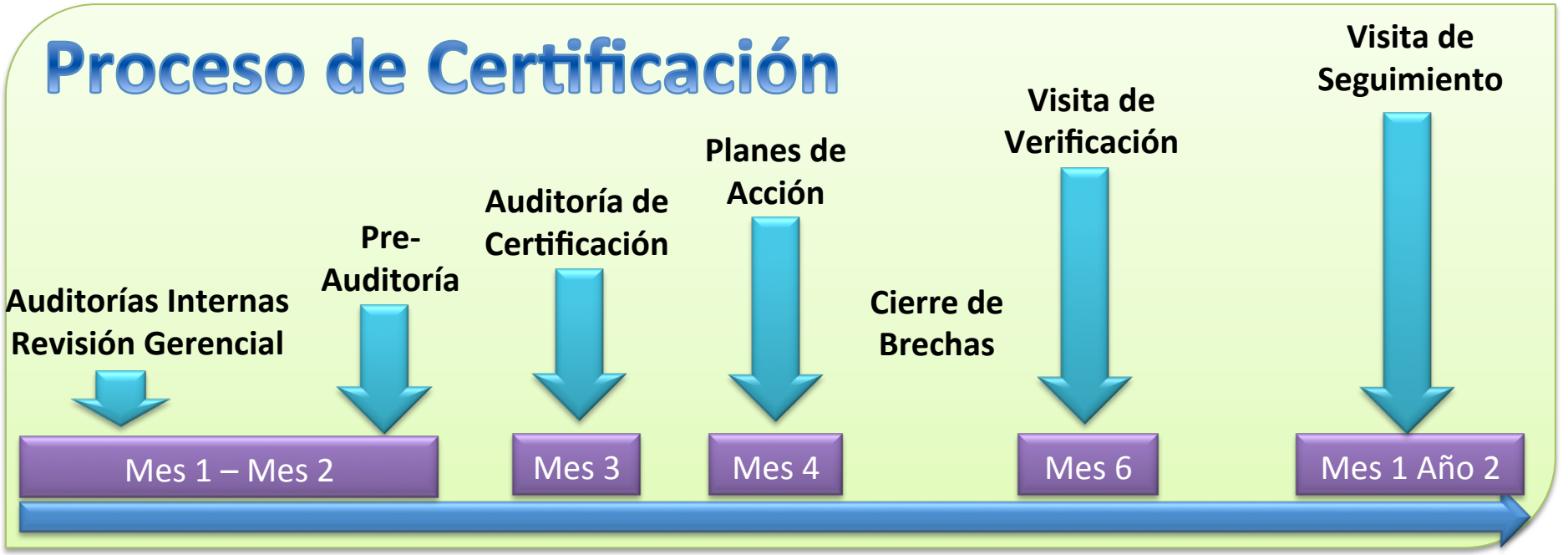
Asamblea General de ACSDA 2017 La Paz – Bolivia

Deceval va más allá



Aspecto Relevantes:

- ✓ Definición del alcance del SGSI
- ✓ Definición del alcance de la auditoría de certificación
- ✓ Elaboración de la declaración de aplicabilidad
- ✓ Auditorias Internas del SGSI
- ✓ Capacitaciones Auditores
- ✓ Revisión Gerencial

Principales beneficios de la certificación ISO 27001

ISO 27001

BUREAU VERITAS
Certification

- Fortalecer confianza del mercado en el manejo de la información custodiada por DECEVAL
- Mitigar riegos de ciber-seguridad
- Documento Cyber resilience in financial market infrastructures IOSCO
- Cumplimiento regulatorio:
  - Factura Electrónica
  - Criterios específicos de acreditación de entidades de certificación digital – ONAC
  - CE052/042
  - Decreto 2364 / 2012

GUÍA DE CIBER-RESILIENCIA – IOSCO:

Gobierno

Recuperación

Aprendizaje y Evolución	Marco de ciber-resiliencia adaptativo y evolutivo. Cultura de la conciencia del riesgo cibernético en todos los niveles de forma regular
Entendimiento Situacional	Identificación de las posibles amenazas cibernéticas, alcance e implicaciones en el mercado de valores.
Pruebas	Probar los elementos del marco resiliencia cibernética para determinar su eficacia general antes de ser desplegados y regularmente después de su puesta en producción.
Identificación	Identificación de operaciones críticas, clasificación de activos de información, inter-dependencias internas y externas.
Protección	Determinación de controles efectivos de seguridad de los sistemas para proteger la confidencialidad, integridad y disponibilidad de bienes y servicios
Detección	La capacidad de reconocer los signos de un posible incidente cibernético
Gobierno	Acuerdos para establecer, implementar y revisar el enfoque de la gestión de riesgos cibernéticos.
Recuperación	Capacidad de reanudar las operaciones críticas rápidamente, de forma segura y con datos precisos.

CIBER-RESILIENCIA: Capacidad de anticipar, resistir, contener y recuperarse rápidamente de un ciber-ataque

GUÍA DE CIBER-RESILIENCIA - IOSCO

Principales fortalezas:

- *Certificación ISO 27001:* Estar certificados en la norma ISO 27001 favorece y facilita la alineación con cualquier estándar internacional ya que esta certificación abarca de manera integral la mitigación de riesgos de seguridad de la información.

- *Gestión de riesgos de ciberseguridad:* Se observa un trabajo completo en apoyo a la gestión de riesgos cibernéticos con un amplio alcance que incluye a las entidades relacionadas con el ecosistema del mercado de valores.

- *Continuidad de negocios*: Los esfuerzos en materia de continuidad del negocio son evidentes y demuestran el compromiso por garantizar la disponibilidad de la información en cada uno de los servicios que soportan los procesos de negocio.

- *Cooperación de toda la entidad*: Se observa que todas las áreas de DECEVAL están involucradas en pro de responder de forma oportuna ante un incidente de seguridad de la información.

- *Personal altamente capacitado*: Se observa compromiso por capacitar a los funcionarios de todas las áreas en materia de seguridad de la información.

GUÍA DE CIBER-RESILIENCIA - IOSCO

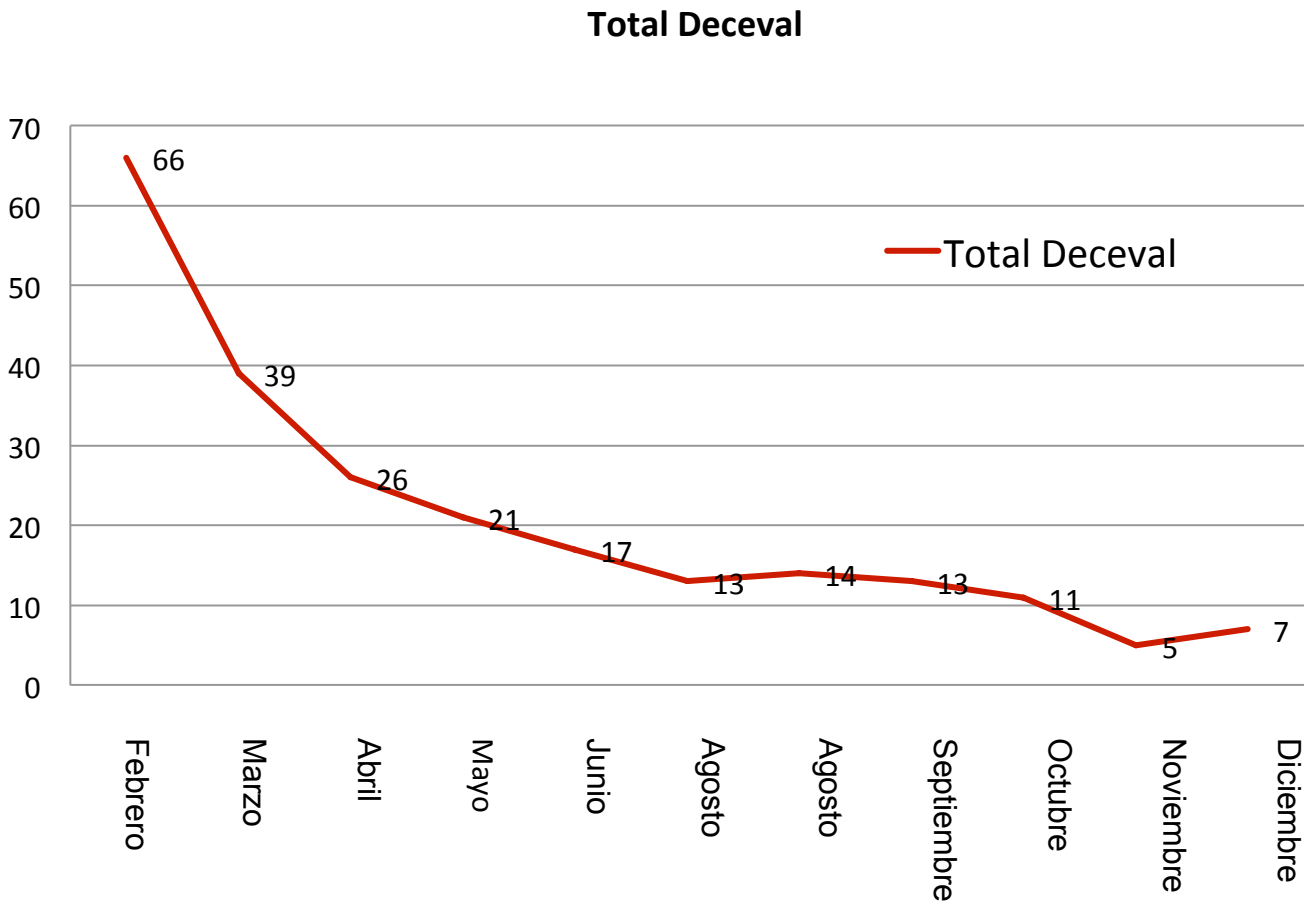
Principales oportunidades de mejora:

- *Compartir Información de Amenazas y Vulnerabilidades del Mercado*: Se evidencian esfuerzos en la cooperación entre entidades del mercado, sin embargo, es importante contar con un esquema conjunto que permita la identificación y mitigación de amenazas y vulnerabilidades cibernéticas que impliquen un riesgo para la industria.

- *Compartir Información de Amenazas y Vulnerabilidades con Autoridades*: Si bien DECEVAL participa activamente en las mesas de ciberseguridad del Ministerio de Defensa, se sugiere hacer alianzas para compartir información de amenazas y vulnerabilidades con las autoridades.

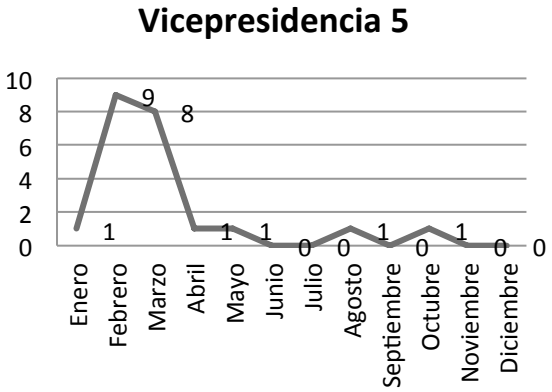
- *Mayor alcance en el SOC de DECEVAL*: Se recomienda integrar el servicio de SOC actual (limitado a solo firewalls) con la herramienta de correlación actual de DECEVAL (Qradar), abarcando una mayor cantidad de activos críticos, mejorando la capacidad de detección y prevención contra amenazas y la ejecución de inteligencia de ciberseguridad.

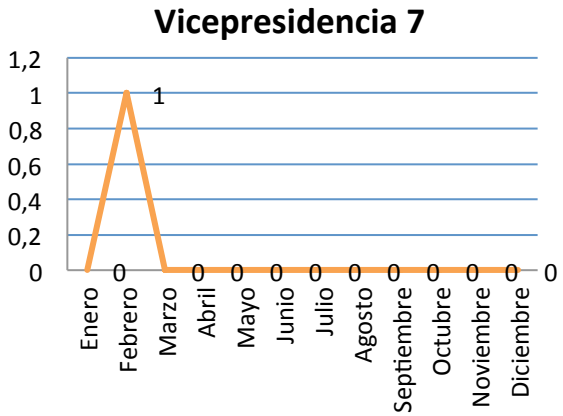
Monitoreo Contraseña Segura 2014

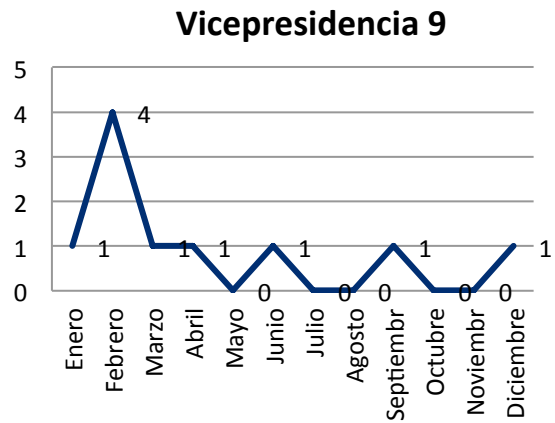


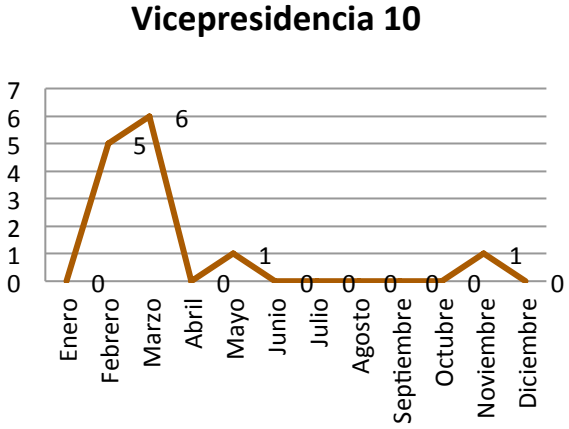
Mes	% Inseguro
Febrero	35.83%
Marzo	20.53%
Abril	13.20%
Mayo	10.66%
Junio	8.63%
Agosto	6.40%
Agosto	6.90%
Septiembre	6.40%
Octubre	5.42%
Noviembre	2.46%
Diciembre	3.45%

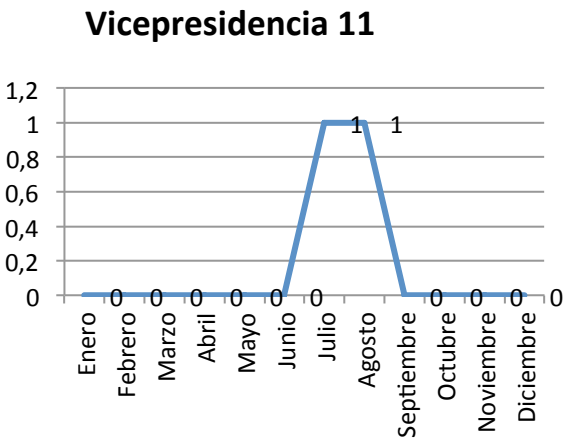
Ejemplo Estadísticas de Contraseñas no Seguras











ACTIVIDADES CON USUARIOS INTERNOS Y EXTERNOS EN DECEVAL

PRINCIPALES ENFOQUES

- Manejo de contraseñas
- Taller de contraseñas seguras
- Manejo de información personal
- Medición de cumplimiento
- Capacitaciones especializadas
- Pruebas especializadas
- Estadísticas mensuales
- Reporte a la alta dirección

EVALUACIÓN DE NIVEL DE RIESGO DE PROVEEDORES

Fase 1: Criterios para la selección de proveedores con mayor nivel de exposición a riesgos de Seguridad de la Información, Seguridad Corporativa y Continuidad del Negocio.

	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
		10%		10%		10%		10%		10%		10%		10%		EVALUACIÓN TOTAL	DESCRIPCIÓN
57	SISTEMAS INTEGRALES DE INFORMACION SISA	0%	X	10%		0%		0%		0%		0%		0%	10%	Riesgo Tolerable
58	TELMEX COLOMBIA SA	0%		0%	X	10%	X	10%		0%	X	10%		0%	30%	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

Nivel de Riesgo:
Del 76% al 100%: Crítico
Del 51% al 75%: Alto
Del 26% al 50%: Moderado
Del 0% al 25%: Tolerable

Periodicidad de Visita:
Rojo: Semestral
Naranja: Anual
Amarillo: Bi-Anual
Verde: Nunca

Los rangos de priorización y la periodicidad de las visitas se explicarán en la siguiente diapositiva.

Fase 2: Preparación del cuestionario sobre Seguridad de la Información, Seguridad Corporativa y Continuidad del Negocio a Proveedores.

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.

Fase 3: Visitas a cada uno de los proveedores con mayor exposición al riesgo de Seguridad de la Información, Seguridad Corporativa y Continuidad del Negocio

Coordinar
- Coordinación con el líder del contrato ly el proveedor la auditoría.

Notificar / Invitar
- Informar sobre auditoría e invitar a las áreas involucradas.

Ejecución
- Visita al proveedor y aplicación del cuestionario de Riesgo.

Informar
- Consolidación y divulgación de resultados con áreas Involucradas.

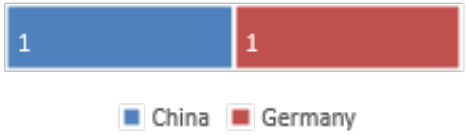
Presentación a Comité de riesgos
- Exposición de resultados y toma de decisiones.

Fortalecimiento de la Ciberseguridad: Mejora en el Servicio de SOC con QRadar

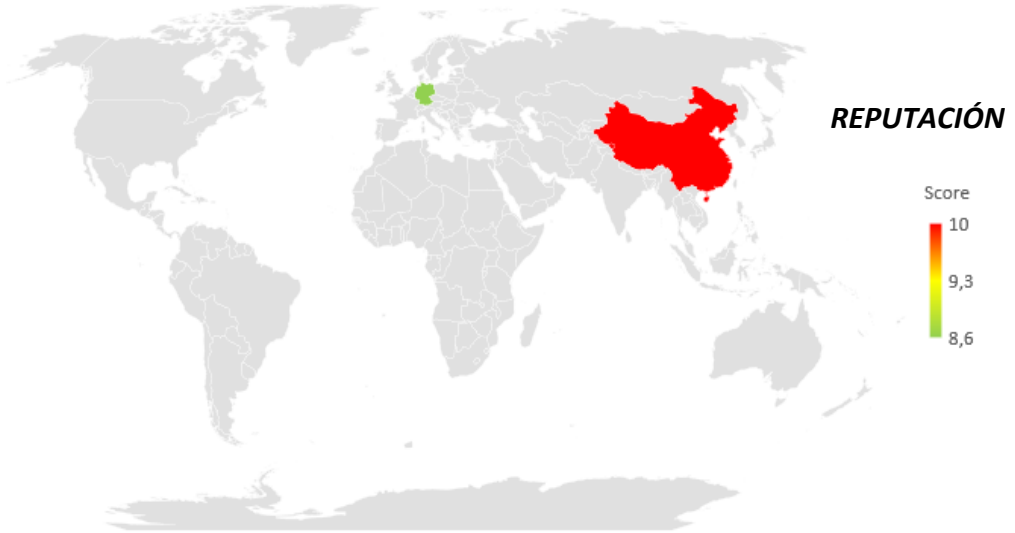
Resultados Enero 2017

UBICACIÓN GEOGRÁFICA

Total
2
países



REPUTACIÓN



Resultados Febrero 2017

Ubicación IP origen

Total
2
países

Conclusión: Monitorear el comportamiento de estas Direcciones IP en el tiempo para establecer si es un ataque dirigido o persistente.

Asamblea General de ACSDA 2017 La Paz – Bolivia

Deceval va más allá