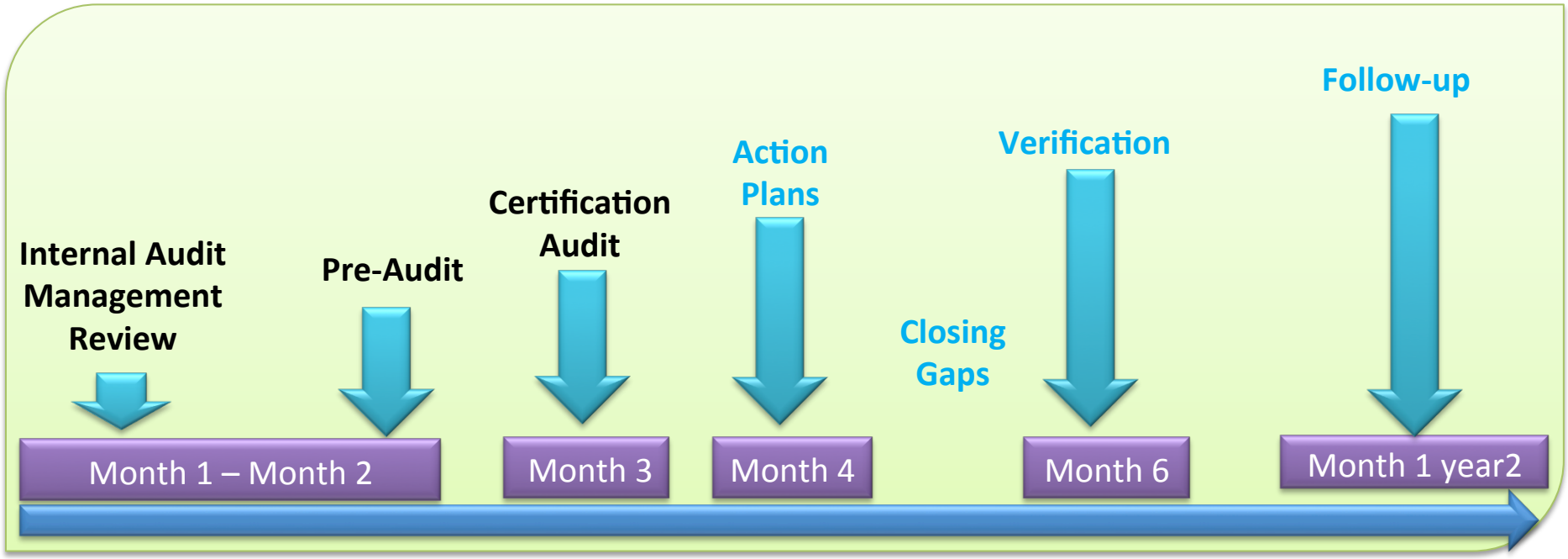
ACSDA
General Assembly
2017
La Paz – Bolivia

Deceval va más allá

Certification Process



Relevant steps:

- ✓ Defining scope of ISMS
- ✓ Defining scope of the certification audit
- ✓ Elaboration of the statement of applicability
- ✓ Internal audits of the ISMS
- ✓ Auditor training
- ✓ Management review

Key Benefits of ISO 27001 Certification

ISO 27001

BUREAU VERITAS
Certification

- Strengthen securities market confidence
- Mitigate cyber security risks
- Compliance with cyber resilience in financial market infrastructures IOSCO Guide
- Regulatory compliance
  - Electronic invoicing
  - ONAC Accreditation
  - CE052/042
  - Decree 2364 2012

CYBER RISKS: Guidance on Cyber Resilience for Financial Market Infrastructures - IOSCO:

- **Learning and Evolving:** Culture of cyber risk awareness whereby its resilience posture, at every level, is regularly and frequently re-evaluated.
- **Situational awareness:** Understanding of the cyber threat within which it operates, and the implications of being in that environment for its business and the adequacy of its cyber risk mitigation measures.
- **Testing:** All elements of a cyber resilience framework should be rigorously tested to determine their overall effectiveness before being deployed within an FMI, and regularly thereafter.
- **Identification:** Identify which of the critical operations and supporting information assets should, in order of priority, be protected against compromise.
- **Protection:** Cyber resilience depends on effective security controls and system and process design that protect the confidentiality, integrity and availability of an FMI's assets and services.
- **Detection:** Ability to recognise signs of a potential cyber incident, or detect that an actual breach has taken place
- **Governance:** Cyber governance refers to the arrangements a company has put in place to establish, implement and review its approach to managing cyber risks.
- **Recovery** : Ability to resume critical operations rapidly, safely, and with accurate data.

CYBER – RESILIENCE GUIDE - IOSCO

Strengths:

- *ISO 27001 Certified:* Being an ISO 27001 certified Company eases and favors compliance with any other international standard as this particular certification covers extensively information security risk mitigation.

- *Cybersecurity risk management:* A complete support in cybersecurity risk management is observed as the Company addresses other related companies within the stock market ecosystem.

- *Business continuity*: Efforts along business continuity are evident and they demonstrate commitment in guaranteeing availability of information in each of the services that support business processes.

- *Full Company cooperation*: It is observed that all areas of DECEVAL are involved in order to respond in a timely manner to an information security incident.

- *Trained Personnel*: A full commitment in training for cybersecurity incidents, throughout the Company, is observed and embedded within security culture.

CYBER – RESILIENCE GUIDE - IOSCO

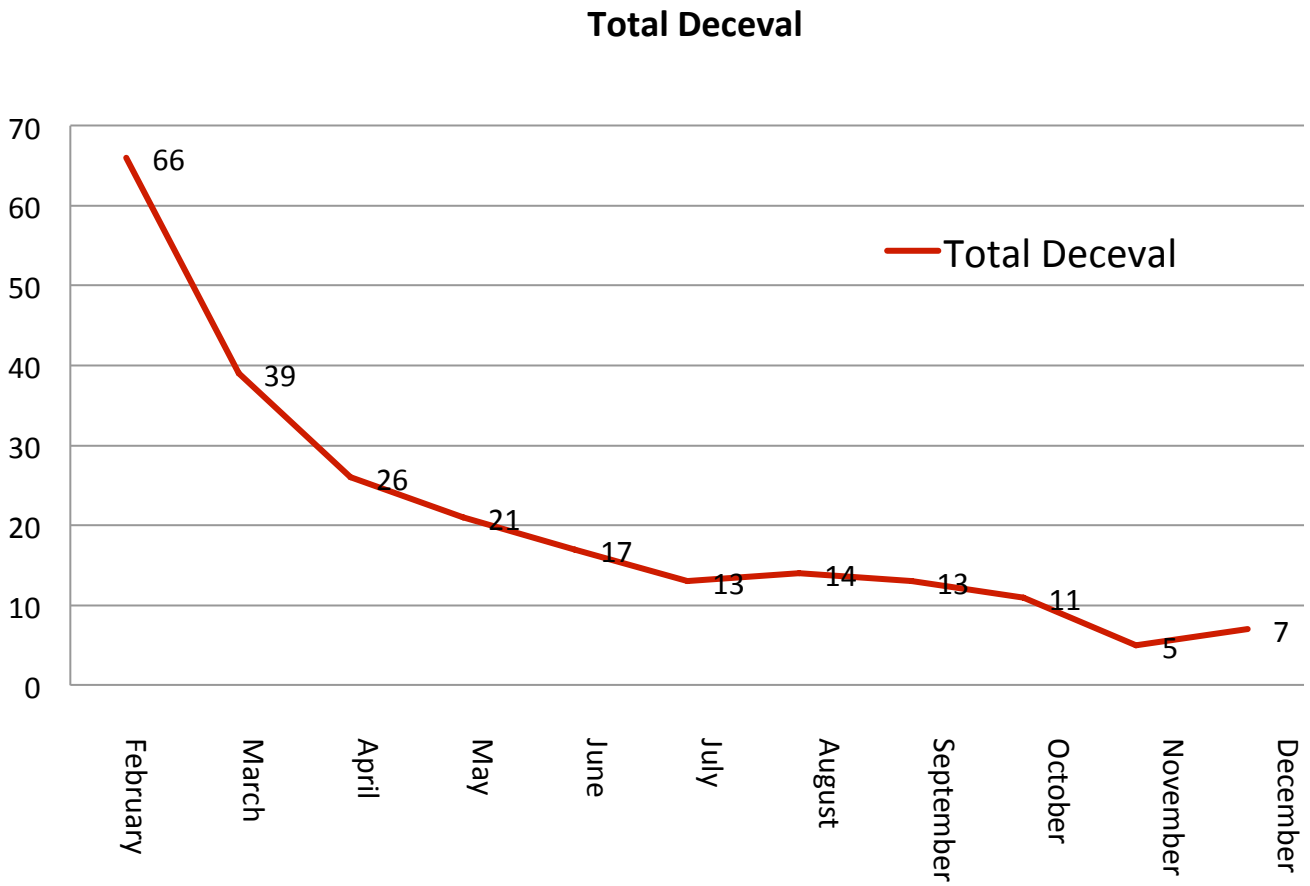
Principal opportunities for improvement:

- *Sharing information regarding threats and vulnerabilities with the market*: Demonstrated efforts are shown for cooperation between other companies within the market. But nevertheless, a formal joint process may be needed to identify and mitigate threats and vulnerabilities which represent a risk for the industry.

- *Involve authorities in threat and vulnerability information sharing*: Even though DECEVAL is present in cybersecurity meetings with the Ministry of Defense, it is advised to formalize partnerships with authorities for cybersecurity threat and vulnerability sharing.

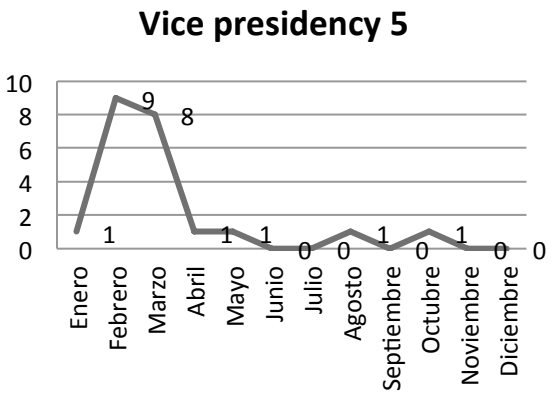
- *Greater SOC Scope*: It is strongly recommended to integrate today's SOC service (limited to firewalls) with the correlation tool used by DECEVAL (Qradar), bringing together more visibility with more critical assets, improving threat detection and prevention capability, and applying cybersecurity intelligence procedures.

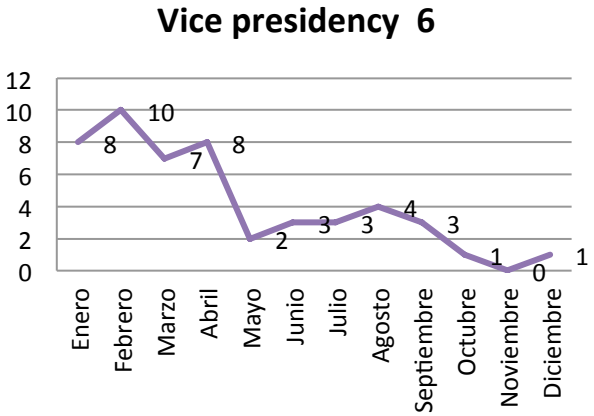
Monitoring Secure Password 2014

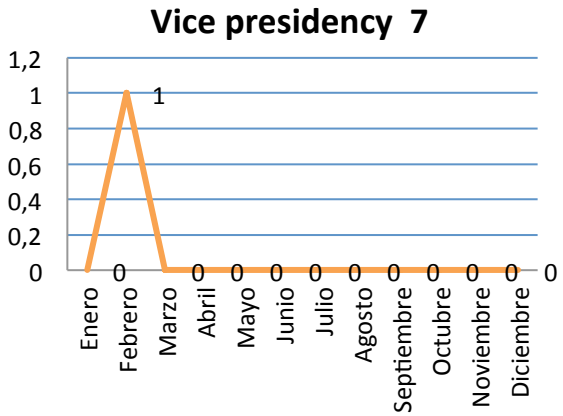


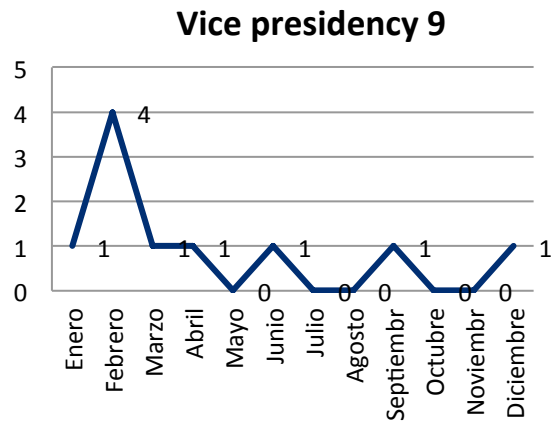
Month	% Unsafe
February	35.83%
March	20.53%
April	13.20%
May	10.66%
June	8.63%
July	6.40%
August	6.90%
September	6.40%
October	5.42%
November	2.46%
December	3.45%

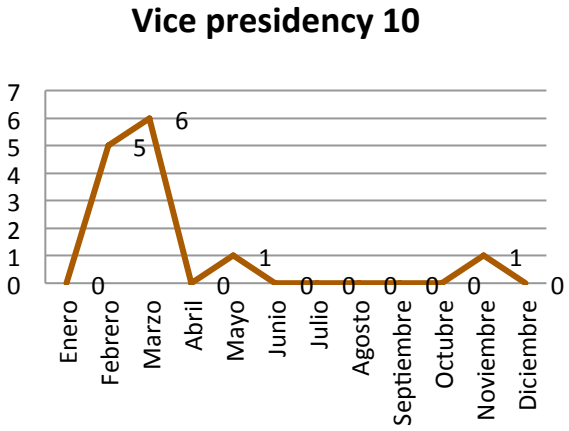
Example Statistics Unsafe Passwords

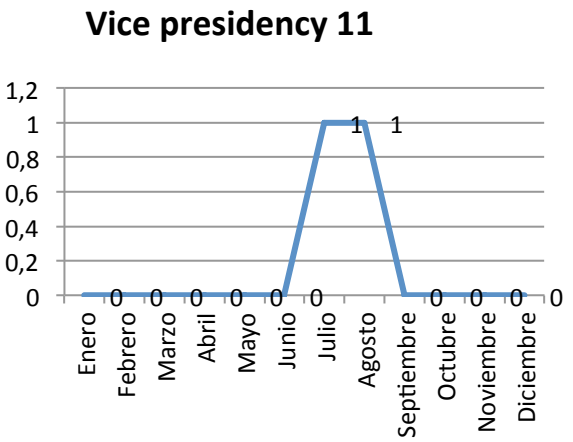












ACTIVITIES WITH INTERNAL AND EXTERNAL USERS DECEVAL

MAIN APPROACHES

- Password management
- Workshop: secure passwords
- Personal Information Management
- Measuring compliance
- Specialized training
- Specialized tests
- Monthly Statistics
- Reporting to senior management

PROVIDER RISK LEVEL ASSESSMENT

Phase1: Criteria for the selection of suppliers with a higher level of exposure to Information Security, Corporate Security and Business Continuity risks

		10%		10%		10%		10%		10%		10%		EVALUACIÓN TOTAL	DESCRIPCIÓN
	Nombre del Proveedor	3	TIENE ACCESO A INFORMACIÓN PRIVADA DE DECEVAL	4	LA INDISPONIBILIDAD DE SUS SERVICIOS GENERA INDISPONIBILIDAD DE UN SERVICIO CORE DE DECEVAL	5	PRESTA SOPORTE SOBRE UN APLICATIVO DE NIVEL 1 O ALGUNO DE SUS COMPONENTES	6	NO EXISTE EN EL MERCADO OTRO PROVEEDOR QUE PRESTE ESTE SERVICIO	7	EL PROVEEDOR ASUME UN PROCESO DE DECEVAL DE FORMA TERCERIZADA	8	EL SERVICIO INCLUYE PERSONAL EN SITIO PERMANENTE O TEMPORAL CON ASIGNACIÓN DE TARJET...	9	EVALUACIÓN TOTAL	DESCRIPCIÓN
57	SISTEMAS INTEGRALES DE INFORMACION SISA	0%	x	10%		0%		0%		0%		10%		0%	10%	Riesgo Tolerable
58	TELMEX COLOMBIA SA	0%		0%	x	10%	x	10%		0%	x	10%		0%	50%	Riesgo Moderado
59	SERTISOFT SA	20%		0%	x	10%	x	10%	x	10%	x	10%		0%	70%	Riesgo Alto
60	GETRONICS COLOMBIA LTDA	20%	x	10%	x	10%	x	10%		0%	x	10%	x	10%	90%	Riesgo Critico

Risk Level:
76% to 100%: Critical
From 51% to 75%: High
From 26% to 50%: Moderate
From 0% to 25%: Tolerable

Frequency of Visit:
Red: Semester
Orange: Annual
Yellow: Bi-Annual
Green: Never

Prioritization ranges and periodicity of visits will be explained in the next slide.

Phase 2: Preparation of the questionnaire on Information Security, Corporate Security and Business Continuity to Suppliers.

14	Preguntas Estándar Cuestionario de Riesgos a Proveedores	
15		
16	1.0 Políticas, normas, estándares, procesos y procedimientos	Respuesta del Proveedor
17	1.1 ¿Tiene políticas, normas, estándares, procesos y procedimientos documentados de Seguridad de la Información y Continiudad del Negocio?	No posee políticas específicas de Seguridad de la Información ni de Continuidad del Negocio, tampoco normas o Información documentada.

Phase 3: Visits to each of the suppliers with the highest exposure to the risk of Information Security, Corporate Security and Business Continuity

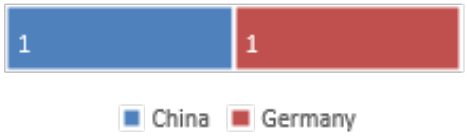
- **To coordinate**
  - Coordination with the contract leader and the audit provider.
- **Notify / Invite**
  - Report on auditing and invite the areas involved.
- **Execution**
  - Visit to the supplier and application of the Risk questionnaire.
- **Report**
  - Consolidation and dissemination of results with areas involved.
- **Presentation to the Risk Committee**
  - Presentation of results and decision making.

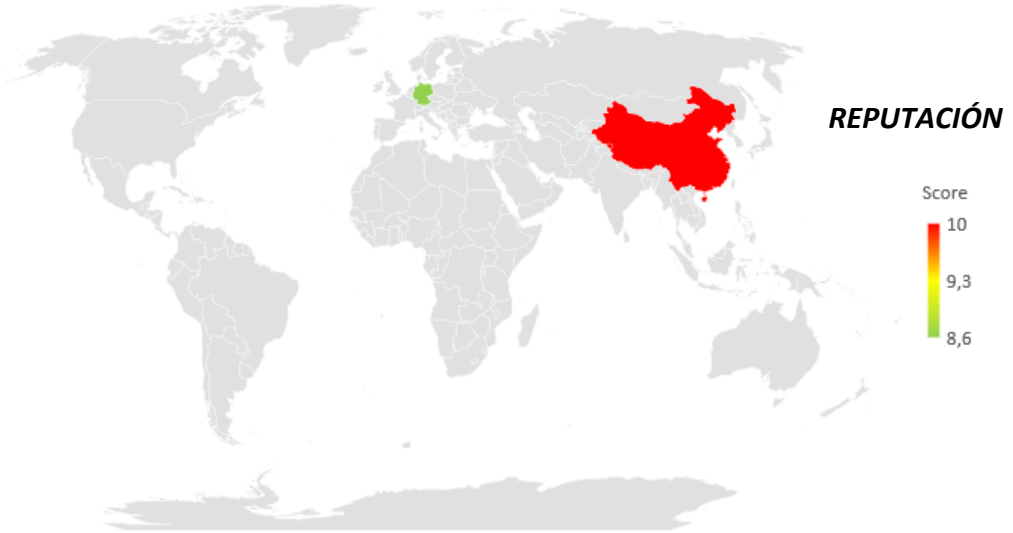
Cyber Security Monitoring 2017

January 2017

GEOGRAPHIC LOCATION
Source ***IP***

Total
2
Countries

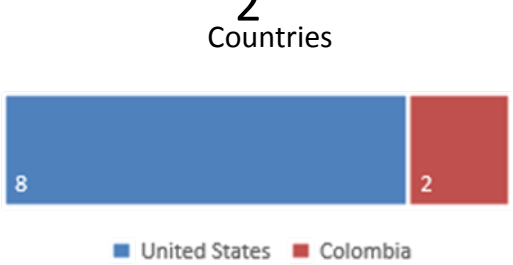


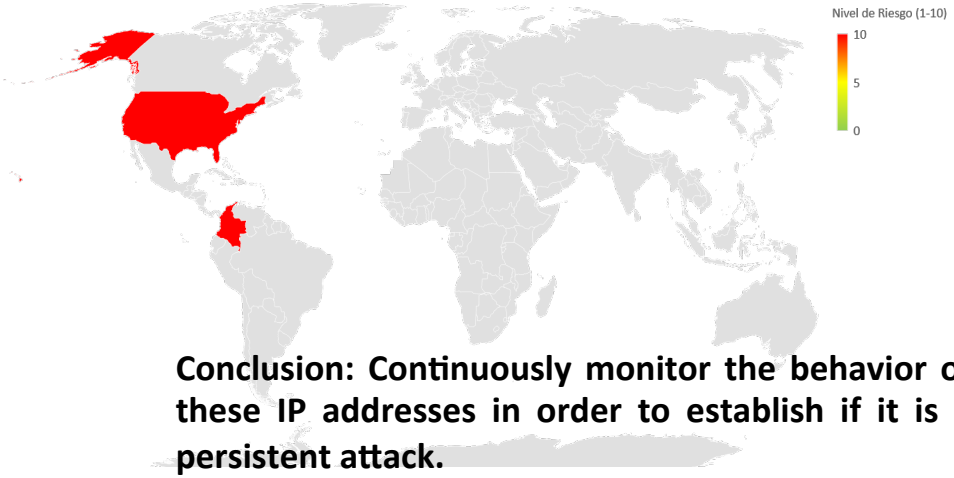


February 2017

GEOGRAPHIC LOCATION
Source ***IP***

Total
2
Countries





Conclusion: Continuously monitor the behavior of these IP addresses in order to establish if it is a persistent attack.

ACSDA
General Assembly
2017
La Paz – Bolivia

Deceval va más allá