tanto de esta realidad; de esta manera lograremos brindar los niveles de seguridad que necesitamos y podremos disfrutar de las posibilidades que nos ofrece la tecnología.

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.

© 2015 ESET, LLC. Todos los derechos reservados. ESET, el logo de ESET, ESET SMART SECURITY, ESET.COM, ESET.EU, NOD32, VIRUS RADAR, THREATSENSE, THREAT RADAR, y THREATSENSE.NET son marcas registradas, marcas de servicios y/o marcas registradas de ESET, LLC y/o ESET, spol. s.r.o. en los Estados Unidos y cualquier otra jurisdicción. Todas las otras marcas registradas y marcas que aparecen en estas páginas son propiedad de sus respectivos dueños y son utilizadas sólo en referencia a dichas compañías y servicios.



ENJOY SAFER TECHNOLOGY™

Para más información visite **www.eset-la.com**

/ESETLA /@ESETLA /company/eset-latinoamerica