The background is a dark, atmospheric image of a city in ruins. In the foreground, several zombies are visible, their faces pale and expressions menacing. They are standing on a street littered with debris. In the background, the city buildings are heavily damaged, with smoke rising from the ruins. The overall tone is grim and ominous.

Ten un plan de  
contingencia por si un  
apocalipsis zombi  
destruye tu WordPress



DO NOT  
COPY





jesus@jesusamieiro.com



# QUADRALIA



# la semana *php*.com







@JesusAmieiro

#WCZGZ



# 1. Contingencias

riesgos

# 1.1. Servicios externos

# Dominio caducado





Join Extra Crunch

Login

Search Q

Startups

Apps

Gadgets

Videos

Audio

Newsletters

Extra Crunch

Advertise

Events

—

More

Transportation

Apple

Tesla

Security


# Foursquare Goes Dark Too. Unintentionally.

MG Siegler @mgsiegler / 10:49 pm CET • March 27, 2010

Comment

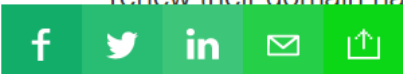
```
Domain Name: FOURSQUARE.COM
Registrar: GODADDY.COM, INC.
Whois Server: whois.godaddy.com
Referral URL: http://registrar.godaddy.com
Name Server: NS1.SLICEHOST.NET
Name Server: NS2.SLICEHOST.NET
Name Server: NS3.SLICEHOST.NET
Status: clientDeleteProhibited
Status: clientRenewProhibited
Status: clientTransferProhibited
Status: clientUpdateProhibited
Updated Date: 03-sep-2009
Creation Date: 25-mar-2002
Expiration Date: 25-mar-2010
```

Earlier we [made fun of Bing](#) for going “dark” today to save energy in a way that doesn’t at all save energy. But Foursquare has an actual way to do that: take down the entire service.

Yesterday, [Foursquare](#) had some downtime. That’s nothing new, startups have downtime all the time — see: Twitter, that was their M.O. for about a year — but the reason for [Foursquare’s](#)  appears to be a little humorous.

While the site is back up and running now, it appears that Foursquare forgot to renew their domain name, which [expired](#) on March 25. As a result, GoDaddy,

```
Domain Name: FOURSQUARE.COM
Registrar: GODADDY.COM, INC.
Whois Server: whois.godaddy.com
Referral URL: http://registrar.godaddy.com
Name Server: NS1.SLICEHOST.NET
Name Server: NS2.SLICEHOST.NET
Name Server: NS3.SLICEHOST.NET
Status: clientDeleteProhibited
Status: clientRenewProhibited
Status: clientTransferProhibited
Status: clientUpdateProhibited
Updated Date: 03-sep-2009
Creation Date: 25-mar-2002
Expiration Date: 25-mar-2010
```



the site and put up their own landing page. Which some

**TC Sessions:  
Robotics + AI  
2020**  
**Discover the  
latest  
robotics  
innovations**

**Berkeley**  
Mar 3

**Save \$150 Today**



Business ▶ Policy

## Microsoft forgets to renew hotmail.co.uk domain

Kindly soul, [El Reg](#) to the rescue

By [Tim Richardson](#) 6 Nov 2003 at 11:49

SHARE ▼

**Exclusive** Microsoft was busy covering up an almighty cock-up last night after forgetting to renew its hotmail.co.uk domain name.

Despite being warned that the domain for its popular Web mail service was up for renewal, it seems Microsoft - or whoever had the task of managing its hotmail.co.uk domain - overlooked this vital piece of administration.

As a result, last month Microsoft lost its claim to the domain and it was duly returned to the open market to be picked up by whomever fancied it

Luckily, the domain was snapped up on the same day - October 23. The new owner - a good hearted soul - then proceeded immediately to contact Microsoft, inform the giant of its slip and arrange to hand back the domain.

However, Microsoft didn't want to know. Despite phone calls and emails - and being fobbed off by Microsoft drones - our man behind this public-spirited deed was completely blanked by the software empire.

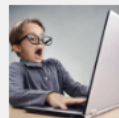
Microsoft only took notice when *The Register* contacted the company yesterday afternoon to enquire why its hotmail.co.uk site was registered to a private individual.

It was then we were told that the matter was under investigation and

### MOST READ



If you haven't shored up that Citrix hole, you were probably hacked over the weekend: Exploit code now available



It's a no to ZFS in the Linux kernel from me, says Torvalds, points finger of blame at Oracle licensing



Tea tipplers are more likely to live longer, healthier lives than you triple venti pumpkin-syrup soy-milk latte-swilling fiends



Y2K quick-fix crick? 1920s come roaring back after mystery blip at UK's vehicle licensing agency



Privacy activists beg Google to ban un-removable bloatware from Android

SUBSCRIBE TO OUR WEEKLY  
TECH NEWSLETTER

SUBSCRIBE



# DDoS DNS



News

Opinion

Sport

Culture

Lifestyle

More

World UK Environment Science Cities Global development Football Tech Business Obituaries

## Hacking

This article is more than 3 years old

## DDoS attack that disrupted internet was largest of its kind in history, experts say

Dyn, the victim of last week's denial of service attack, said it was orchestrated using a weapon called the Mirai botnet as the 'primary source of malicious attack'

Major cyber attack disrupts internet service across Europe and US

Nicky Woolf in San Francisco

@nickywoolf

Wed 26 Oct 2016 21.42 BST



367 423



▲ Dyn estimated that the attack had involved '100,000 malicious endpoints', and the company said there had been reports of an extraordinary attack strength of 1.2 terabits (1,200 gigabytes) per second. Photograph: Alamy

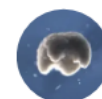
## most viewed



Why is Gwyneth Paltrow selling a candle that smells like her vagina?



At least six dead after huge sinkhole in China swallows bus and pedestrians



Scientists use stem cells from frogs to build first living robots



Harry and Meghan: Queen gives reluctant blessing to couple's plans

Home

Noticias

# Un ataque DDoS a Dinahosting tumba 60.000 webs españolas

NOTICIA

 [CARRO](#) [SOBRE DINAHOSTING](#) [EN PROMO](#) [ÁREA CLIENTE](#)

[DOMINIOS](#) [HOSTING](#) [VPS](#) [DEDICADOS](#) [REALCLOUD](#) [HOUSING](#) [RESELLERS](#) [MÁS SERVICIOS](#) [GRATIS](#)

[REGISTRO](#) [LINUX/WINDOWS](#) [TU MEDIA](#) [SOLO PARA TI](#) [MUY SENCILLO](#) [TU SERVER EN DH](#) [GANA CON DH](#) [PARA TU PROYECTO](#) [GRATIS EN DH](#)

[CLASIFICA GRATUITA](#) [AYUDA DESK 900 854 000](#) [TE LO EXPLICAMOS CON DETALLE](#) [O ABRE UN CHAT](#)

## TU CERTIFICADO SSL AL MEJOR PRECIO

¡Más seguridad y confianza para aumentar tus ventas!



**Mighty Marcos**

Compañero de Strong Miguel

Cuando Mighty Marcos entra en el Campo de Batalla con la carta SSL...



**Thawte SSL 123**

Aumenta la seguridad de la web con un Thawte SSL 123. Pon en juego esta carta y te ahorras un...



**Thawte Wildcard SSL**

Asegura tu servidor y subdominios con un solo certificado. Con esta carta te ahorras un...



**Strong Miguel**

Criatura - Programador PHP

La fuerza bruta puede a veces abrir una puerta cerrada, pero Strong Miguel lucha con Wildcard SSL.

# Pagos bloqueados



# Should Startups Avoid Stripe? How We Got Our Account Back

By [Mark Gavalda](#) • Updated on July 8, 2019



362 Shares



**Update:** This post was originally written back in 2014. A few hours after this was published we were contacted by various people at Stripe and got our account reinstated. And we have had no problems with them since. [Skip down to the follow-up.](#)

# Correo transaccional bloqueado



Data Centre ► **Cloud**

## SendGrid services are down and out of action

Tried logging in or signing up? Big bag of fail? Thought so

By [Andrew Silver](#) 16 Oct 2017 at 09:26

4 SHARE ▼



Anyone wanting to log in or sign up to cloud-based email marketing service SendGrid is out of luck as an unspecified glitch has taken its services offline.

At 0051 PDT (0851 BST), the firm said in a [status update](#), "We are currently investigating reports of intermittent availability of our login and sign up pages. We apologise for any inconvenience."

SendGrid has over 100,000 customers, who use the service for everything from sending newsletters to transaction or sign-up

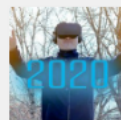
### MOST READ



ICANN finally reveals who's behind purchase of .org: It's [redacted] and [redacted] – you don't need to know any more



Are you getting it? Yes, armageddon it: Mass hysteria takes hold as the Windows 7 axe falls



Welcome to the 2020s: Booby-trapped Office files, NSA tipping off Windows cert-spoofing bugs, RDP flaws...



World's richest bloke battles Oz catastro-fire with incredible AU\$1m donation (aka load of cheap greenwashing)



NASA is Boeing to get to the bottom of that Starliner snafu... plus SpaceX preps to blow up a Falcon 9

SUBSCRIBE TO OUR WEEKLY  
TECH NEWSLETTER

SUBSCRIBE



# 1.2. Infraestructura



# Desastres naturales



iStock

## Hurricane Sandy

The Huffington Post, Gawker, Gizmodo and BuzzFeed went offline after a the basement flooded at a data centre hosted by Datagram during **Hurricane Sandy**. Similarly, many leading telecoms firms such as Verizon were left without power during one of the worst storms in US history.

[See larger image](#)

iStock

## Lightning strikes Amazon and Microsoft data centres

Microsoft and Amazon's European cloud services were out for a weekend after its data centres were hit by lightning in Dublin in 2011.

The natural disaster took out the main power and the backup generator which meant that businesses on AWS EC2 platform and Microsoft's Business Productivity Online Suite **went offline.**



iStock

## Yahoo goes down

Yahoo's data centre staff were driven nuts by several rodents in its Santa Clara location.

Mike Christian, a director of engineering at the internet giant told a conference in 2012:  
"A frying squirrel did take out half of our Santa Clara data centre two years back."

Surprisingly, squirrels are often the cause of power outages **in the US**.





iStock

## Shark attacks Google

Not quite an attack on a data centre - but in August 2014, Google's Cloud product manager Dan Belcher said that the search giant wraps its trans-Pacific underwater cables in Kevlar to prevent against **shark attacks**. Several theories as to why sharks are attracted to underwater cables exist - including the idea that they mistake pulsing currents for threats.

# Seguridad (DDoS)

Advertisement

# 'Anonymous' hacking shuts down ALL websites hosted by GoDaddy including thousands of small businesses

- Web hosting giant hacked and all of the websites run through GoDaddy were shut down temporarily as a result of Monday's attack
- Service was eventually restored for the bulk of customers by 5:43pm

By DAILY MAIL REPORTER

PUBLISHED: 23:36 GMT, 10 September 2012 | UPDATED: 12:06 GMT, 11 September 2012



35

View comments

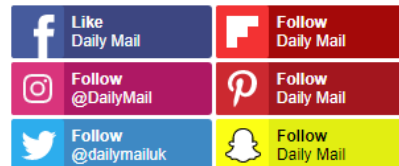
Thousands and possibly millions of websites hosted by GoDaddy.com were down for several hours on Monday, causing trouble for the mainly small businesses that rely on the service.

A Twitter feed that claims to be affiliated with the 'Anonymous' hacker group says it was behind the outage, but this couldn't be confirmed by the Associated Press.

**FoxNews** identified the hacker as twitter user Own3r after he emailed the site and they verified his identity through various Twitter claims.


☐ Site ☐ Web Enter your search Search

Advertisement



## DON'T MISS

**EXCLUSIVE** Smiling Meghan Markle visits women's shelter to 'boost spirits' as she is seen for the first time since fleeing the UK



► Sam Faiers and Ferne McCann kick off Billie's 30th birthday with montage of throwback snaps spanning from childhood to TOWIE fake tan fails



► Rochelle Humes delights fans as she introduces adorable daughters Alaia, 6, and Valentina, 2, to social media



► Nicole Scherzinger, 41, showcases her washboard abs in a neon crop top as she cosies up to muscular





Follow Slashdot blog updates by subscribing to our blog RSS feed

## Linode Under DDoS Since Christmas (linode.com)



149

Posted by Soulskill on Friday January 01, 2016 @08:03PM from the angry-people-creating-other-angry-people dept.

[hol](#) writes:

Linode has been getting hit with DDoS attacks since Christmas Day, and it looks like their pain is set to continue. The attackers are rotating DDoS traffic through various regions of Linode's service. They say, "All of these attacks have occurred multiple times. Over the course of the last week, we have seen over 30 attacks of significant duration and impact. As we have found ways to mitigate these attacks, the vectors used inevitably change. As of this afternoon, we have mostly hardened ourselves against the above attack vectors, but we expect more to come. ... Once these attacks stop, we plan to share a complete technical explanation about what has been happening." See [their status page](#) for updates.

ddos internet security 

### Related Links



[Majority of Americans OK With Warrantless Internet Surveillance](#)

[Submission: Linode under DDoS since Christmas](#)

[A Brief History of the ESA](#)

['Catastrophic' DDoS Attack Hits Linode Servers Over Labor Day Weekend](#)

Linode Under DDoS Since Christmas

Archived Discussion

Load All Comments

18 Full 71 Abbreviated 11 Hidden



Comments Filter: **All** Insightful Informative Interesting Funny

The Fine Print: The following comments are owned by whoever posted them. We are not responsible for them in any way.

# Errores humanos

# Amazon's massive AWS outage was caused by human error

One incorrect command and the whole internet suffers.

By Jason Del Rey | @DelRey | Mar 2, 2017, 2:20pm EST

f t SHARE



Sean Gallup / Getty

Amazon today blamed human error for the the big AWS outage that took down a bunch of

## The Latest



A new generation of philanthropists are ticked off at Trump — and their parents



The government is again asking Apple to





iStock

## Fat fingers deal a blow to Joyent

An administrator at cloud provider Joyent rebooted every single virtual server hosted in the company's data centre in May 2014 in one swipe, much to the **firm's embarrassment**.

"It should go without saying that we're mortified by this...the immediate cause was operator error, there are broader systemic issues that allowed a fat finger to take down a data centre," said CTO at Joyent, in **a post on Hacker News**.

# 1.2. Infraestructura

- Conectividad
- Alimentación
- Refrigeración
- Hardware de red

# 1.3. Hardware

- Disco duro
- Fuente de alimentación
- Memoria
- Tarjeta de red

# 1.4. Software

- Sistema operativo
- Servicios: NGINX, MySQL, FPM,...
- ~~No~~ actualización (WP): núcleo, plugin, tema
- Conflicto: plugins y/o temas



# 1.5. Seguridad

- Ataque fuerza bruta
- Exploits
- Inyecciones SQL

# 1.5. Seguridad

- Botnet: DDoS, SEO,...
- Defacement
- Fuga de información

# Millions of Facebook records were exposed on public Amazon server

Security researchers found the Facebook data on an unprotected server, including 22,000 passwords stored in plain text.



Alfred Ng



April 3, 2019 12:20 PM PDT

ES





# Capital One data breach involves 100 million credit card applications

Data stolen also included 140,000 Social Security numbers and 80,000 bank account numbers.



Alfred Ng, Mark Serrels July 30, 2019 9:35 AM PDT

ES



Capital One Financial's offices in San Francisco



## 2. Plan de contingencia









# Pérdidas

- Clientes/negocio: económica
- Reputación
- Datos operativos



# Plan de contingencia

- Seguridad de la información
  - Confidencialidad
  - Integridad
  - Disponibilidad —> Continuidad

# Plan de contingencia

- Investigar potenciales problemas
  - Evaluación riesgo
- Evitar o minimizar los potenciales problemas
  - Tratamiento del riesgo

# Plan de contingencia

- Riesgos
  - Identificar
  - Valorar probabilidad
  - Valorar gravedad
  - Tratarlos: medidas de control

# Identificar riesgos

- Dominio caducado
- DNS no operativo
- Datacenter caído
- Servidor caído



# Identificar riesgos

- Servicios caídos: NGINX, MySQL,...
- Aplicación (WordPress) caída
- Información incorrecta
- Servicio externo no operativo

# Identificar riesgos

- DDoS al servidor
- Fuga de información

# Evaluar riesgos

Probabilidad	
Descripción	Nivel
Inminente	5
Muy probable	4
Probable	3
Poco probable	2
Improbable	1

Gravedad	
Descripción	Nivel
Extremadamente grave	5
Significativamente grave	4
Grave	3
Leve	2
Irrelevante	1

# Tratar los riesgos

- Llevar a cabo medidas de control si es necesario
- Distintos escenarios —> distintos tramientos



# 2.1. Ejemplos

# DNS no operativo

- Probabilidad: poco probable
- Gravedad: significativamente grave
- Medidas control: contratación 2º proveedor

# Ataque fuerza bruta

- Probabilidad: inminente
- Gravedad: significativamente grave
- Medidas control: plugin de control, cambio del usuario por defecto, clave robusta

# Disco duro estropeado

- Probabilidad: poco probable
- Gravedad: extremadamente grave
- Medidas control: plan de respaldo, SLA
- Procedimiento de respuesta



# 3. Respaldos

# Respaldo

Hay 2 tipos de personas:

- Las que hacen copias de seguridad
- Las que nunca han perdido sus datos

# Respaldo

- Último punto de un plan de contingencia
- Respaldar:
  - Ficheros
  - Base de datos
  - Configuración y versión del software

# Responsable

- Personal de la empresa
- Administrador externo
- Empresa de hosting



# Método

- ~~Manual~~
- Automatizado
  - Scripts
  - Software/servicio especializado
  - Plugin

Completa



Diferencial



Incremental



# Número de copias

- Estrategia 3-2-1
  - 3 copias de los datos
  - En 2 soportes distintos
  - 1 respaldo en otra localización

# Periodicidad

- Mensual
- Semanal
- Diaria
- Varias veces al día



# Conservación

- Analizarlo para cada caso
- Ejemplo:
  - Mensuales: 3 meses
  - Semanales: 4 semanas
  - Diarios: 7 días

# Verificación

- Evitar restaurar respaldo incorrecto
- Verificar de forma periódica
- Designar un responsable

# Plugins

- UpdraftPlus
- BackWPup
- ManageWP Worker
- VaultPress (Jetpack)

# 4. Monitorización



# Monitorización

- Básica: uptime, certificado, dominio,...
- Avanzado: Zabbix, Nagios,...
- A medida: monitor, BBDD, UI



host ▾ interval 1m ▾

uptime

N/A

cpus

4

memory

2.084 GB

user

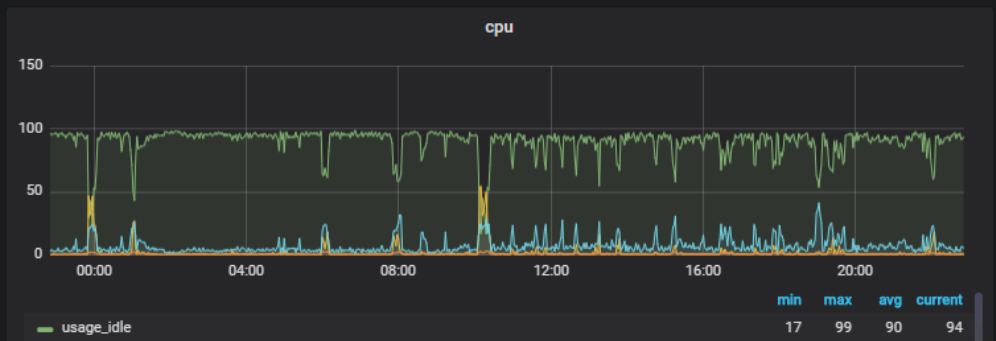
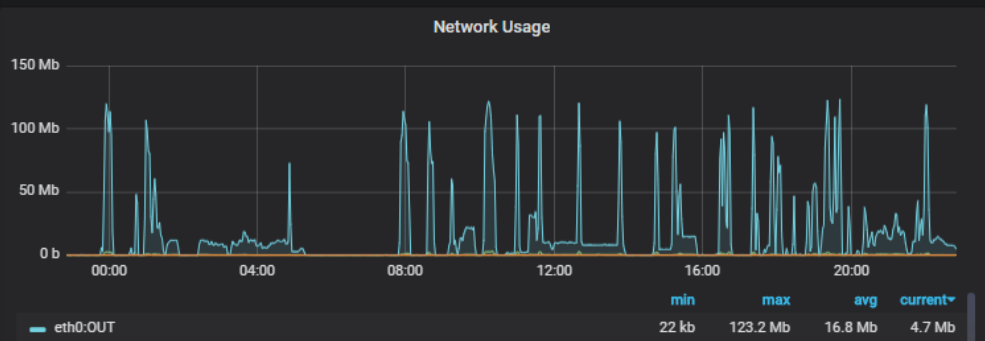
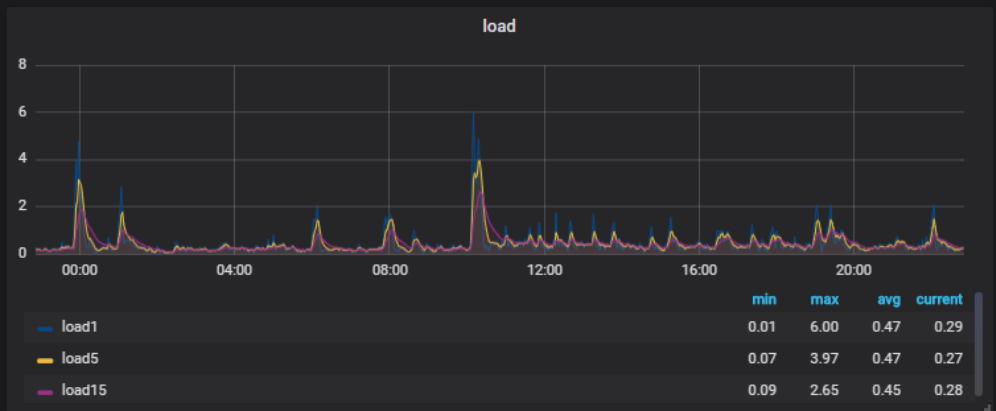
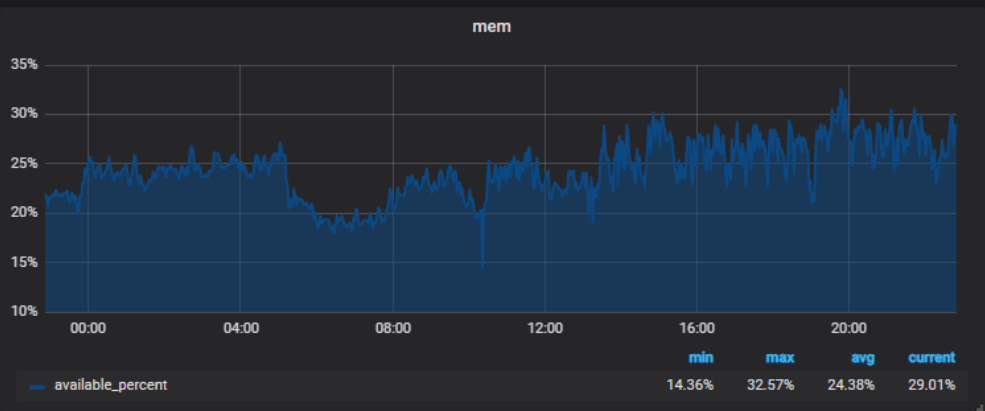
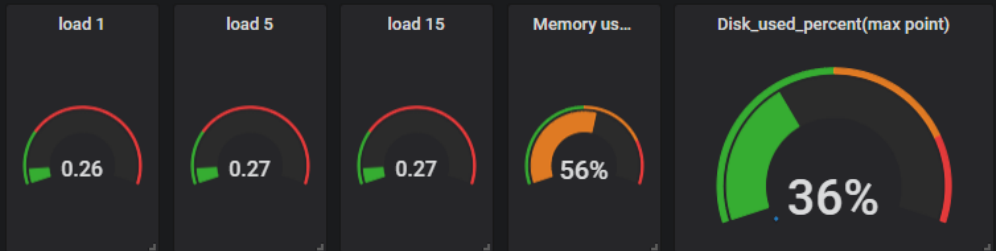
0

total proce...

133

total threads

221



# 5. Unas preguntas

ISP  
desaparece







## Gandi loses data, customers told to use their own backups

(gandi.net)

447 points by webrobots 5 days ago | [hide](#) | [past](#) | [web](#) | [favorite](#) |

370 comments

add comment

📄 MUST READ: [The dark side of IoT, AI and quantum computing: Hacking, data breaches and existential threat](#)

# Company shuts down because of ransomware, leaves 300 without jobs just before holidays

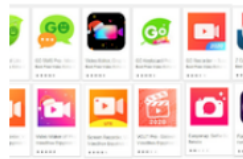
Company tells employees to seek new employment after suspending all operations right before Christmas.



By Catalin Cimpanu for Zero Day | January 3, 2020 -- 14:42 GMT  
(14:42 GMT) | Topic: [Security](#)



## MORE FROM CATALIN CIMPANU



As on Google Play, these ransomware applications are not for sale. They are available in other free or low-cost applications.

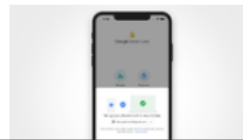
### Security

More than 600 million users installed Android 'fleeceware' apps from the Play Store



### Security

Facebook to notify users of third-party app logins



### Security

You can now use an iPhone as a security key for Google accounts

An Arkansas-based telemarketing firm sent home more than

SPECIAL FEATURE

NOTICIAS

## Una de cada cinco empresas atacadas por ransomware, cierra

Publicado el 4 agosto, 2017 por **Fernanda Ortiz**



Cuando uno se imagina cuáles pueden ser los objetivos de un ataque de ransomware, piensa con frecuencia en empresas grandes, tecnológicas y organismos gubernamentales. Pero no siempre sucede así. Muchas más veces de las que se cree, el ransomware ataca a pequeñas y medianas empresas, con consecuencias bastante desastrosas para ellas: una de cada cinco

LO ÚLTIMO

+LEÍDO

+COMENTADO



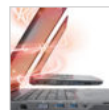
NOTICIAS / Hace 15 min  
**La Administración Trump quiere bloquear más ventas a Huawei**



NOTICIAS / Hace 3 horas  
**La inversión en tecnología a nivel global alcanzará los 3,9 billones en 2020**



NOTICIAS / Hace 4 horas  
**Banco Sabadell e IBM llegan a un acuerdo para el avance tecnológico de la entidad**



NOTICIAS / Hace 4 horas  
**Fujitsu apuesta por la Realidad Virtual en entornos empresariales con sus workstation**



NOTICIAS / Hace 7 horas  
**Google Chrome bloqueará las cookies de terceros en Chrome**



NOTICIAS / Hace 7 horas  
**Apple niega el acceso al iPhone de Pensacola y desata la ira de Trump**

MOVILIDAD PROFESIONAL

IMPRESIÓN PROFESIONAL

UNIVERSO LENOVO



# 6. Preguntas



jesus@jesusamieiro.com

