

12 MARZO 2021

II CONGRESO DE  
SEGURIDAD DE LA  
INFORMACIÓN Y  
CIBERSEGURIDAD

# “Desafíos de la seguridad en la nube”



**Speaker:**

Jorge Andres Flores Zepeda

**Linkedin**

[linkedin.com/in/jorgeandresfloreszepeda](https://www.linkedin.com/in/jorgeandresfloreszepeda)

SOCHISI.CL/ENVIVO





**Hablemos de  
la nube y sus  
desafíos en  
cuanto a  
seguridad...**

**Todos  
sabemos de la  
nube, no es  
cierto?**



# Sobre todo sabemos sus ventajas

Generales y casi generales

## En términos generales

- Calidad de la seguridad
- Cumplimiento de regulaciones
- Inmortalidad del storage
- Down time mínimo
- Escalabilidad

## Y en casi todas las situaciones

- Costo
- Disponibilidad de soluciones



# Todos parecieran pensar que es mas seguro...

Pero es así?

## Fifty-seven percent believe the cloud offers better data security

Source: Cisco 2018 Security Capabilities Benchmark Study



For more info visit: [cisco.com/go/acr2018](https://cisco.com/go/acr2018)



# A favor podemos decir...



## Aislamiento de VMs

Una máquina virtual es un entorno aislado con acceso a un subconjunto de recursos físicos del sistema informático. Cada VM parece estar ejecutándose en el hardware básico, dando la apariencia de múltiples instancias de la misma computadora, aunque todas son compatibles con un solo sistema físico.

## Ataque de Hypervisor

Un hipervisor (en inglés hypervisor) o monitor de máquina virtual (virtual machine monitor) es una capa de software para realizar una virtualización de hardware que permite utilizar, al mismo tiempo, diferentes sistemas operativos (sin modificar o modificados, en el caso de paravirtualización) en una misma computadora

## Infraestructura Virtual

La infraestructura virtual es una colección de componentes definidos por software que conforman un entorno de TI empresarial. Una infraestructura virtual proporciona las mismas capacidades de TI que los recursos físicos, pero con software, de modo que los equipos de TI pueden asignar estos recursos virtuales rápidamente y en múltiples sistemas, según las distintas necesidades de la empresa.

## Recuperación

Es muy posible y natural poner parte o el total del ambiente en cuarentena y recuperarnos rápidamente de incidentes.





**Pero  
todavía  
algunas  
cosas  
pueden  
fallar**



# Los desastres mas comunes, siguen siendo comunes en la NUBE



**Data  
Breach**



**Data  
Loss**



**Toma de Control de  
Cuentas**



**Interfaces  
API/Inseguras**



**DDoS**



**El  
problema  
del “agente  
interno”**



**Abuso de recursos  
compartidos**







# Hay un GAP entre ON- PREMISE y CLOUD Security

## Mas segura, pero mas inmadura

Mientras que el 75% de los profesionales de TI ven la nube pública como más segura que sus propios centros de datos, el 92% también siente que su inmadurez en sus programas de seguridad en la nube está creando una brecha de preparación.

## Y aquí vamos con la responsabilidad compartida...

Un número cada vez mayor de empresas están identificando su propia falta de conocimiento de responsabilidad compartida en la protección de la nube, como una causa clave para las configuraciones y lagunas erróneas frecuentes y este malentendido va hasta la cima con sólo el 8% de los líderes cibernéticos que entienden completamente el papel de su equipo en asegurar la nube frente al proveedor de servicios en la nube.







**Cuando las organizaciones hablan  
anónimamente... 59% dice que sus  
credenciales han sido robadas y 76% dicen que  
han perdido datos**

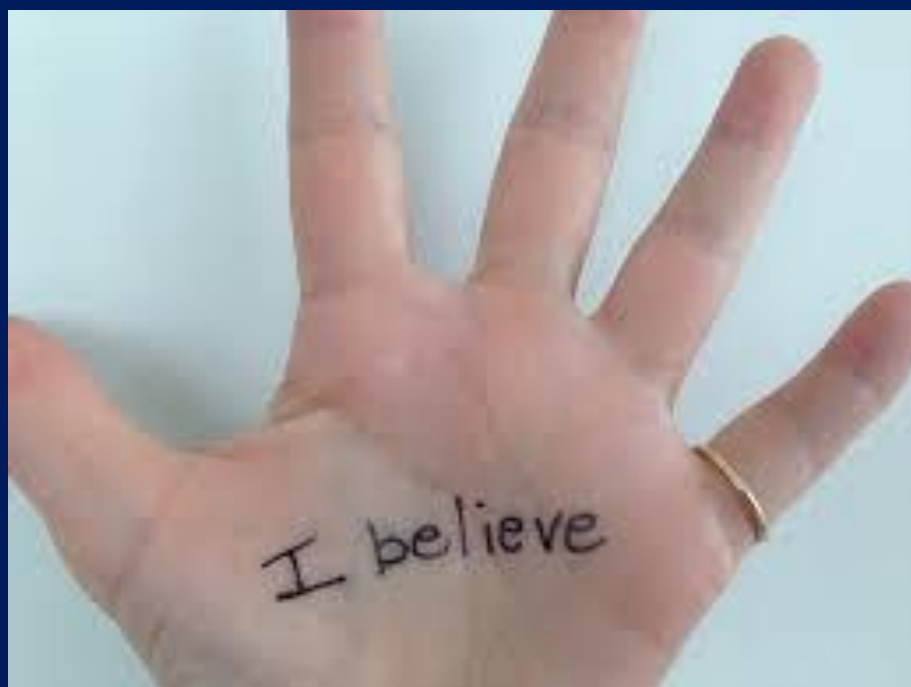
Es decir... los BREACH se ocultan... que  
novedad!



# Y aparecen cosas relativamente nuevas

## Cloudjacking y Cryptojacking





**El uso de servicios en la nube parece un poco arriesgado. Sin embargo, si se siguen las medidas de seguridad adecuadas, la nube puede ser más segura que un centro de datos tradicional.**

Yo sigo pensando...



# Para prepararnos

Debemos preguntarnos

Como llega el desastre





# Cuando ponemos la tecnología en manos de la gente – Origen “Operacional”



<https://www.wral.com/-oh-my-gosh-raleigh-woman-s-snow-photo-goes-viral/13390109/>

North Carolina – 2 kilómetros de desastre - 2014

SOCHISI.CL/ENVIVO





**No podemos  
cubrirlo todo  
inmediatamente,  
pero podemos  
partir por lo que  
esta al alcance**





# La cadena de sucesos

## Por separado o “todo revuelto”

### TOP RISKS

**VM Sprawl**



**Datos  
sensitivos  
en una VM**



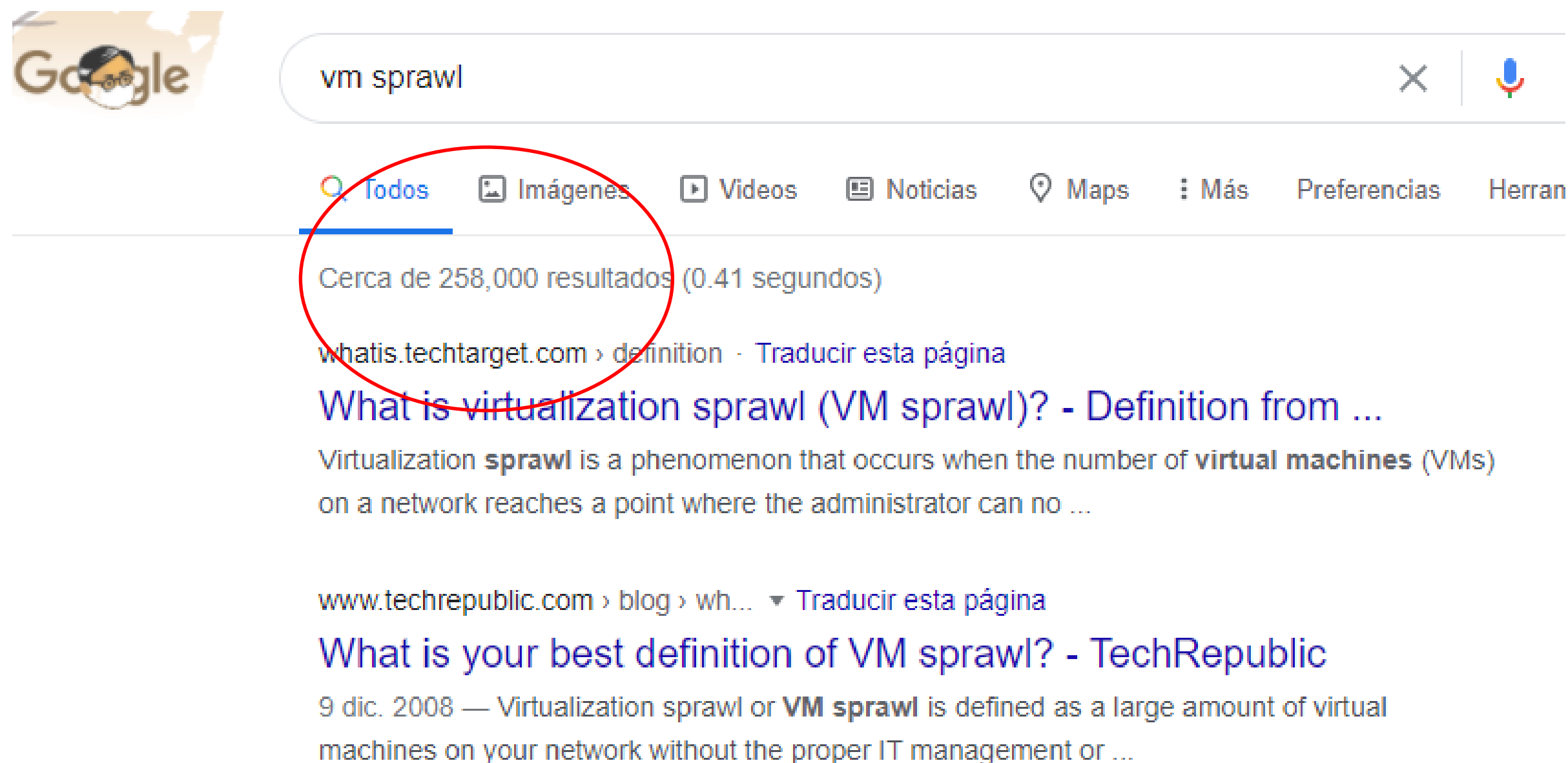
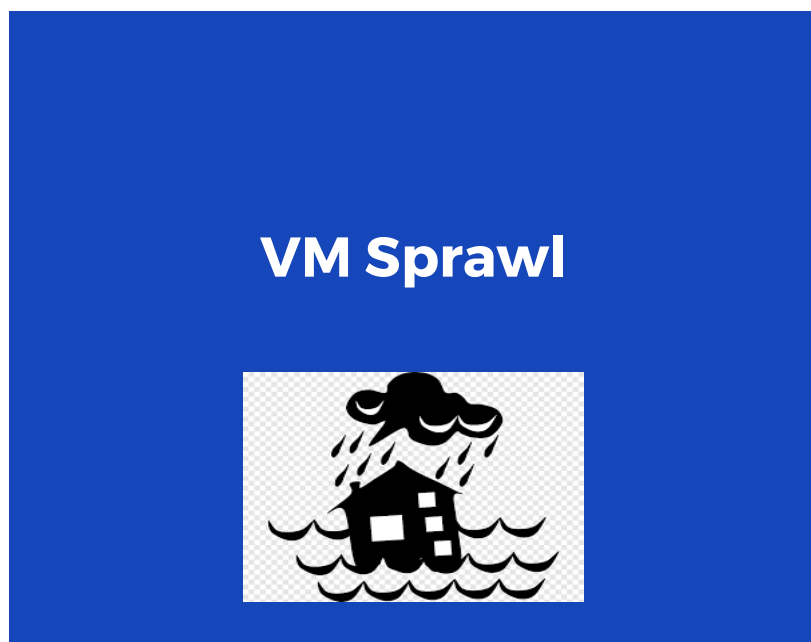
**Seguridad OFFLINE y  
VM “durmiendo”**



**Golden Images  
“comprometidas”**



# El VM Sprawl es tan popular que...





# TOP RISKS

VM Sprawl



Datos  
sensitivos  
en una VM



Seguridad OFFLINE y  
VM “durmiendo”



Golden Images  
“comprometidas”



- *Certificados expuestos en las maquinas virtuales – Usar herramientas adecuadas*
- *Mucha información personal innecesariamente colocada – Compartimentar/Borrar/Higiene*

# TOP RISKS

## VM Sprawl



## Datos sensitivos en una VM



## Seguridad OFFLINE y VM “durmiendo”



## Golden Images “comprometidas”



- *Maquinas durmiendo no son actualizadas – Actualizar y parchar todo*
- *Viejas imágenes siguen activas – Actualizar o inactivar*

# Cuando perdemos control... y el riesgo se hace realidad

**Perdida de visibilidad de la infraestructura**



**Se agotan los recursos**



**Seguridad del Hypervisor**





# Cuando perdemos control... y el riesgo se hace realidad

**Perdida de visibilidad de la infraestructura**



**Se agotan los recursos**



**Seguridad del Hypervisor**



- *La infraestructura se vuelve invisible para las herramientas tradicionales - Revisar que las antiguas herramientas aun sirvan/Cambiarlas*
- *Encriptar todo el trafico*

# Cuando perdemos control... y el riesgo se hace realidad



- *Acceso a recursos por parte de infraestructura virtual puede generar decaimiento – Scaling y Sobre-Aprovisionar*
- *DDoS pueden ser visible por agotamiento de servicios – Enfatizar el monitoreo*



# Cuando perdemos control... y el riesgo se hace realidad

Perdida de visibilidad de la infraestructura



Se agotan los recursos



Seguridad del Hypervisor



- Si es que es parte de nuestra responsabilidad: Parchar / **“Provenance”**

# O tenemos sensación de vértigo...

**Accesos no permitidos**



**Signos de  
perdida de  
control en  
los portales**



**Efectos en el  
WorkLoad**



# O tenemos sensación de vértigo...



- *Una llave para muchas credenciales / Cambiar la filosofía, entrenar a los usuarios*
- *Evitar el “la misma que en google” **nightmare***



# O tenemos sensación de vértigo...



- *Portales no mas seguros que una pagina WEB, escalan en fuentes de intrusión – Profundizar la seguridad*
- ***Securitizar la WEB en su Arquitectura y Programación.***

# O tenemos sensación de vértigo...

Accesos no permitidos



Signos de  
perdida de  
control en  
los portales



Efectos en el  
WorkLoad



- *Iguals servidores o medidas de seguridad en ambientes muy distintos (producción y marketing por ejemplo) – Segmentar el **workload**, trabajar seguridades distintas.*

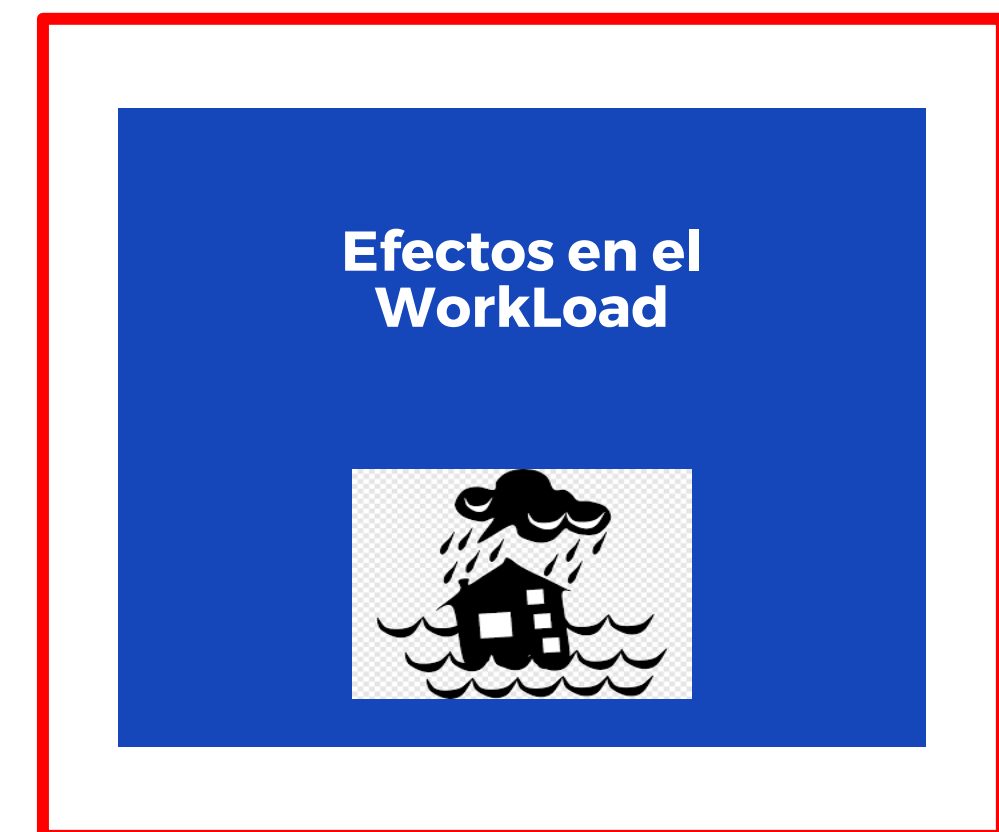
**Forbes**

Jan 3, 2018, 05:12pm EST

# Massive Intel Vulnerabilities Just Landed -- And Every PC User On The Planet May Need To Update

 **Thomas Brewster** Forbes Staff   
Cybersecurity  
Associate editor at Forbes, covering cybercrime, privacy, security and surveillance.

 This article is more than 3 years old.

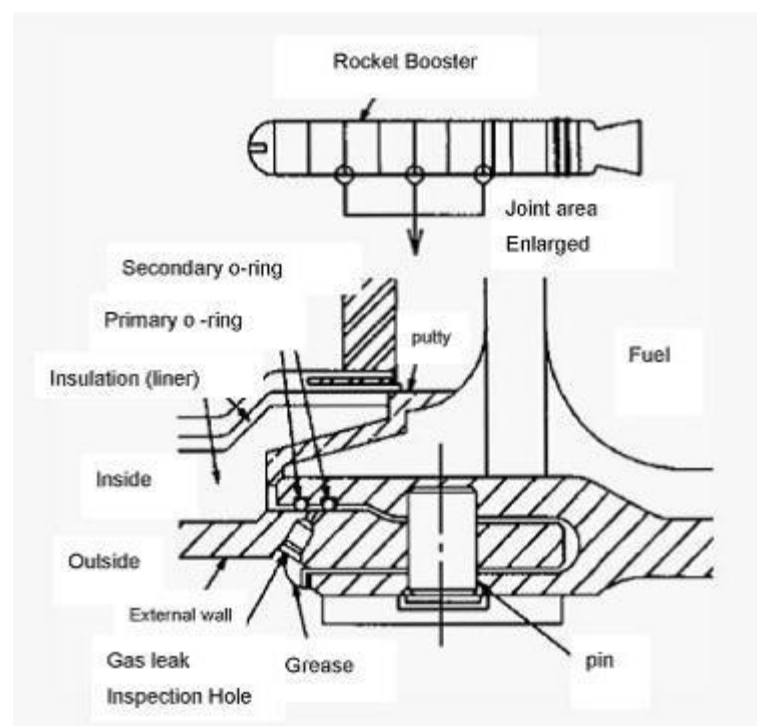



- *Iguals servidores o medidas de seguridad en ambientes muy distintos (producción y marketing por ejemplo) – Segmentar el **workload**, trabajar seguridades distintas.*





# Cuando el error es de principios o “management subyacente”



<https://www.history.com/topics/1980s/challenger-disaster>

Explosión del Challenger - 1984





## TOP errores de Filosofía o Management




**Responsabilidad...**  
**(lo hablaremos++)**



**Entrenamiento**



**Automatizacion**



**Cumplimiento**



**Liderazgo**





# O, es un tema de arquitectura



[https://en.wikipedia.org/wiki/Collapse\\_of\\_Lotus\\_Riverside\\_Block\\_7](https://en.wikipedia.org/wiki/Collapse_of_Lotus_Riverside_Block_7)

Lotus Riverside - SHANGAI - 2009



Si pensáramos en nuestro hogar...



### **Problema 1 – Nunca terminamos de migrar - Realmente**

Fuimos híbridos por mucho tiempo, no nos adaptamos, tuvimos que mantener por mucho tiempo ambos ambientes



### **Problema 2 – Nos cambiamos de casa, pero mantuvimos los muebles**

Mantuvimos las mismas reglas y herramientas ON PREMISE

Si pensáramos en nuestro hogar...



**Problema 3 – Nos gusto tanto la sala de estar que pusimos allí los dormitorios...**

No establecimos ambientes separados y dejamos todo en la misma red con las mismas protecciones



**Problema 4 – Se nos ocurrió pintar la casa... cuando ya estábamos viviendo en ella**

No aplicamos parches, correcciones de seguridad, hasta que ya teníamos los ambientes en productivo





# Basta de Penas! Como nos preparamos?





# Mas que largas recetas...

Conceptos Claves

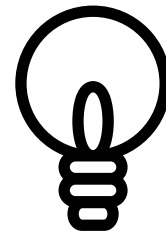


## Responsabilidad y Recursos

Una vez mas...

---

---



## Mirada de Infraestructura

Una mirada holística de nuestra  
plataforma

---

---



## No perder de vista a los seres humanos

Siempre se reduce a eso

---

---

# Mas que largas recetas...

Conceptos Claves



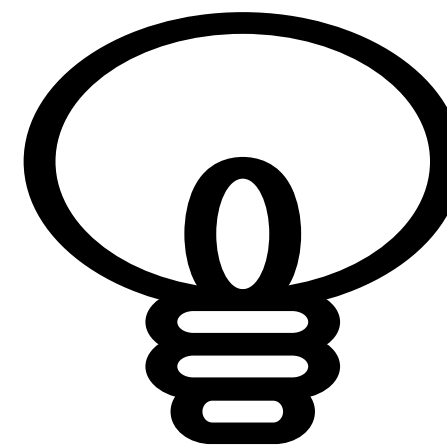
**No perder de vista a los seres humanos**

Siempre se reduce a eso



# Y como cualquier auditor diría...

Es un tema de RISK MANAGEMENT



**Winston Churchill y Dwight D. Eisenhower tenían ideas similares**

Churchill decía, “**Los planes son de poca importancia, pero planificar es esencial**”, mientras Eisenhower decía, “**Los planes no sirven para nada, pero planificar es todo**” Eisenhower iba mas allá diciendo “...La definición de ‘Emergencia’ es aquello que es inesperado, de manera tal de que lo que lo que estabas esperando no ocurrirá.”

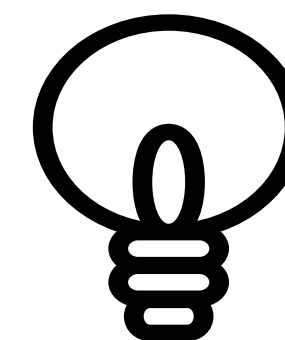
*No se puede evitar el riesgo, pero se puede planificar*





# Y si te vas a caer...

CAE CON GRACIA



Planea para que tu seguridad  
falle, luego planea para que una  
vez que falle, se recupere bien...  
luego falla amablemente



12 MARZO 2021

# ¡Muchas Gracias!

Desafíos de la seguridad en la Nube

**Speaker:**

Jorge Andres Flores Zepeda

**Linkedin**

[linkedin.com/in/jorgeandresfloreszepeda](https://www.linkedin.com/in/jorgeandresfloreszepeda)

**II CONGRESO DE  
SEGURIDAD DE LA  
INFORMACIÓN Y  
CIBERSEGURIDAD**



**SOCHISI**

DIGITAL SECURITY  
THINK TANK

SOCHISI.CL/ENVIVO



# Y los espero en...

<https://diplomadociberseguridad.com/>

## Arquitecto Cloud



Recuerde revisar aquí el calendario para el detalle de los horarios. A continuación encuentra los ciclos en los que se realizará este curso:

Ciclo 2 15 de Marzo al 24 de Abril 2021	Ciclo 4 05 de Julio al 7 de Agosto 2021	Ciclo 6 25 de Octubre al 4 de Diciembre 2021
--	--	---

## Seguridad en la Nube



Recuerde revisar aquí el calendario para el detalle de los horarios. A continuación encuentra los ciclos en los que se realizará este curso:

Ciclo 3 10 de Mayo al 12 de Junio 2021	Ciclo 5 23 de Agosto al 2 de Octubre 2021	Ciclo 7 10 de Enero al 12 de Febrero 2022
---	--	--