FSA LATAM
SECURITY BUSINESS INTELLIGENCE

Seguridad en la Nube Continuidad Operacional

Julio Balderrama – Director FSA LATAM
@juliobalderrama

Bogot[a 30/09/2016

/fsalatam

@fsalatam

/company/fsalatam

Cloud

¿Quienes realmente utilizan la nube?

Los ciudadanos

Todos poseemos una gran cantidad de información en la nube

- Con conocimiento
- Sin conocimiento
  - - tipo y cantidad o como llego!

Google, WhatsApp, Dropbox, OneDrive, Drive, iCloud, Facebook, …

Utilización de la nube a diario

- Utilización en forma rutinaria
- Conectados en forma permanente
- Hoy en día se puede saber todo lo que hacemos diariamente

Conocimiento de los ciudadanos para con la protección

Preguntas:

- Están en la nube?
- Poseen sus móviles conectados?
- Poseen claves en el móvil? Que tipo de clave?
- Se encuentra cifrado?
- Disponen de una tarjeta de memoria adicional?
- Se encuentra cifrada la tarjeta de memoria?

FSA LATAM
SECURITY BUSINESS INTELLIGENCE

Secreto de la configuración

Como configuramos la privacidad?

- Que información se sincroniza?
- Bakups automáticos de “toda la información”
- Fotos, archivos, resguardo de la conversaciones de WhatsApp, sms, logs de llamadas

- Como prevenir el resguardo de la información sensible?

FSA LATAM
SECURITY BUSINESS INTELLIGENCE

Como se protege

Preguntas incomodas

- Doble factor de autenticación?
- Que de medio / forma?
- Cifrado de los datos en la nube?
- Antvirus / antimalware en el dispositivo?

- Como te proteges?

Personal / Laboral

- Los servicios en la nube para la utilización personal y laboral

FSA LATAM
SECURITY BUSINESS INTELLIGENCE

Que motiva?

- Comunicaciones unificadas
- Acceso remoto
- Aplicaciones Cloud
- Monitorización
- Servicios de correo
- Continuidad del negocio (RDP)
- Backup
- Foco en el negocio

Y la seguridad?

FSA LATAM
SECURITY BUSINESS INTELLIGENCE

Seguimos ...

En las empresas

- Falta de personal especializado
- Sistemas locales muy costosos
- Dependencia local
- Obsolescencia tecnológica
- Falta de equipamiento
- Mayor movilidad

Riesgos Personal

Riesgos de estar en la nube

- Privacidad
- Confidencialidad

La letra pequeña, enemiga de la privacidad, como por ejemplo compartir "algunos" servicios de fotos o archivos con otros usuarios

Términos de servicio: "..podría compartir sus fotografías en su servicio .... Les da el derecho de "usar o distribuir"

Riesgos Organización

- Nuevos riesgos

Ejemplo:

- Sitio web
- Aplicaciones
- Base de datos
- Contenedores de información

- Recurrimos a las empresas que brindan “mágicas” soluciones”

Promovedores de servicios

"marketing" sobre soluciones en la nube

- Los conocen realmente?
- Donde resguardan la información?
- Cómo la resguardan?
- Los visitaron?
- Que controles físicos y lógicos disponen?
- Cual es el nivel mínimo aceptable de seguridad

FSA LATAM
SECURITY BUSINESS INTELLIGENCE

Cumplimiento

- Quienes controlan?
- Realizan controles a sus proveedores?
- Cual es el criterio que se aplica?
- Formación del personal?
- Alcance de los controles
- Cada cuanto tiempo se realiza?
- Como se comunica los hallazgos a los proveedores

El mayor desafío

Para mantener los datos en la nube de forma segura es:

CONCIENTIZACION

Redacción de estándares de aseguramiento a nivel organizacional o adherirse a los existentes en el mercado

FSA LATAM
SECURITY BUSINESS INTELLIGENCE

CSA

Cloud Security Alliance es una organización sin fines de lucro que se encarga de generar documentos, prácticas y recomendaciones, políticas para el uso seguro del Cloud Computing

Familia ISO 27001

Normas dedicadas a la privacidad de Cloud Computing

- ISO/EC 27017
- ISO/IEC 27018

Establecen prácticas y códigos de conducta para la protección de la información en redes públicas

FSA LATAM
SECURITY BUSINESS INTELLIGENCE

Ultimo informe de amenazas

La nube avanza pero no su seguridad

Según el informe de datos ocultos (Shadow Data Theart Report)

- **12%** documentos y archivos que se comparten en forma generalizada contienen información regulada y datos confidenciales como información legal y código fuente.
- **95%** aplicaciones de nube de clase empresarial no cumplen con SOC2.
- **63%** actividad riesgosa de usuarios en la nube indica intentos de transferir datos sin autorización.

http://dc.bluecoat.com/shadow-data-report-20161H

FSA LATAM
SECURITY BUSINESS INTELLIGENCE

Ultimo informe de amenazas

La nube avanza pero no su seguridad

Según el informe de datos ocultos (Shadow Data Theart Report)

- **37%** actividad sospechosa en la nube indica intentos de hackear cuentas de usuarios en la nube.
- **71%** aplicaciones empresariales de nube no provee autenticación de factores múltiples.
- **11%** aplicaciones empresariales de nube aún son vulnerables a uno o más de los exploits principales, como FREAK, Logjam, Heartbleed, Poodle SSLv3, Poodle TLS y CRIME.

http://dc.bluecoat.com/shadow-data-report-20161H

Estándares de seguridad en la nube

¿Qué estándares existen?

CSA Cloud Controls Matrix v3.0.1 (CMM)

CSA STAR Certification

ISO/IEC 27017 Código de buenas prácticas de controles de servicios basados en computación en la nube

FSA LATAM
SECURITY BUSINESS INTELLIGENCE

CCM v3.0.1

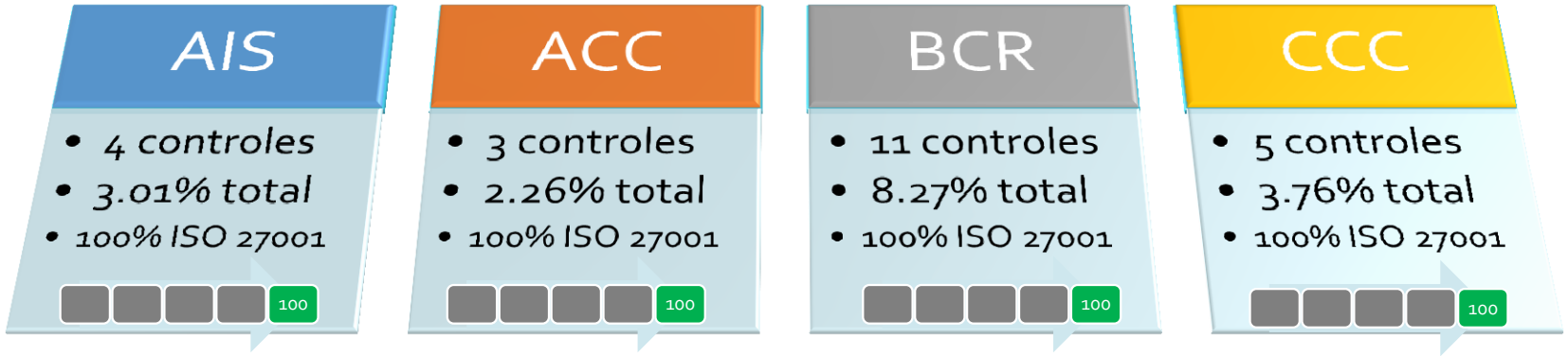
Matriz de Controles de Cloud

AIS Application & Interface Security	HRS Human Resources Security
AAC Audit Assurance & Compliance	IAM Identity & Access Management
BCR Business Continuity Mgmt & Op Resilience	IVS Infrastructure & Virtualization
CCC Change Control & Configuration Management	IPY Interoperability & Portability
DSI Data Security & Information Lifecycle Mgmt	MOS Mobile Security
DSC Datacenter Security	SEF Sec. Incident Mgmt, E-Disc & Cloud Forensics
EKM Encryption & Key Management	STA Supply Chain Mgmt, Transparency & Accountabil
GRM Governance & Risk Management	TVM Threat & Vulnerability Management

133 CONTROLS
Cloud Controls Matrix v3.0.1

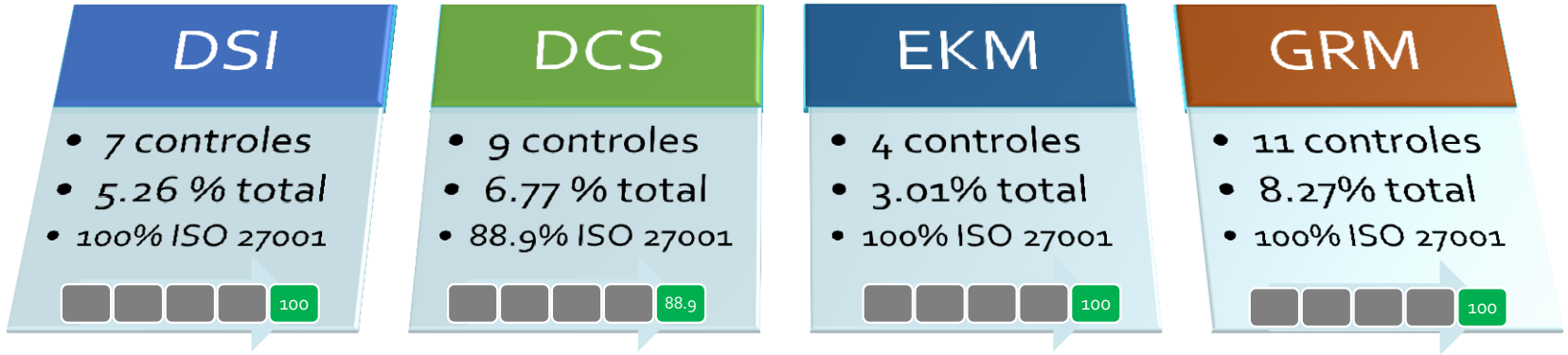
https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/

CCM v3.0.1 vs ISO 27001



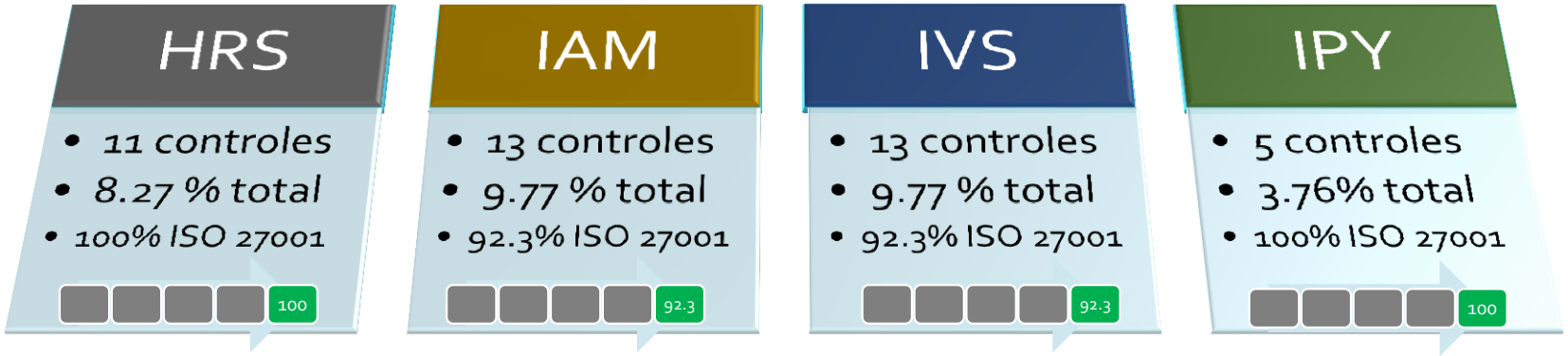
- Aplicación y seguridad en la interfaz (AIS)
- Aseguramiento de la auditoria y cumplimiento (ACC)
- Gestión de continuidad del negocio y resiliencia operacional (BCR)
- Control de cambios y gestión de configuración (CCC)

CCM v3.0.1 vs ISO 27001



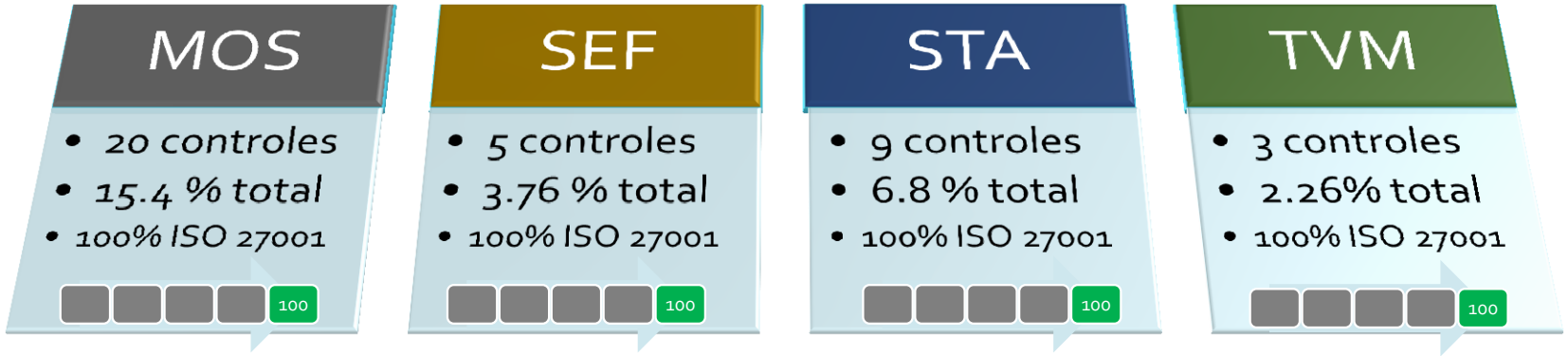
- Seguridad de los datos y ciclo de vida de la gestión de información (DSI)
- Seguridad en el centro de datos (DCS)
- Encriptación y gestión de claves (EKM)
- Gobernanza y gestión de riesgos (GRM)

CCM v3.0.1 vs ISO 27001



- Recursos humanos (HRS)
- Gestión de acceso y identidad (IAM)
- Seguridad de la virtualización y infraestructura (IVS)
- Portabilidad y Interoperabilidad (IPY)

CCM v3.0.1 vs ISO 27001



- Seguridad móvil (MOS)
- Gestión de incidentes de seguridad, E-Discovery y forense en la nube (SEF)
- Gestión de la cadena de suministro, la transparencia y rendición de cuentas (STA)
- Gestión de vulnerabilidades y amenazas (TVM)

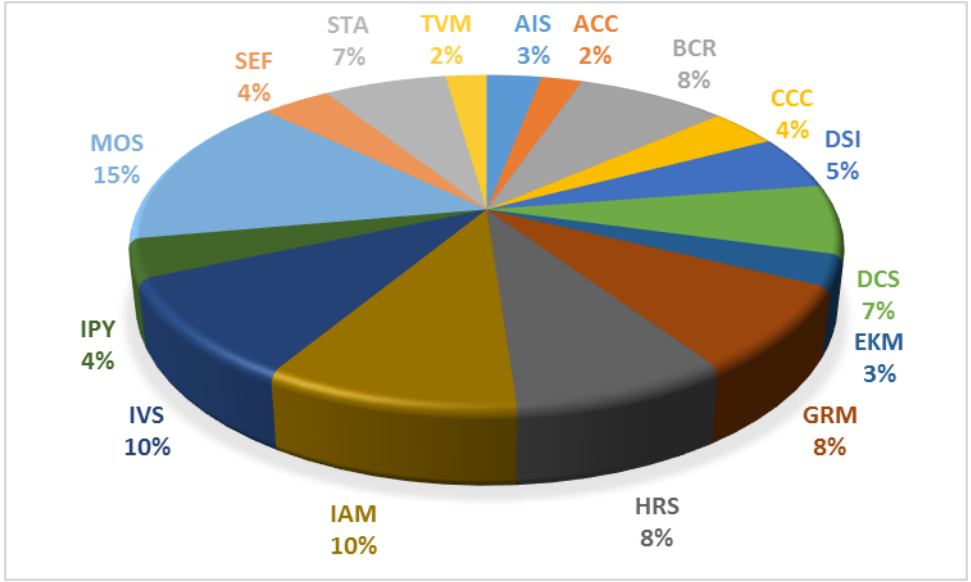
FSA LATAM
SECURITY BUSINESS INTELLIGENCE

Esfuerzo con Cloud Control Matrix!!

98,3% alienado

ISO 27001

Esfuerzo 1,66%



AIS	Application & Interface Security	HRS	Human Resources Security
AAC	Audit Assurance & Compliance	IAM	Identity & Access Management
BCR	Business Continuity Mgmt & Op Resilience	IVS	Infrastructure & Virtualization
CCC	Change Control & Configuration Management	IPY	Interoperability & Portability
DSI	Data Security & Information Lifecycle Mgmt	MOS	Mobile Security
DSC	Datacenter Security	SEF	Sec. Incident Mgmt, E-Disc & Cloud Forensics
EKM	Encryption & Key Management	STA	Supply Chain Mgmt, Transparency & Accountability
GRM	Governance & Risk Management	TVM	Threat & Vulnerability Management

Estándares de seguridad en la nube

¿Qué estándares existen?

CSA Cloud Controls Matrix v3.0.1 (CMM)

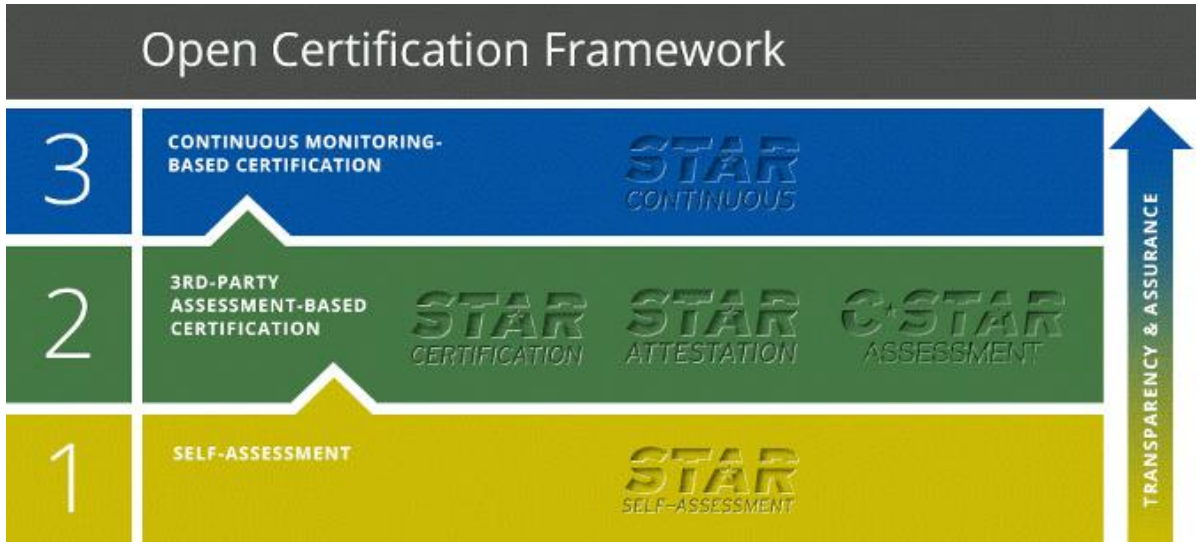
CSA STAR Certification

ISO/IEC 27017 Código de buenas prácticas de controles de servicios basados en computación en la nube

CSA STAR

CSA Security, Trust & Assurance Registry (STAR)

- El registro de evaluación, confianza y seguridad **CSA STAR (Security, Trust & Assurance Registry)** de la organización Cloud Security Alliance es un mecanismo de evaluación de la seguridad de los proveedores de servicios en la nube, aunando principios de transparencia, rigor en la auditoría, armonización de estándares y monitorización continua.



https://cloudsecurityalliance.org/star/

CSA STAR

Para la evaluación ofrece una matriz de controles cloud (**Cloud Controls Matrix (CCM)**) con correspondencias con distintos estándares, mejores prácticas y normativas (COBIT, HIPPA, ISO27001, ISO 27017, ISO 27018, ISO 27036, NIST SP800-53, Fed RAMP, PCI DSS, BITS, GAPP, entre otras)

La matriz de controles cloud cubre las áreas de:

- Cumplimiento
- Gobernanza de datos
- Seguridad de las instalaciones
- Recursos humanos
- Seguridad de la información
- Legal
- Gestión de operaciones
- Gestión de riesgos
- Gestión de versiones
- Resiliencia
- Arquitectura de seguridad.

Estándares de seguridad en la nube

¿Qué estándares existen?

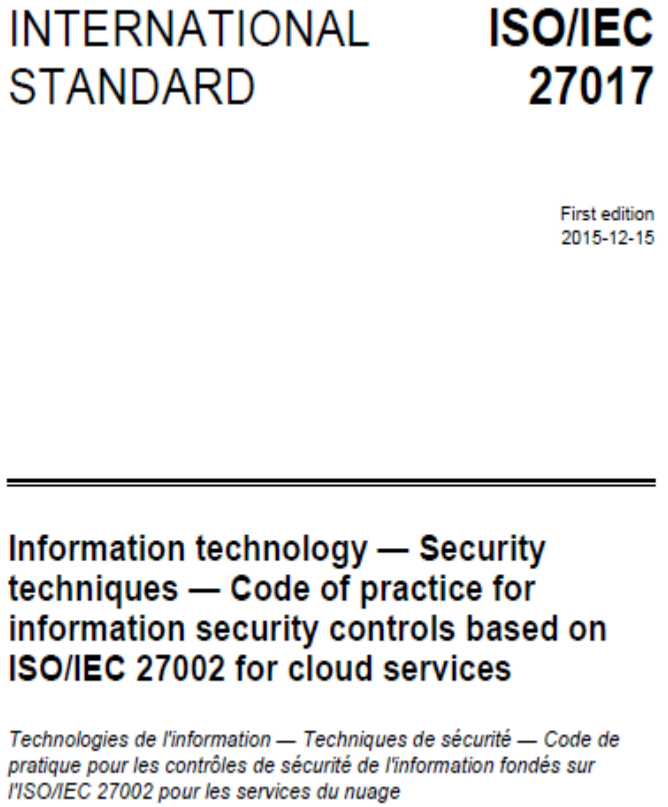
CSA Cloud Controls Matrix v3.0.1 (CMM)

CSA STAR Certification

ISO/IEC 27017 Código de buenas prácticas de controles de servicios basados en computación en la nube

ISO/IEC 27017

- **Código de práctica para los controles de seguridad de la información según la norma ISO 27002 para los servicios en la nube**", lo que implica que la norma está basada en los controles de seguridad que recoge la norma ISO 27002



INTERNATIONAL STANDARD

ISO/IEC 27017

First edition
2015-12-15

Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

Technologies de l'information — Techniques de sécurité — Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage

ISO/IEC 27017

ISO 27001	ISO 27017
5 Políticas de seguridad de la Información	Moderar
6 Organización de la seguridad de la Información	Moderar
7 La seguridad de los recursos humanos	Moderado/Bajo
8 Gestión de activos	Moderado/Bajo
9 Control de acceso	Alto
10 Criptografía	Moderar
11 La seguridad física y ambiental	Moderado/Alto
12 Seguridad Operaciones	Moderado/Alto
13 Seguridad Comunicaciones	Moderado/Alto
14 Sistema de adquisición, desarrollo y mantenimiento	Moderar
15 Relaciones con los proveedores	Moderado/Alto
16 Información de gestión de incidentes de seguridad	Moderar
17 Aspectos de Seguridad de Información de la Gestión de la Continuidad del Negocio	Bajo
18 Cumplimiento	Moderado/Alto

Los más importante

Cada uno de nosotros y las organizaciones debemos tomar la responsabilidad que la protección de la información es responsabilidad de cada uno de nosotros, es nuestra información, nosotros somos los dueños de los datos y cada día nos encontramos más expuestos, pero si uno toma todos los recaudos puede mantener la continuidad operacional

FSA LATAM
SECURITY BUSINESS INTELLIGENCE

Contacto

Muchas gracias!!

Julio Balderrama

julio@fsalatam.com
+54911 3271 2639
@juliobalderrama