



# Guía de Seguridad en Informática para PYMES

Dra. Aury M. Curbelo

Universidad de Puerto Rico Recinto de Mayaguez

Facultad de Administración de Empresas

[aury.curbelo@upr.edu](mailto:aury.curbelo@upr.edu)

# *Certified Master Security Professional*

**CNDP**

Certified Network  
Defense Professional

ETHICAL HACKER

+

**CCFI**

Certified Cybercrime  
Forensic Investigator

=

**CMSP**

Certified Master  
Security Professional

Inter American University of Puerto Rico

# Certificaciones

# Objetivos

- Definir que es seguridad informática, seguridad física y lógica de las tecnologías de la información.
  - Enumerar las principios básicos de seguridad.
  - Mencionar los conceptos básicos de Confidencialidad, Integridad y Disponibilidad de datos.
  - Discutir las políticas y mecanismos de seguridad en informática.
  - Discutir el impacto de las redes sociales y la importancia de contar con una política de uso de las redes sociales en el negocio.
-

Copyright 2006 by Randy Glasbergen.  
[www.glasbergen.com](http://www.glasbergen.com)



**“Information security is a major priority at this company.  
We’ve done a lot of stupid things we’d like to keep secret.”**

# Ecosistema tecnológico



J	LONGITUDE
	-62.9619;
	-63.1975;
	-62.8174;
	-62.8958;
	47.59665 -63.2673;
	47.62411 -62.9363;
3.5 Y	47.55619 -62.71;
3.5 Y	47.53093 -62.71;
3.5 Y	47.82698 -62.71;
709 N	47.9557;
709 N	47.82698 -62.71;
709 N	47.9557;

# BYOD Is Riskiest

BYOD = Bring Your Own Device

Which device poses the greatest risk to your organization?

Any employee-owned mobile device



Work-issued smart phones, laptops/netbooks, tablets, broadband cards or flash drives

2011 ISACA IT RISK/REWARD BAROMETER

## Information Security and Risk Management Jobs on the Rise

Percentage of IT leaders projecting increased need\* for:

**34%**

RISK MANAGEMENT STAFFING

**40%**

INFORMATION SECURITY STAFFING

\*Over the next 12 months



**ISACA®**

Trust in, and value from, information systems

Source: 2011 ISACA IT Risk/Reward Barometer-US Edition  
([www.isaca.org/risk-reward-barometer](http://www.isaca.org/risk-reward-barometer))

<http://www.isaca.org/Pages/Survey-Risk-Reward-Barometer.aspx>



## Online Banking [Sign Off](#)

Locations · Mail · Help · En Español

Enter keyword(s)



Last sign in: 2/12/2011 at 10:13 p.m. ET

### - Personal Accounts

Select your accounts and information, visit the Security Center

GREEN  
TIP

Go Green.  
Use Paperless  
Statements.

Learn more

I want to...

#### Bank Accounts

##### Account

Home Equity Line of Credit 723

##### Balance

\$254,723.73

[View options](#)

Mortgage-4570

\$427,865.73

[View options](#)

My Portfolio

and more - see you

investments -

you single s

for where y

the Net

#### Communication Center

Mail

Alerts

#### Help Center

Help

#### Tutorials

Tutorials

#### How-to Videos

How-to videos

#### More Learning

More learning

SECURITY FAIRY

# **Our Disaster Recovery Plan Goes Something Like This...**



# Casos





Hannaford Bros. Supermarket Chain  
(Portland, ME)

*Date of Breach:* March 17, 2008

*Number of Records:* **4.2 Million**



TD Ameritrade Holding Corporation  
(Omaha, NE)

*Date of Breach:* September 14, 2007

*Number of Records:* 6.3 Million



Fidelity National Information Services  
Certegy Check Services Inc.  
(Jacksonville, FL)

*Date of Breach:* July 3, 2007

*Number of Records:* 8.5 Million total records

Bank of New York Mellon  
(Pittsburgh, PA)

*Date of Breach:* March 26, 2008

*Number of Records:* As many as 12.5 million customer records  
are thought to be compromised

UNITED STATES  
DEPARTMENT OF VETERANS AFFAIRS

U.S. Dept. of Veteran's Affairs  
(Washington, DC)

Date of Breach: May 22, 2006

Number of Records: As many as 28.6 Million records



TJ Stores (TJX)  
(Framingham, Mass.)

Date of Breach: January 17, 2007

Number of Records: 45.7 Million credit and debit card account numbers

## 40M credit cards hacked

Breach at third party payment processor affects 22 million MasterCards.

July 27, 2005: 6:16 PM EDT

Air Teeanne Sahadi CNN Money senior writer

CardSystems  
(Tucson, AZ)

Date of Breach: June 16, 2005

Number of Records: Over 40 million card accounts

## U.S. Government Suffers 'Largest Release Of Personally Identifiable Information Ever'

Records of more than 70 million military personnel in

U.S. Military Veterans

Date of Breach: October 2, 2009

Number of Records: 76 Million



¿Pasará esto  
en  
Puerto Rico?

# Policía y tribunales

1



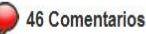
Enviar



Imprimir



Compartir



46 Comentarios



Tamaño de letra



## Suspenden vista para destitución de empleada que presuntamente robó datos de ciudadanos de Guayanilla

sábado, 18 de septiembre de 2010

05:07 p.m.

Inter News Service

La vista para la destitución de una empleada que presuntamente se apropió ilegalmente de documentos sensativos y confidenciales de la base de datos de la computadora de la Oficina de Servicios al Ciudadano de la Alcaldía de Guayanilla, fue suspendida, anunció el alcalde Edgardo Arlequín Vélez.

Sin embargo, el alcalde de Guayanilla admitió que a pesar de que hace dos meses se detectó el hurto de información, todavía no se ha referido información al Negociado Federal de Investigaciones (FBI) ni al Departamento de Justicia, para que tomen cartas en el asunto.

Un esquivo Arlequín Vélez dió a Inter News Service que aunque

“La vista para la destitución de una empleada que presuntamente se apropió ilegalmente de documentos sensativos y confidenciales de la base de datos de la computadora de la Oficina de Servicios al Ciudadano de la Alcaldía de Guayanilla”

“... la empleada que presuntamente utilizó un "pen drive (o puerto USB de almacenamiento de datos)" para almacenar la información de los ciudadanos que acudieron a solicitar servicios a la Casa Alcaldía.”

# Fugas de información en Puerto Rico

**U.S. Department of Health & Human Services**  
**HHS.gov** *Improving the health, safety, and well-being of America*

[HHS Home](#) | [HHS News](#) | [About HHS](#)      [Search](#)      [Search](#)      [OCR](#)      [All HHS](#)

Font Size [-](#) [+](#)      [Print](#)      [Download Reader](#)

## Health Information Privacy

[Office for Civil Rights](#)      [Civil Rights](#)      [Health Information Privacy](#)

[OCR Home](#) > [Health Information Privacy](#) > [HIPAA Administrative Simplification Statute and Rules](#) > [Breach Notification Rule](#)

### Breaches Affecting 500 or More Individuals

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. These breaches are now posted in a new, more accessible format that allows users to search and sort the posted breaches. Additionally, this new format includes brief summaries of the breach cases that OCR has investigated and closed, as well as the names of private practice providers who have reported breaches of unsecured protected health information to the Secretary. The following breaches have been reported to the Secretary:

[Full DataSet CSV format \(18 KB\)](#) [XML format \(57 KB\)](#)

Select a column head to sort by that column. Select again to reverse the sort order. Select an individual record to display it in full below the table.

Filter:  5 records showing

Name of Covered Entity	State	Individuals Affected	Date of Breach	Type of Breach	Location of Breached Info
MMM Health Care Inc.	NY	1,907	2010-02-04	Unauthorized Access/Disclosure	Paper
PMC Medicare Choice	NY	605	2010-02-04	Unauthorized Access/Disclosure	Paper
Puerto Rico Department of Health	PR	400,000	2010-09-21	Unauthorized Access/Disclosure, Hacking/IT Incident	Network Server
Puerto Rico Department of Health	PR	2,621	2010-03-14	Unknown	Computer
Puerto Rico Department of Health	PR	115,000	2010-09-03	Unauthorized Access/Disclosure	Other Portable Electronic Device

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breatchtool.html>

# “Fuga de información”



“De acuerdo a estudios de mercado, 63% de las empresas públicas y privadas pierden anualmente archivos de información valiosa, pero solo 23% es por robo.

De la pérdida de información 57% se debe al extravío de equipos portátiles, como computadoras, celulares, agendas electrónicas, o dispositivos como discos compactos y memorias USB.”

<http://www.liderempresarial.com/num175/10.php>

# ¿Qué es fuga de Información?

- “Se denomina **fuga de información** al incidente que pone en poder de una persona ajena a la organización, información confidencial y que sólo debería estar disponible para integrantes de la misma.”

# Ejemplos de fuga de información

- Un empleado vendiendo información confidencial a la competencia (incidente interno e intencional),
- Un empleado que pierde un documento en un lugar público (incidente interno y no intencional)
- La pérdida de una laptop o un *pen drive*,
- Acceso externo a una base de datos en la organización o un equipo infectado con un Spyware que envíe información a un delincuente.

# Incidentes de Seguridad

Personas contra PCs

## Amenazas Internas

Integridad de empleados

Robo de propiedad intelectual

Fuga de información

Espionaje industrial

Interrupción operacional

Conflictos entre empleados

Crimen corporativo

Conducción de negocio personal

Bajo desempeño del empleado

PCs contra PCs

## Amenazas Internas y Externas

Hackers y el crimen organizado

Eventos Zero Day: Worms, Viruses, Troyanos

Proxies, P2P, Herramientas Hackers, Exploits

Anti Forensic, Keyloggers, ScreenLoggers

Root Kits

Alternate Data Stream

Esteganografía

Políticas de seguridad Interna

Compliance



**Una de las principales amenazas que enfrenta toda organización para proteger su información es el factor humano.**



**Los estudios demuestran que el 75 por ciento de los incidentes de seguridad son causados por errores o por desconocimiento humano.**

---

# **Seguridad informática es vital para las empresas.**



**Cada vez es más importante identificar al trabajador o usuario que accede a un ordenador o a un software.**

---

# **Es común escuchar la frase "mi empresa es pequeña, quien va a desear mi información"**



Las PYMES son las que se encuentran más desprotegidas, y por ende más fácil de vulnerar por programas dañinos o "curiosos" con conocimientos limitados pero con malas intenciones.



**Las pequeñas empresas  
suelen ser más vulnerables  
porque **supuestamente** no  
disponen de los recursos  
para protegerse de forma  
adecuada contra los ataques.**

**Los sistemas de información se han  
constituido como una base  
imprescindible para el  
desarrollo de cualquier actividad  
empresarial...**



**Es fundamental saber qué recursos de la compañía necesitan protección para así controlar el acceso al sistema y los derechos de los usuarios del sistema de información.**

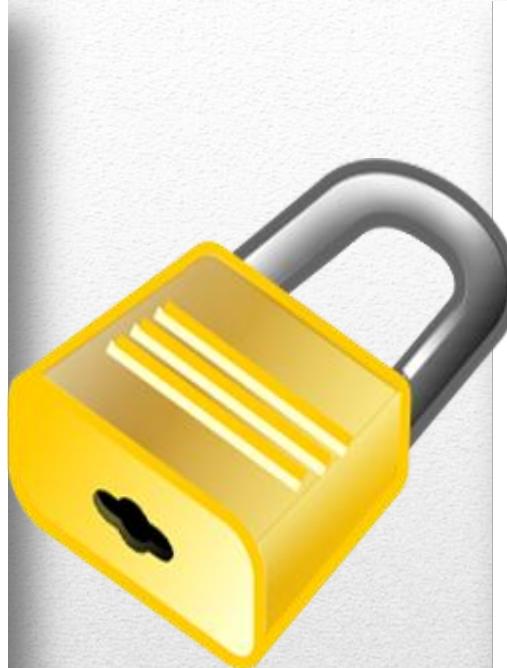
---



NISTIR 7621

## Small Business Information Security: The Fundamentals

Richard Kissel



National Institute of Standards and Technology  
Technology Administration  
U.S. Department of Commerce

Generally Accepted Principles and Practices  
for Securing  
Information Technology Systems

## National Institute for Standards and Technology (NIST)

Marianne Swanson

*Dashara Cottman*

<http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf>

<http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf>

# Guías de Seguridad

---



2011 ISACA IT Risk/Reward Barometer—Latin America Edition  
[www.isaca.org/risk-reward-barometer](http://www.isaca.org/risk-reward-barometer)  
\*n=235 unless otherwise indicated

Respondents are Latin American business and IT professionals,  
and are members of ISACA.

Due to rounding, responses may not add up to 100%.

Media Inquiries:  
Kristen Kessinger, ISACA, +1.847.660.5512, [news@isaca.org](mailto:news@isaca.org)

1. How well does your enterprise integrate IT risk management with its overall approach to risk management?
  - a. Very effectively—Management of IT risks is fully integrated into our business risk management approach. 23%
  - b. Somewhat effectively—Management of IT risks is somewhat addressed in our business risk management approach. 47%
  - c. Not effectively—Management of IT risks is rarely, if ever, included in our business risk management approach. 18%
  - d. We do not have a formal approach to business risk management. 12%
2. Which of the following do you believe about cloud computing (including software as a service)? (n=234)
  - a. The benefits of cloud computing outweigh the risks. 16%
  - b. The risks of cloud computing outweigh the benefits. 20%

5. Which one of the following is your enterprise's greatest hurdle when addressing IT-related business risk? (n=227)

- a. Not sure how to tailor best practices to the environment 10%
- b. Lack of management support 14%
- c. Budget limits 32%
- d. Lack of cooperation across risk management silos 15%
- e. Business lines not willing to fully engage in risk management 30%

8. Which of the following mobile devices do you believe represents the greatest risk to your enterprise? (n=228)

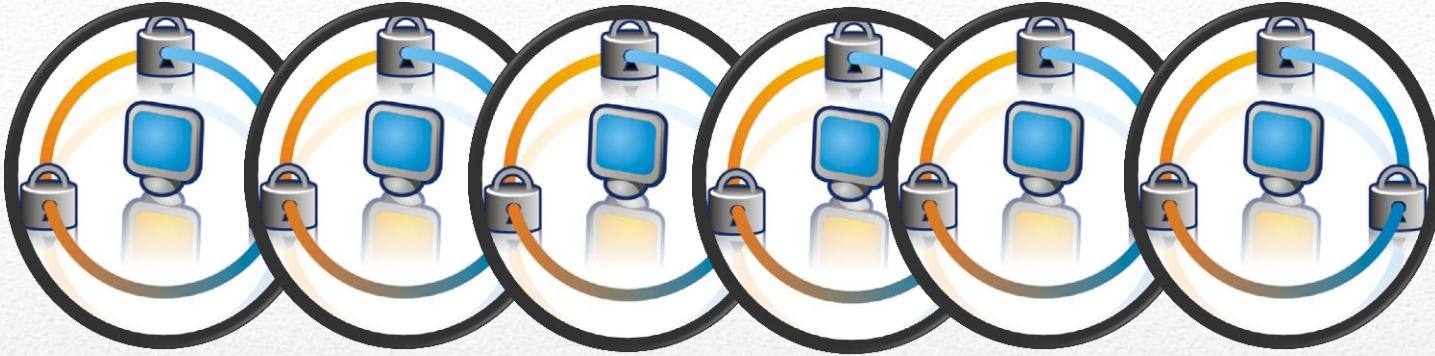
- a. Work-supplied smart phones 15%
- b. Work-supplied laptops/netbooks 25%
- c. Work-supplied tablet computers 3%
- d. Work-supplied broadband cards 0%
- e. Work-supplied flash drives 15%
- f. Any employee-owned mobile device 37%
- g. None of these pose significant risk. 4%
- h. Other (please specify) 0%

9. Does your enterprise have a security policy in place for mobile computing? (n=227)

- a. Yes, and it is kept up to date and/or well communicated to staff. 27%
- b. Yes, but it is in need of updating and/or most staff are not aware of it. 30%
- c. No, but we are planning to implement one soon. 28%
- d. No, and there are no plans for one. 10%
- e. I am unsure. 4%

# ¿Qué es seguridad en infomática?

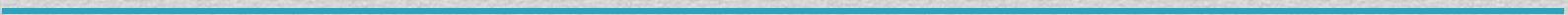
- La seguridad puede entenderse como aquellas reglas técnicas y/o actividades destinadas a prevenir, proteger y resguardar lo que es considerado como susceptible de robo, pérdida o daño, ya sea de manera personal, grupal o empresarial.
- En este sentido, es la información el elemento principal a proteger, resguardar y recuperar dentro de las redes empresariales.



**La seguridad informática es una disciplina que se relaciona a diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios.**

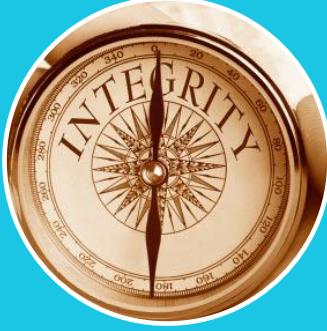
# La seguridad de los datos

- La seguridad de los datos comprende tanto la protección física de los dispositivos como también la ***integridad, confidencialidad y autenticidad*** de las transmisiones de datos que circulen por ésta.

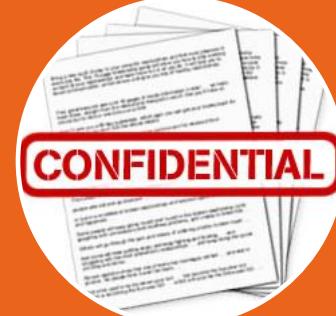




Disponibilidad



Integridad



# CONFIDENCIALIDAD

# DISPONIBILIDAD

# INTEGRIDAD



## ATRIBUTOS DE LA SEGURIDAD

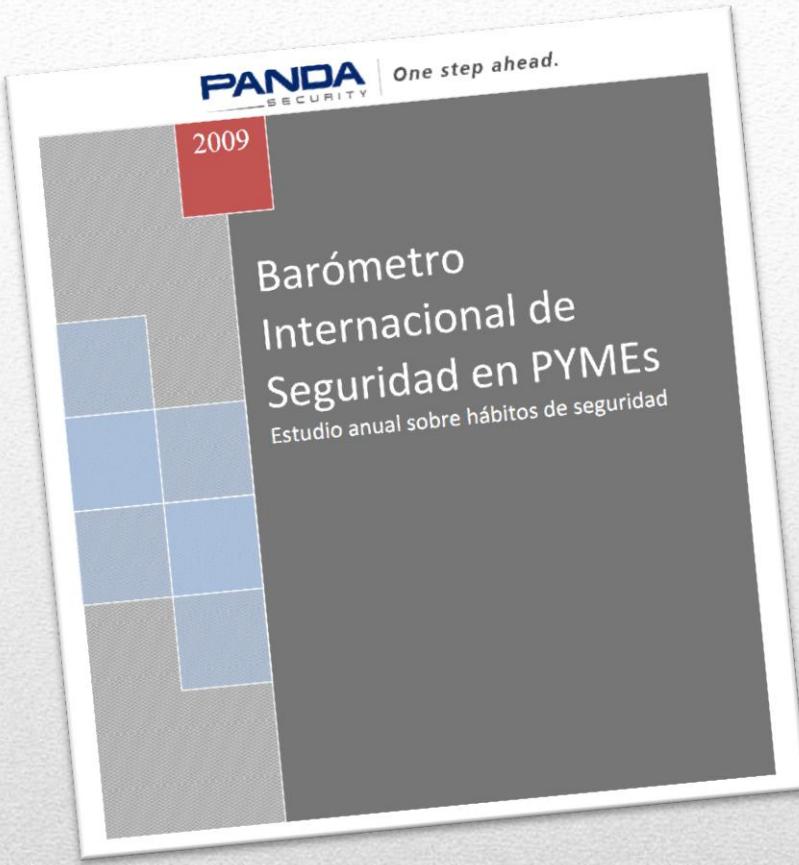
Se refiere a tener la información restringida a aquellos sujetos que no tiene autorización, solo para usuarios definidos por la dirección de la empresa tendrán acceso

Es muy importante que la información de los sistemas esté disponible en cualquier momento que lo necesiten los usuarios designados o procesos autorizados

Para la empresa es muy importante que su información se mantenga sin modificación y que las personas que estén autorizados para hacerlo trabajen bajo estrictas normas de operación

# Importancia de la seguridad en informática en la PYMES

- El uso de las computadoras en las pymes se acerca al 100%, pero **no todas tienen tan claro** que deban dedicar recursos a la seguridad y el mantenimiento de los sistemas informáticos.
- **Ante los riesgos informáticos** las pymes necesitan tomar **precauciones** con el fin de impedir ataques o infecciones externas.
- Según Coelco (Comercio electrónico del conocimiento), un 50% de los delitos a futuro se cometerán por medio de sistemas virtuales (ciberfraudes), **resaltando que un 50% de las pymes nacionales no aplican una política de seguridad informática.**



- Panda Security informó que el 64% de las pymes han reportado incidentes de seguridad.
- Estos incidentes de seguridad han afectado el 47% de su productividad.
- Uno de los motivos de esta situación es no observar los procesos críticos ni detectar la amenaza.

**“Generalmente, las pequeñas y medianas empresas no tienen una visión global sobre la situación de su seguridad.”**

“La falta de recursos provoca, a veces, que muchas PYMES cuenten con una seguridad insuficiente o no sepan exactamente cuáles son las medidas que tienen que adaptar para estar protegidos.”

# Seguridad informática para pymes

## ¿Gasto o inversión?





“...las pequeñas y medianas empresas (PyMES) no invierten en cuestiones de seguridad, "cuando deciden hacerlo es cuando ven un crecimiento en su compañía, pero les cuesta más sí nunca han invertido...”

“...las compañías grandes, medianas y pequeñas que deciden no invertir en seguridad informática **es porque no creen que esa inversión les traiga algún costo-beneficio**, "al contrario lo ven como algo que va hacer efectivo, pero que no les generará muchos beneficios".

# ¿Cuánto invertir en seguridad informática?

- A la hora de calibrar el gasto a realizar en una instalación de seguridad informática hay tres valores que deben ser tenidos en cuenta.
  - Debe conocerse el valor de la información o de los sistemas que deben protegerse.
  - ¿Cuánto vale el “know how” de la compañía?
  - ¿Cuánto vale en este momento el proyecto de un nuevo producto que está todavía en desarrollo?

**¿Cuánto cuesta tener  
parada una hora la red de  
una empresa?**

---

# Paypal....



Una operación de hackers unidos ha realizado un ataque contra uno de los bancos que congeló los fondos de WikiLeaks.

Los hackers desplegaron un ataque de DDOS a PayPal, empresa que canceló la cuenta para donar a WikiLeaks.

*At around 10:30 am PT Monday, a network hardware failure resulted in a service interruption for all PayPal users worldwide...*

The PayPal outage cost its users between 7 and 32 million USD

<http://royal.pingdom.com/2009/08/04/the-paypal-outage-cost-its-users-between-7-and-32-million-usd>

<http://pandalabs.pandasecurity.com/tis-the-season-of-ddos-wikileaks-edition/>

**Operation: Payback**  
irc://irc.anonops.net/operationpayback est. 2010

Target: <https://www.paypal.com/>  
When: In a few hours.

We will fire at anyone or anything that tries to censor WikiLeaks, including multi-Billion dollar companies such as [PayPal](#).

[Twitter](#) you're next for censoring #Wikileaks discussion.  
The major shitstorm has begun.

Set your LOIC HIVE server to [loic.anonops.net](http://loic.anonops.net), channel [#loic](#)

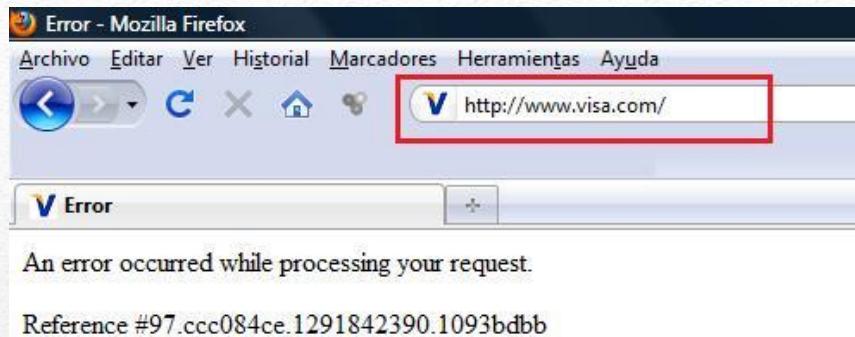
Get on our IRC network!  
<irc://irc.anonops.net/OperationPayback>

<http://www.anonops.net/>



*Overall, the problems lasted approximately 4.5 hours before being fully resolved*

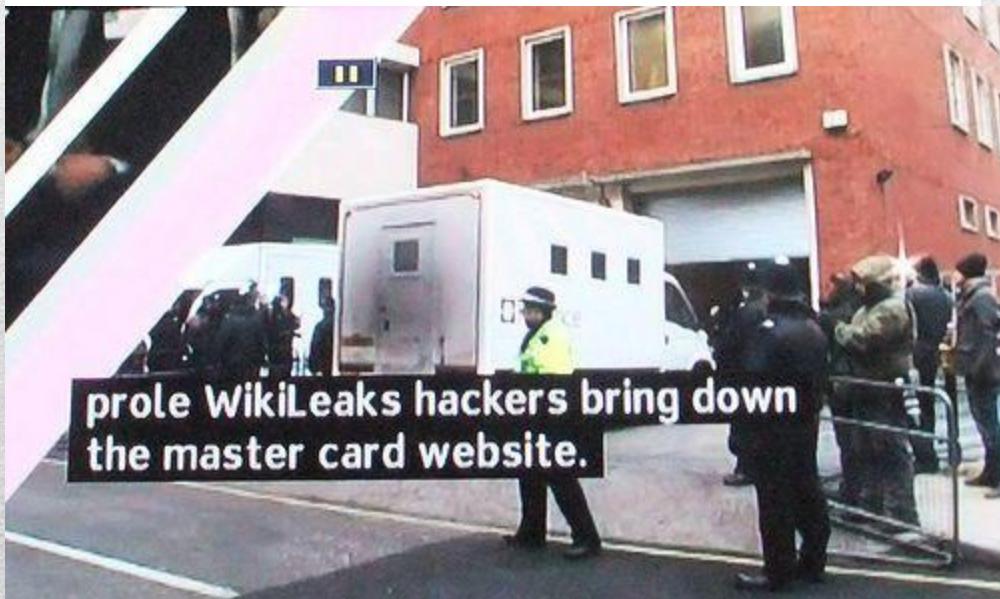
PayPal has stated that the service was completely down, globally, for about one hour.



@AnonyWatcher  
Anonymous

TANGO DOWN - mastercard.com -  
Restricting funds to Julian Assange and  
#Wikileaks. All countries should be down,  
too. #OperationPayback #DDoS

1 hour ago via web ☆ Favorite ↗ Retweet ↗ Reply



Por haberse negado a gestionar las donaciones a WikiLeaks, los sitios web de MasterCard y Visa sufrieron nuevos ataques DoS del grupo Anonymous

# Reacciones



@LBisaTwit  
Lee Barnett

#payback can you stop the DDoS on postfinance for 10 minutes so that I can bank please? pretty please?

11 minutes ago via web ☆ Favorite ⤒ Retweet ⤓ Reply

*'Anonymous' señaló que están contemplando Amazon como próximo blanco de los ataques. Por su parte PayPal señaló a través de su cuenta de Twitter que estaba "funcionando plenamente a pesar de los ataques", que sólo habían conseguido "ralentizar el sitio durante breves períodos".*

# ¿Cuánto invertir en seguridad informática? (cont)

- En ningún caso deberá emplearse una cantidad superior al valor en sí de la información a proteger.
  - Es como intentar guardar un trozo de tela manchada en una caja fuerte, ya que el valor de compra de una caja fuerte es muy superior al de la tela.
  - Ahora, si la tela la manchó un tal Leonardo da Vinci y le puso por título “La Gioconda”, quizá la inversión en medidas de seguridad adicionales merezca la pena.
- Medir el costo que le supondría a un atacante conseguir romper las barreras de seguridad y obtener la información protegida.

# **Pasos para implementar la seguridad informática en su empresa**



# Paso 1: Seguridad física

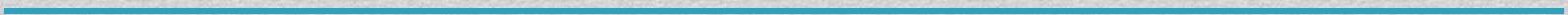
- La Seguridad Física consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial"
- Las principales amenazas que se prevén en la seguridad física son:
  - Desastres naturales, incendios accidentales tormentas e inundaciones.
  - Amenazas ocasionadas por el hombre.
  - Disturbios, sabotajes internos y externos deliberados.

# Paso 1: Seguridad física

- Control de Accesos
  - Utilización de Guardias
  - Utilización de Detectores de Metales
  - Utilización de Sistemas Biométricos
  - Protección Electrónica
  - Alarmas

# Paso 2: Seguridad Lógica

- Seguridad Lógica consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo.“



# Paso 2: Seguridad Lógica

- Restringir el acceso a los programas y archivos.
  - Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
  - Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
  - Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
  - Que la información recibida sea la misma que ha sido transmitida.
  - Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
  - Que se disponga de pasos alternativos de emergencia para la transmisión de información.
-

# Otras sugerencias...

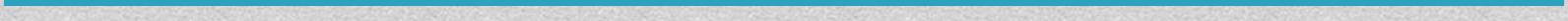
---

# Pasos para proteger su datos

- Mantenga actualizado el software que utiliza.
- Instale un antivirus en los servidores y estaciones de trabajo.
  - Actualícelos todos los días.
  - Existen antivirus gratuitos y las actualizaciones siempre son libres.
- Instale un Firewall de software o hardware.
- Configure los permisos necesarios en cada recurso de su red.
  - Aplique el **principio de menor privilegio** que dicta que si alguien no debe acceder a un recurso, entonces no debe acceder.
- Utilice software legal y obténgalo de sitios confiables.

# Pasos para proteger su datos

- Utilice contraseñas seguras.
  - La mayoría de los ataques apuntan a obtener su contraseña.
  - Si Ud. no utiliza contraseñas o pone su nombre como clave de acceso sólo le hace más fácil el trabajo al atacante.
- No confíe en llamados telefónicos que no pueda identificar.
  - **La Ingeniería Social** es un técnica por la cual personas inescrupulosas obtienen información engañando a su víctima. Los medios utilizados pueden ser fax, mails o llamados telefónicos.



# Pasos para proteger su datos

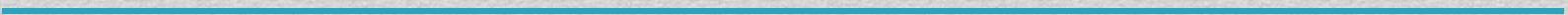
- No instale aplicaciones por defecto. Todas ellas suelen tener **mejores prácticas** que dan la orientación necesaria para brindar un mínimo de seguridad.
- **La tecnología no lo es todo**, por eso tenga en cuenta los lineamientos y políticas existentes.
- Y por último y lo más importante realice copias de seguridad (backup) de forma automática o manual.

# **Microsoft -“9 pasos para implementar la seguridad informática en su empresa”**

- Establecer una política de seguridad de la pyme.
- Proteger los equipos de escritorio y portátiles.
- Proteger la red.
- Proteger los servidores.
- Mantener los datos a salvo.
- Proteger las aplicaciones y los recursos.
- Realizar la gestión de las actualizaciones.
- Proteger los dispositivos móviles.
- Tener protección de datos de carácter personal.

# Políticas de Seguridad

- Surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos.



# Políticas de Seguridad

- Requiere un alto compromiso de la gerencia y la organización.
  - Ser holística (cubrir todos los aspectos relacionados con la misma).
  - Adecuarse a las necesidades y recursos.
  - Definir estrategias y criterios generales a adoptar en distintas funciones y actividades, donde se conocen las alternativas ante circunstancias repetidas.
-

# Políticas de Seguridad: Redes Sociales

- Las redes sociales, como Twitter o Facebook, abren la puerta a nuevas amenazas para los datos corporativos.
- Por ello, las empresas necesitan protegerse adoptando políticas de seguridad.
- El problema es que los empleados, incluso sin malas intenciones, pueden filtrar inadvertidamente información sensible en este tipo de redes.
- Las empresas deben desarrollar estrategias específicas para las redes sociales y que se comuniquen detalladamente a los empleados para satisfacer los objetivos de sus negocios.

# Caso #1- Domino's Pizza



# Domino's YouTube Video: YouTube Can Get You Fired, Too



April 15, 2009 by Stan Schroeder

410

Like

Send

44 people like this.

Ads by Google

[Study in Spain](#) - Earn your hospitality degree from Les Roches Marbella in Spain.

[LesRoches.net](#)

I'm not sure how to approach this subject. There seems to be a rising trend of people doing illegal or harmful things and filming it or taking pictures of themselves, and my initial reaction is to say "don't do it" On the other hand, it's probably good that they're doing it because now they got caught, and the entire world knows of their evil deeds.



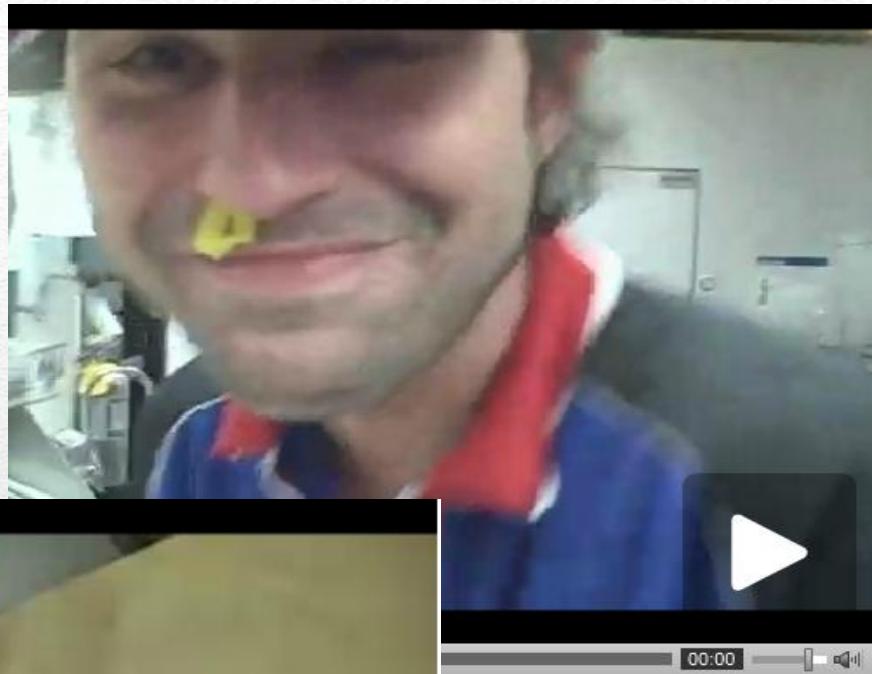
In this particular case, a couple of Domino's employees have filmed themselves doing gross things to food that'll probably get served to customers, and posted it to YouTube. Due to reactions and some quite clever investigative work of appalled viewers, both were promptly fired.

For the rest of us, it sadly shows that these things (hopefully, very rarely) do happen in restaurants. It also shows that, luckily, people who are dumb enough to do something like that are also incapable of understanding that posting something on YouTube means that the entire world can see it. Kudos to that.

If you're not easily grossed out, the offending video is below.



<http://consumerist.com/2009/04/dominoes-rogue-employees-do-disgusting-things-to-the-food-put-it-on-youtube.html#c12066956>



[http://www.goodasyou.org/good\\_as\\_you/2009/04/video-let-the-dominoes-appall.html](http://www.goodasyou.org/good_as_you/2009/04/video-let-the-dominoes-appall.html)



\*\*UPDATE: From Domino's corporate:

Thank you for bringing these to our attention. I don't have the words to say how repulsed I am by this – other than to say that these two individuals do not represent that 125,000 people in 60 countries who work hard every day to make good food and provide great customer service. I've turned this over to our security department. We will find them. There are far too many clues that will allow us to determine their location quite easily.

Regards,

Tim McIntyre

Vice President, Communications

Domino's Pizza, LLC

<http://consumerist.com/2009/04/consumerist-sleuths-track-down-offending-dominos-store.html>

**\*\*UPDATE, 4/14: More from corporate:**

Hi, Jeremy.

We just got off the phone with the franchise owner, who was absolutely dumbfounded by this. He has told us that he will be terminating their employment effective immediately. We suggested that he call them and get a written statement from them, asking them to "explain" (to the extent anyone can, really) their actions. We are also seeking legal counsel to see what kind of action we can take against them for damage to the brand.

You are welcome to use anything I've sent to you in the past 24 hours. I do want to thank you for bringing this to our attention...I just wish it hadn't been posted so prominently on your web site...while it was certainly fair game, it does hurt the company and the thousands of people we employ in this country whether it's intended or not.

Regards,

Tim

Tim McIntyre  
Vice President, Communications  
Domino's Pizza, LLC

We respond:

<http://consumerist.com/2009/04/consumerist-sleuths-track-down-offending-dominos-store.html>

**With 65% of respondents in a follow up study indicating that they were less likely to order from Domino's after the release of the video, Domino's sales suffered.**

## Domino's loses 10% of its value in one week

[social media case studies](#)

[social media risk](#)

15 March 2010 | 1 Comment



Tweet

2



Like



Be the first of your friends to like this.

### Overview

As a prank, two Domino's employees engaged in several health department violations, re-corded their activities and posted them to YouTube. The videos quickly "went viral" and consumers all over the web were exposed to Domino's employees doing a variety of unseemly things to their pizza.



**Domino's stock price dropped 10% over the week costing shareholders millions.**

# Lecciones aprendidas

- **Respuesta Rápida-**
    - atendiendo y monitoreando lo que pasa en las redes sociales acerca del negocio.
  - **Atender todos los canales disponibles-**
    - no asumir que solo fue a través de un solo canal (YouTube) y no se iba a difundir a otros medios sociales.
  - **Tener una política de uso de las redes sociales**
-

# Video

## Domino's employees face criminal charges



<http://www.youtube.com/watch?v=eYmFQjszaec>

# Domino's Pizza Reborn

Domino's® Pizza Turnaround

dominosvids

34 videos

Subscribe



# Preguntas



Dra. Aury M. Curbelo

[aury.curbelo@upr.edu](mailto:aury.curbelo@upr.edu)

787-202-8643

<http://digetech.net>

---