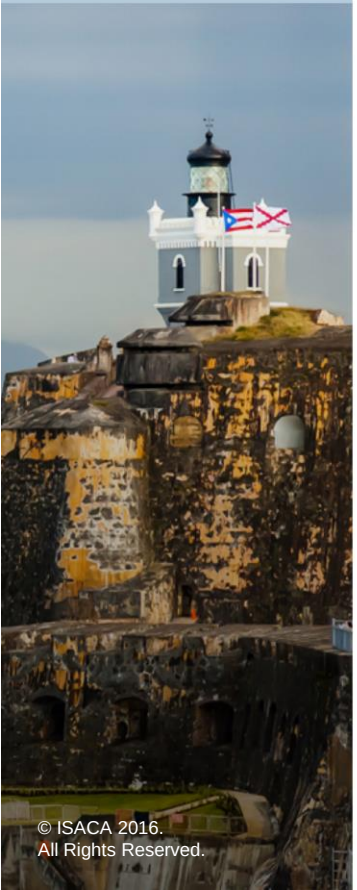
2016 LATIN CACS™
AN ISACA EVENT

La Muerte del Password

Luciano Johnson, MSc, MBA, CISM, CRISC
Cyber Security Director



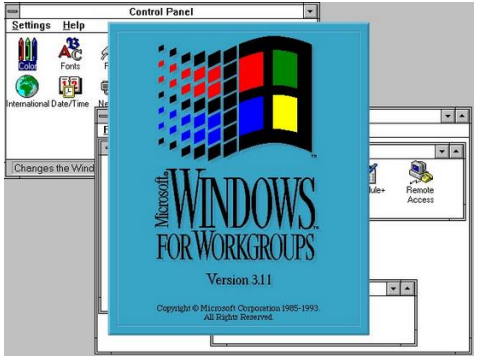
Agenda

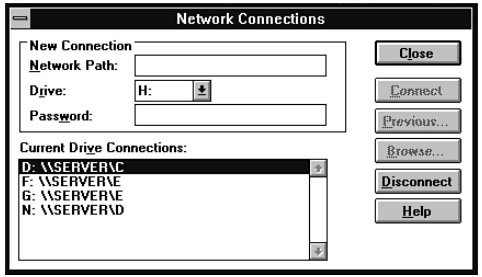
- Contraseña: del cielo al infierno
- Gestión de Riesgos de la contraseña
- Más seguridad a las aplicaciones y usuarios
- Autenticación: nuevas estrategias

© ISACA 2016.
All Rights Reserved.

Contraseña: del cielo al infierno

- ¿Por que empezamos a utilizar contraseñas?
  - La aparición de las redes informáticas
  - Los recursos compartidos (documentos, impresoras)

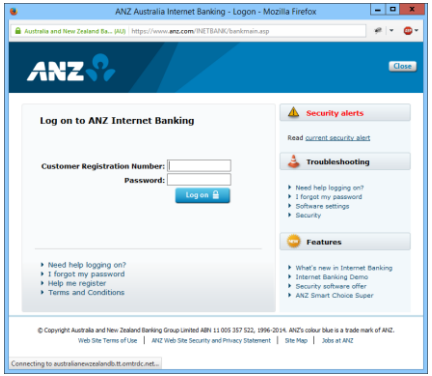




© ISACA 2016.
All Rights Reserved.

Contraseña: del cielo al infierno

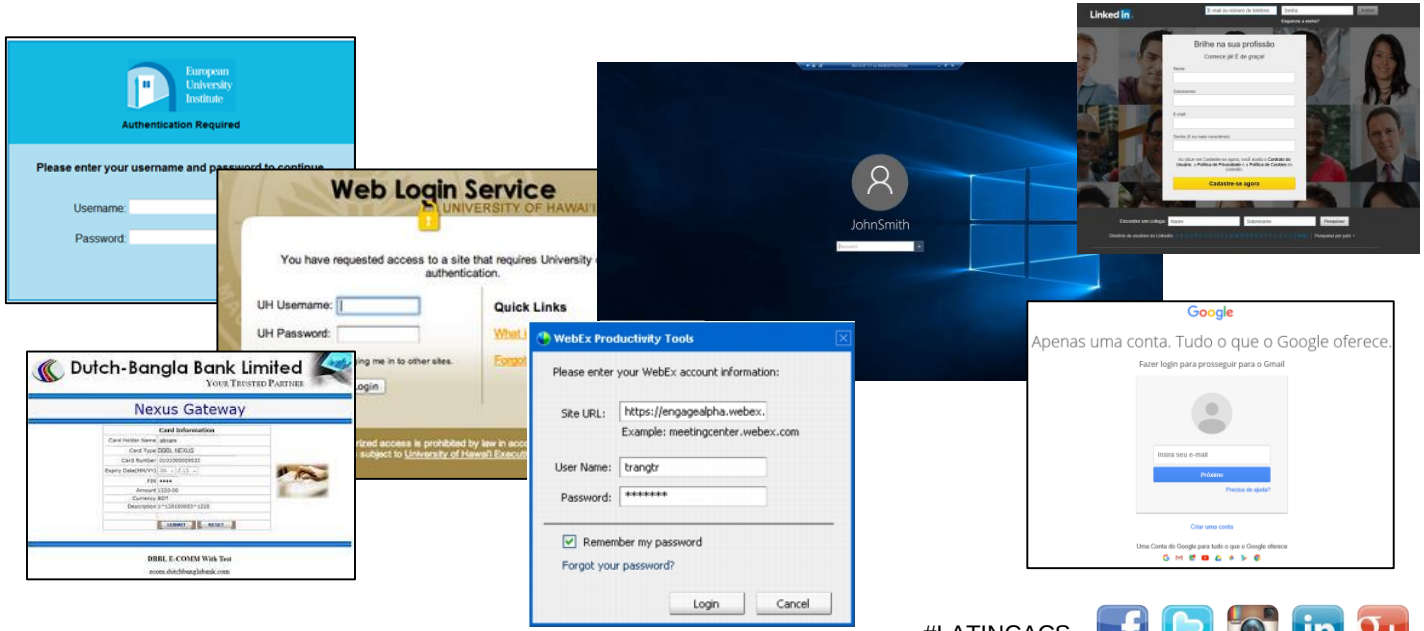
- ¿Por que empezamos a utilizar contraseñas?
  - Personalizar el acceso a los servicios compartidos
  - Proteger la información personal



© ISACA 2016.
All Rights Reserved.

Contraseña: del cielo al infierno

- Problemas con el uso de contraseñas!
  - El exceso de contraseñas para demasiados servicios



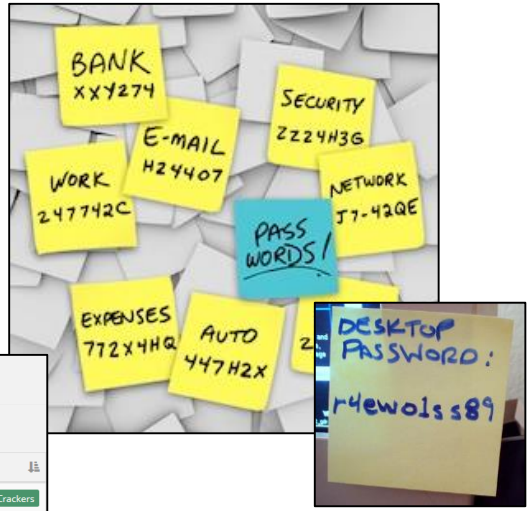
#LATINCACS

ISACAHQ @ISACANews @ISACANews ISACA +ISACA

© ISACA 2016.
All Rights Reserved.

Contraseña: del cielo al infierno

- Problemas con el uso de contraseñas!
  - Falta cultura del usuario
  - Fácil de descifrar contraseñas
  - Ataques de fuerza bruta



THE 25 MOST USED PASSWORDS

password	12345	letmein	michael	2000
123456	dragon	monkey	shadow	jordan
12345678	pussy	696969	master	superm
1234	baseball	abc123	jennifer	harley
qwerty	football	mustang	111111	123456

Hacker Tools > Password Crackers

Show 10 entries

Name of Hacking Tool Name	
Aircrack	Password Crackers
Crowbar	Password Crackers
John the Ripper	Password Crackers
L0phtCrack	Password Crackers
Medusa	Password Crackers

© ISACA 2016.
All Rights Reserved.

Contraseña: del cielo al infierno

- Problemas conocidos de las contraseñas!
  - Sistemas / redes hackeado
  - Fraudes
  - Las fugas de información privada

© ISACA 2016.
All Rights Reserved.

Contraseña: del cielo al infierno

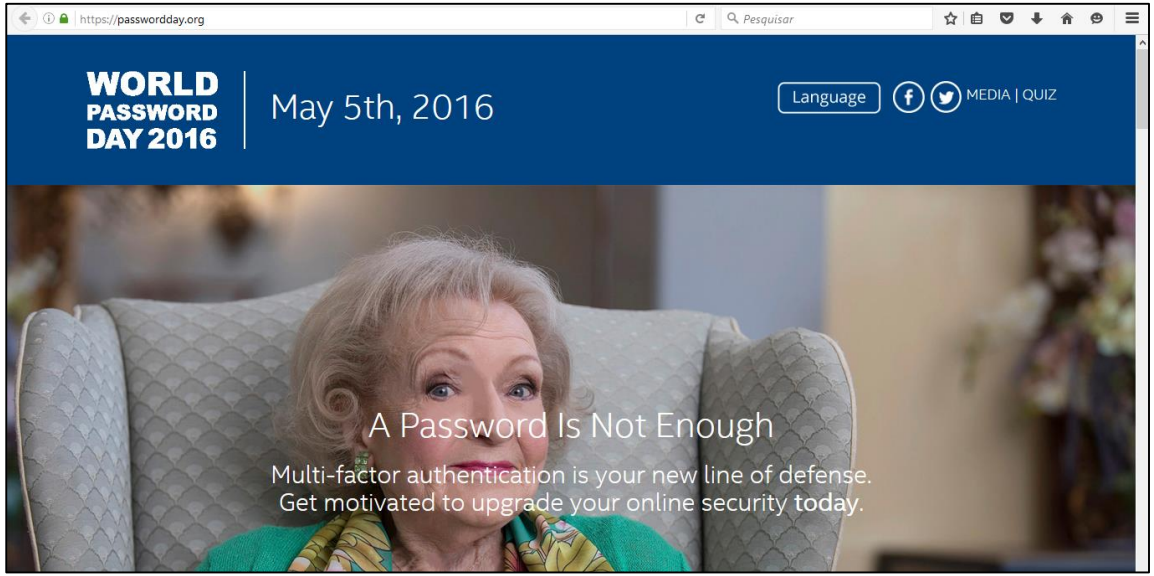
Los usuarios privilegiados

- Problemas conocidos de las contraseñas!
  - **Home Depot**
    - 109 millones de registros (56 millones de tarjetas de crédito / débito y 53 millones de direcciones de correo electrónico del cliente)
    - acceso inicial a la red a través credenciales robadas de un proveedor de terceros
  - **Anthem**
    - 80 millones de registros (datos personales)
    - Acceso a la base de datos a través de robo de al menos cinco credenciales de empleados
  - **Ashley Madison**
    - Más de 30 millones de registros (datos personales)
    - El código fuente revela credenciales no modificables (fichas de AWS, contraseñas de bases de datos, claves SSH)

© ISACA 2016.
All Rights Reserved.

Contraseña: del cielo al infierno

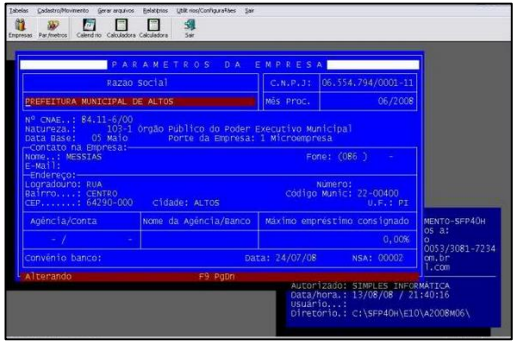
La Muerte de la Contraseña



© ISACA 2016.
All Rights Reserved.

Gestión de Riesgos de la contraseña

- Los sistemas con contraseñas débiles
  - Sistemas heredados
  - Los sistemas con autenticación propia



© ISACA 2016.
All Rights Reserved.

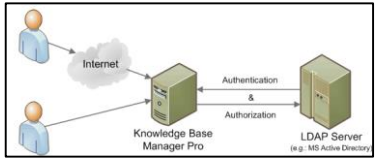
Gestión de Riesgos de la contraseña

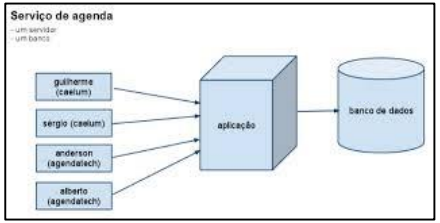
- La construcción de su matriz de contraseñas
  - Método de autentificación
  - Almacén de contraseña
  - La comunicación cifrada
  - Recordatorio de contraseña
  - Captcha
  - Directiva de contraseña
    - Caracteres #
    - Tipo de caracteres
    - La vida de la contraseña
    - Historial de contraseña
    - Bloqueo de contraseña

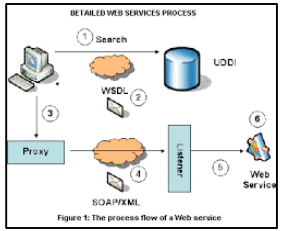
© ISACA 2016.
All Rights Reserved.

Gestión de Riesgos de la contraseña

- La construcción de su matriz de contraseñas
  - Método de autentificación
    - LDAP (MS-AD...)
    - Servicios web
    - Procedimientos almacenados
    - Autenticación propia







© ISACA 2016.
All Rights Reserved.

Gestión de Riesgos de la contraseña

- La construcción de su matriz de contraseñas
  - Almacén de contraseña
    - Texto sin formato
    - Cifrado de dos vías
    - Cifrado unidireccional (HASH)

```
select login, password from user;
---------------------------------
LOGIN                    PASSWORD
jsilva                   123456
mcarvil                  Havalom56
ahertx                   %TCO#2015
pgrandson                **9090**
```

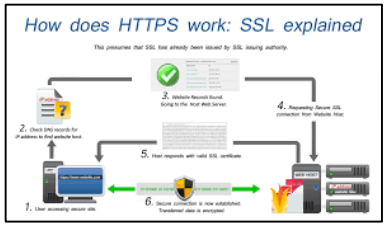
```
select login, password from user;
---------------------------------
LOGIN                    PASSWORD
jsilva                   LKnu87%*r4#ee#dbhjgj
mcarvil                  JiyugF54JU#WW*()34FF$#vJTfY*
ahertx                   XWE@53F%4bhffdxHTGjbjh
pgrandson                Bjhgg$f$76tV
```

```
select login, password from user;
---------------------------------
LOGIN                    PASSWORD
jsilva                   KbvD%434Fyyg¨%tg%$fg897
mcarvil                  WefHUgv%4396%gg&5fJTfY*
ahertx                   BvjY85VCTd%d#4dHJohfi&*
pgrandson                Mbijg%804fHiybf$yGGGy*7
```

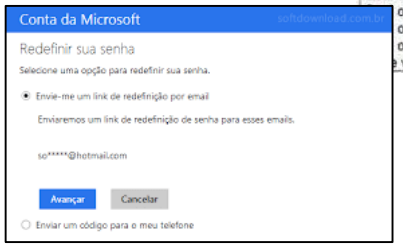
© ISACA 2016.
All Rights Reserved.

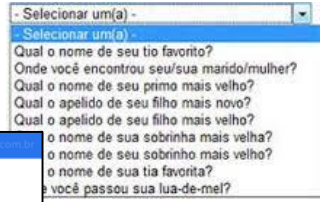
Gestión de Riesgos de la contraseña

- La construcción de su matriz de contraseña
  - La comunicación cifrada
    - HTTPS/SSL
    - HTTP



  - Recordatorio de contraseña
    - preguntas y respuestas
    - Email
    - Recordatorio con la contraseña





© ISACA 2016.
All Rights Reserved.

Gestión de Riesgos de la contraseña

- La construcción de su matriz de contraseñas
  - Captcha
    - Prueba pública completamente automática de Turing para diferenciar entre computadoras y humanos. (Completely Automated Public Turing test to tell Computers and Humans Apart)

© ISACA 2016.
All Rights Reserved.

Gestión de Riesgos de la contraseña

- La construcción de su matriz de contraseñas
  - Directiva de contraseñas
    - # Caracteres
      - Al menos 3
      - Al menos 8
      - Al menos 12

```
password: 123
password: X7Y%

password: 12345678
password: Mt%%fA4d

password: 123456789012
password: Kmd22y69s201
```

```
password: 123456
password: navidad
password: 25year10
password: #25%year*10
password: Year#25*D10
```

- Tipos de caracteres
  - Numérico
  - Alfabético
  - Alfanumérico
  - Los caracteres alfanuméricos + especiales
  - caracteres especiales + alfa-numérico + mayúsculas y minúsculas

© ISACA 2016.
All Rights Reserved.

Gestión de Riesgos de la contraseña

- La construcción de su matriz de contraseñas
  - La vida de la contraseña
    - indefinido
    - 120 días
    - 90 días
    - 45 días

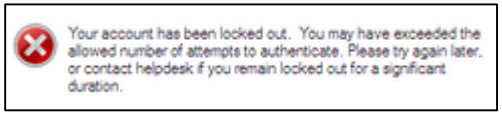
  - Historial de contraseña
    - indefinido
    - Últimos 3 contraseñas
    - Últimos 6 contraseñas

```
select * from auth_user where login = 'jsilva';
-----------------------------------------------
LOGIN   PASSWORD
jsilva  %Mac78Ta4

select * from auth_user where login = 'jsilva';
-----------------------------------------------
LOGIN   PASSWORD        PASSW1          PASSW2
jsilva  %Mac78Ta4       Alfa%89##       M4f4%IOw

select * from auth_user where login = 'jsilva';
-----------------------------------------------
LOGIN   PASSWORD        PASSW1          PASSW2          PASSW3          PASSW4
jsilva  %Mac78Ta4       Alfa%89##       M4f4%IOw        Tab3bU14        Log$meIN
```

  - Bloqueo de contraseña
    - indefinido
    - 5 intentos
    - 3 intentos



© ISACA 2016.
All Rights Reserved.

Gestión de Riesgos de la contraseña

- Matriz, Peso e Puntuaciones

System	authentication	store	crypto channel	passwd reminder	captcha	characters #	characters type	end of life	history	lock	General Score
App 1											
App 2											
App 3											
App 4											
App 5											

item	weight
authentication	4
store	6
crypto channel	3
passwd reminder	2
captcha	4
characters #	4
characters type	4
end of life	3
history	2
lock	3

© ISACA 2016.
All Rights Reserved.

Gestión de Riesgos de la contraseña

- Matriz, Peso e Puntuaciones

	Authentitation	Score
A	LDAP	10
B	WebServices	8
C	Stored Procedures	5
D	Local	2

	Store	Score
A	Crypto 1 way (hash)	10
B	Crypto 2 way	6
C	Plain Text	1

	Crypto Channel	Score
A	HTTPS/SSL	10
B	HTTP	3

	Passwd Reminder	Score
A	Passwd Reset	10
B	Q & A	6
C	E-mail	1

	Captcha	Score
A	Yes	10
B	No	1

	characters #	Score
A	# 12	10
B	# 8	6
C	# 3	1

	characters type	Score
A	AN+special+CaSe	10
B	AN+special	8
C	alpha-numeric	4
D	alphabetic	2
E	numeric	1

	End of Life	Score
A	45 dd	10
B	90 dd	8
C	120 dd	5
D	never	2

	History	Score
A	last 6	10
B	last 3	6
C	never	1

	Lock	Score
A	3x	10
B	5x	6
C	never	1

© ISACA 2016.
All Rights Reserved.

Gestión de Riesgos de la contraseña

- Matriz - Promedio Ponderado

$$\text{Puntuación general} = \frac{(\text{Peso Item1 x Item1 Score}) + (\text{Peso Item2 x Item1 Score}) + \ldots + (\text{Peso Item10 x Item Score})}{(\text{Peso Item1} + \text{Peso Item2} + \ldots + \text{Peso Item10})}$$

- Ejemplo

System	authentication	store	crypto channel	passwd reminder	captcha	characters #	characters type	end of life	history	lock	General Score
App 1	A	A	A	C	B	A	A	B	B	A	8,0571
App 2	B	B	A	A	A	B	B	C	C	B	7,1143
App 3	C	B	A	C	B	C	B	C	C	B	4,6571
App 4	D	C	B	B	B	B	C	C	C	C	2,8286
App 5	A	A	A	C	A	A	A	B	B	A	9,0857

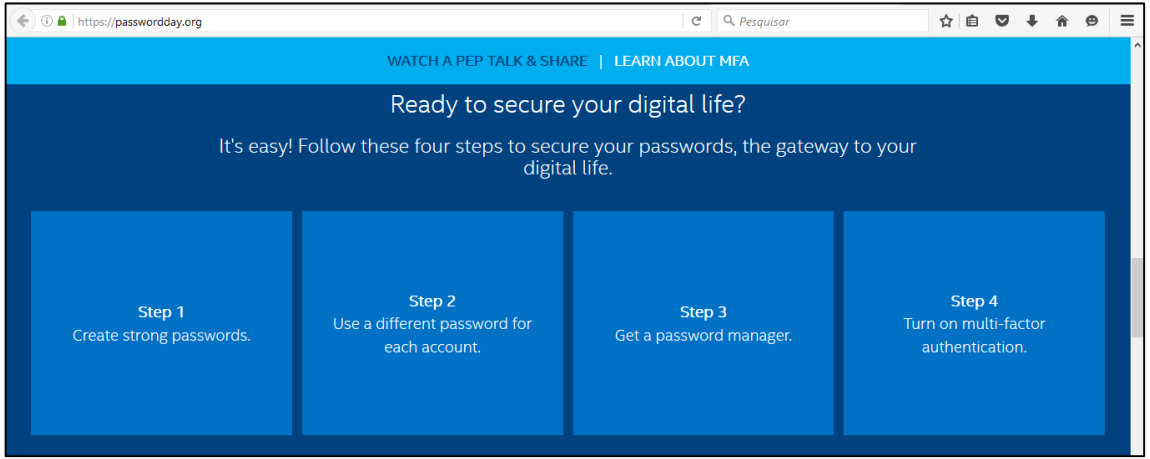
System	General Score
App 5	9,0857
App 1	8,0571
App 2	7,1143
App 3	4,6571
App 4	2,8286

System	General Score
App 5	9,0857
App 1	8,0571
App 2	7,1143
App 3	4,6571
App 4	2,8286

© ISACA 2016.
All Rights Reserved.

Más seguridad a las aplicaciones y usuarios

- La mejora de la identificación y autenticación
  - ¿Qué **sabes**?: los inicios de sesión y contraseñas



© ISACA 2016.
All Rights Reserved.

Más seguridad a las aplicaciones y usuarios

- La mejora de la identificación y autenticación
  - ¿Qué **tienes**?: tokens y tarjetas

© ISACA 2016.
All Rights Reserved.

Más seguridad a las aplicaciones y usuarios

- La mejora de la identificación y autenticación
  - ¿Qué **son**?: biometría

© ISACA 2016.
All Rights Reserved.

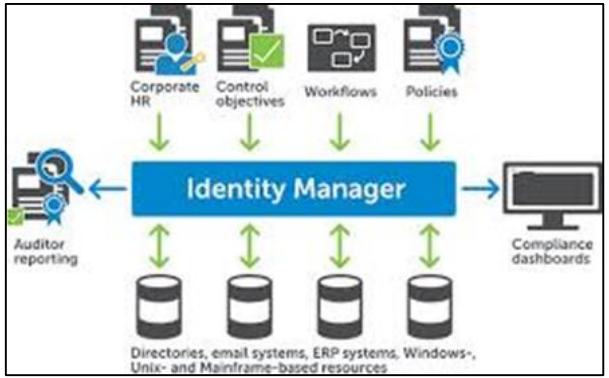
Más seguridad a las aplicaciones y usuarios

- La mejora de la identificación y autenticación
  - ¿Es este nuestro futuro?

© ISACA 2016.
All Rights Reserved.

Más seguridad a las aplicaciones y usuarios

- Proceso sólido de conceder el acceso;
  - El uso de soluciones IDM (Identity Manager)
  - Procesos de RBAC (Role Based Access Control)
  - Campañas de certificación de acceso



© ISACA 2016.
All Rights Reserved.

2016 LATIN CACS AN ISACA EVENT

Más seguridad a las aplicaciones y usuarios

- Gestión de acceso privilegiado;

Caja fuerte de contraseñas

- ✓ autenticación fuerte
- ✓ Gestión de credenciales
- ✓ Control de acceso basado en roles
- ✓ Supervisión de sesiones
- ✓ Grabación de sesiones
- ✓ Gestión de credenciales A2A

#LATINCACS

© ISACA 2016.
All Rights Reserved.

Más seguridad a las aplicaciones y usuarios

- Protección de Datos;

Estructurado (bases de datos)

No Estructurado (sistemas de archivos)

Mainframe

Databases

Filesystem

Big Data

Supervisión de la actividad

Análisis de vulnerabilidad

Identificación de datos sensibles

Bloque de actividades sospechosas

Protección de Datos

Eventos de auditoría

Gestión centralizado

Security Policies

Dashboard

Compliance

Vulnerability

Alerts

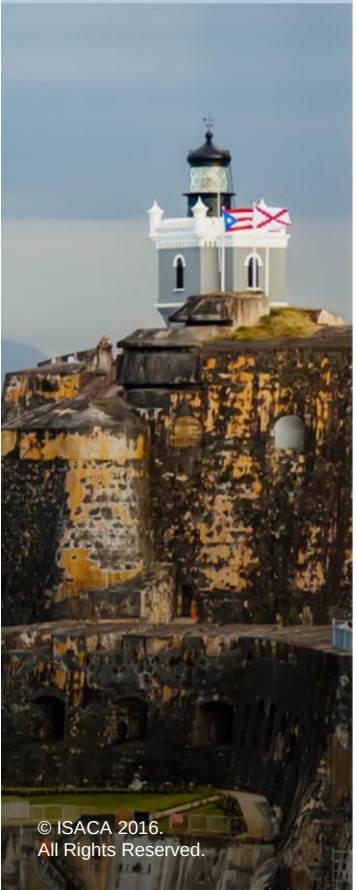
#LATINCACS

© ISACA 2016.
All Rights Reserved.

Más seguridad a las aplicaciones y usuarios

- Y los usuarios, ¿qué es lo que se enfrentarán?
  - Contraseña cada vez más **fuerte y complejo**
  - **Tiempo de vida** corto de contraseña
  - El uso intensivo de la **biométrica: dedos, manos, iris, detalles faciales**
  - **Autenticación multifactor**

© ISACA 2016.
All Rights Reserved.



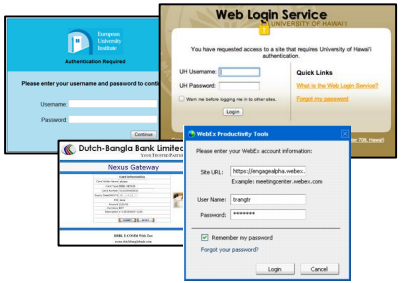
Más seguridad a las aplicaciones y usuarios

- Y los usuarios, ¿qué es lo que se enfrentarán?
  - **La responsabilidad** civil
  - **Los cambios culturales** en el uso de la tecnología
  - **Los marcos reguladores y legislación**

© ISACA 2016.
All Rights Reserved.

Autenticación: nuevas estrategias

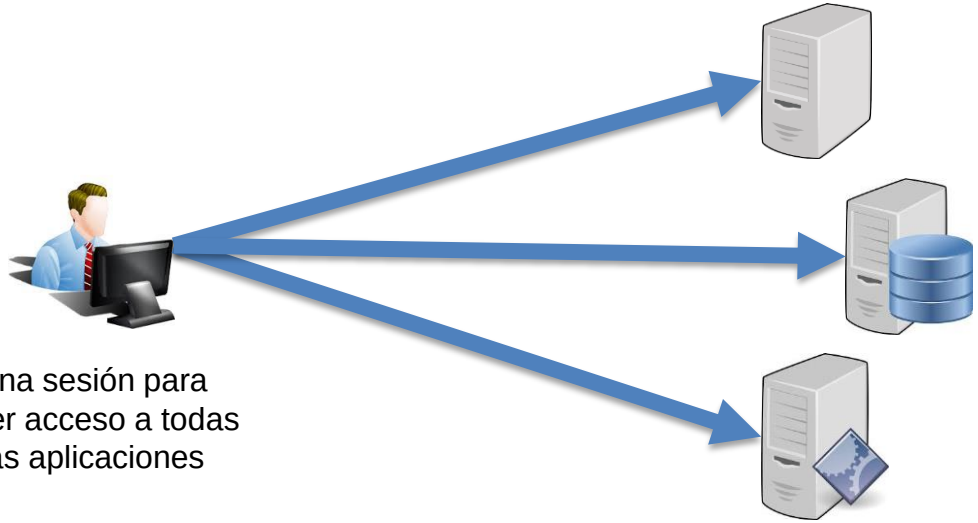
- ¿Lo que se busca mejorar y cómo?
  - La seguridad del usuario
    - La disminución de la cantidad de nombres de usuario / contraseñas



© ISACA 2016.
All Rights Reserved.

Autenticación: nuevas estrategias

- ¿Lo que se busca mejorar y cómo?
  - La seguridad del usuario
    - la autenticación simplificada

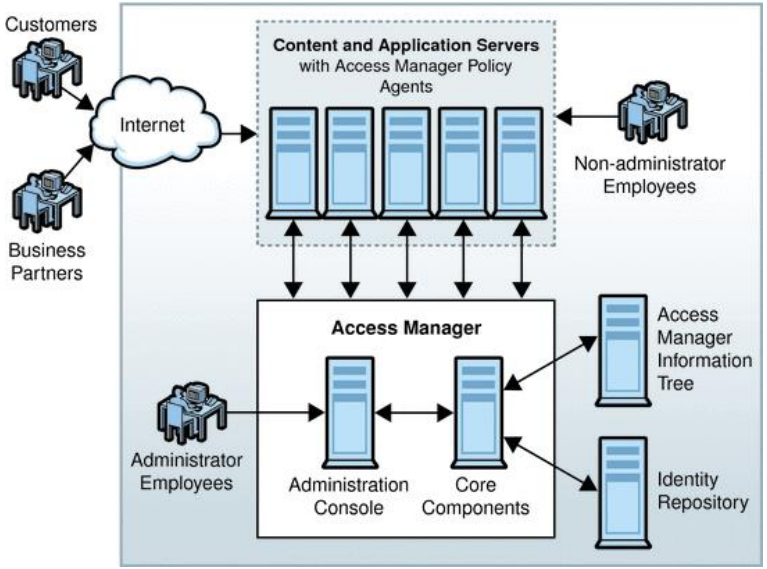


Una sesión para tener acceso a todas las aplicaciones

© ISACA 2016.
All Rights Reserved.

Autenticación: nuevas estrategias

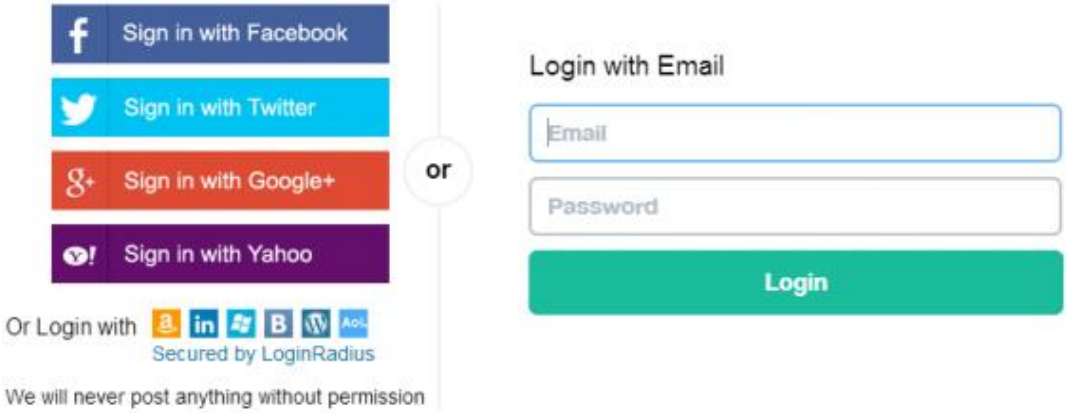
- ¿Lo que se busca mejorar y cómo?
  - Seguridad de las aplicaciones a través de la gestión de accesos



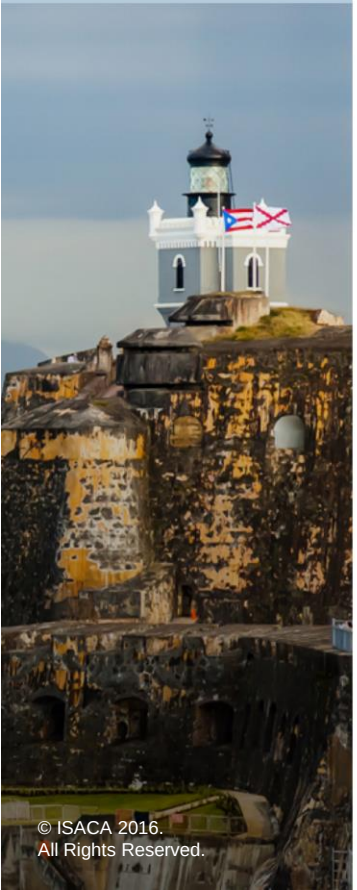
© ISACA 2016.
All Rights Reserved.

Autenticación: nuevas estrategias

- Nuevos métodos de autenticación

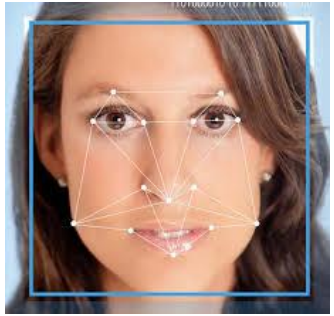


© ISACA 2016.
All Rights Reserved.

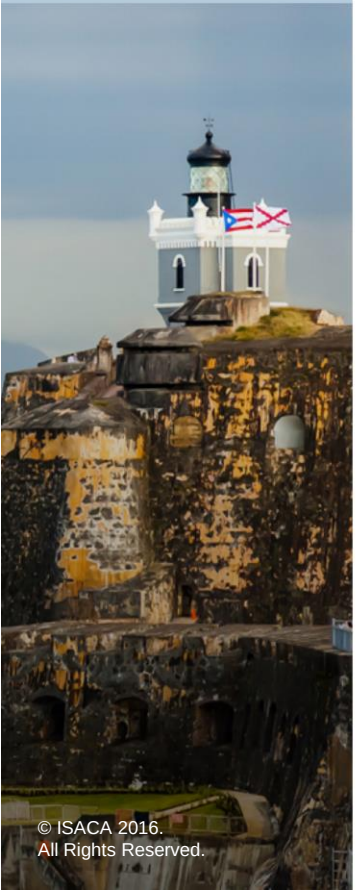


Autenticación: nuevas estrategias

- Dispositivos de autenticación



© ISACA 2016.
All Rights Reserved.



Autenticación: nuevas estrategias

- ¿Y los usuarios?
  - El factor humano es determinante en el uso de la tecnología!

  - La cultura y la formación es vital para el éxito de la tecnología!

© ISACA 2016.
All Rights Reserved.

2016 LATIN CACS™
AN ISACA EVENT

Muchas Gracias!!!

Luciano Johnson, MSc, MBA, CISM, CRISC
Cyber Security Director

luciano@iso27000.com.br
https://br.linkedin.com/in/lucianojohnson