XV REUNIÓN DE AUDITORES INTERNOS
DE BANCOS CENTRALES

“Estrategias para gestionar amenazas tecnológicas y ciberseguridad”

BANCO CENTRAL DE CHILE, SANTIAGO, CHILE

SEPTIEMBRE 25 - 27, 2019

BANCO DE ESPAÑA
Eurosistema

ESTRATEGIAS FRENTE A AMENAZAS TECNOLÓGICAS

Luis E. Pardo Merino
Director de Auditoría Interna

XV REUNIÓN DE AUDITORES INTERNOS DE BANCOS CENTRALES

Santiago de Chile
26 de Septiembre de 2019

AUDITORIA INTERNA

ÍNDICE

1. Gobernanza
2. Medidas de carácter técnico
3. Vigilancia
4. Resiliencia
5. Formación y concienciación
6. Iniciativas gubernamentales

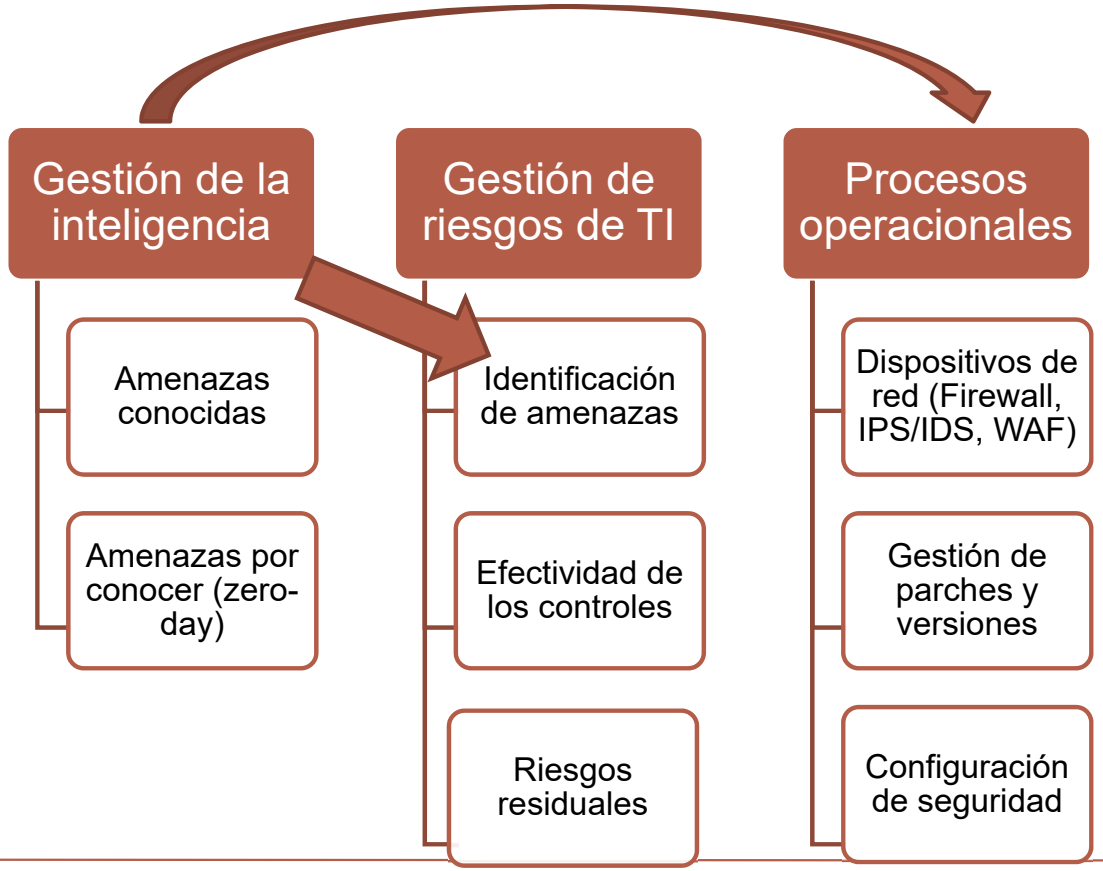
- **Política de seguridad de Tecnologías de la Información (TI) y ciberseguridad**
  - Principios de alto nivel y modelo de gobierno. Modelo de reporte de informes de seguridad.
  - Política de entornos de "servicios en la nube" (cloud services)
- **Definición de funciones y responsabilidades**
  - Segregación de funciones:
    1. *Función de seguridad de los sistemas de información y ciberseguridad.*
    2. *Función de Gestión de Riesgos de Tecnologías de la Información (TI) / Función de Vigilancia de la Seguridad de TI*
  - Implantación de un Centro de Operaciones de Seguridad (SOC)
    - *Monitorización de eventos de seguridad y la gestión de ciberincidentes*
- **Cuerpo normativo de Seguridad de los Sistemas de Información**
- **Clasificación de la información (pública, restringida, confidencial, secreta)**
  - Medidas de protección incrementales
- **Marco de gestión de riesgos de TI**
  - Metodología integral de análisis de riesgos de TI
- **Cuadro de mandos de seguridad de TI**
  - Identificación, definición e implementación de métricas e indicadores

2. MEDIDAS DE CARÁCTER TÉCNICO

BANCO DE ESPAÑA
Eurosistema

- **Inventariado y clasificación de los activos de información: sólo dispositivos y software autorizados**
- **Gestión de Identidades y control de accesos**
  - Autenticación robusta dependiendo de la sensibilidad de la información (MFA).
  - Control sobre identidades y accesos privilegiados.
- **Desarrollo seguro de software**
  - Revisión de código fuente de aplicaciones.
- **Protección antimalware**
- **Seguridad del sistema operativo (actualizaciones)**
- **Prevención de fugas de información**
  - Implantación de herramientas para la protección de documentos y archivos con información sensible frente a accesos no autorizados.
  - Herramientas DLP (Data Loss Prevention) y control de flujos de información sensible
- **Seguridad de red**
  - DMZ y segmentación de redes
- **Seguridad del puesto de usuario**
- **Política de criptografía y cifrado**

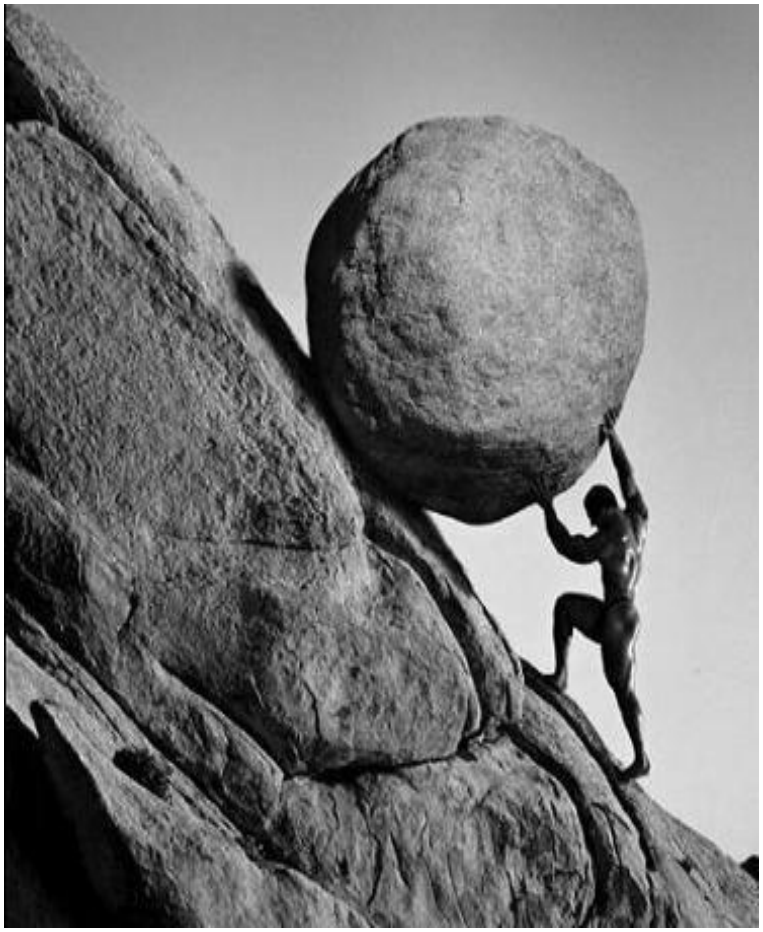
- **Inteligencia de amenazas (Threat Intelligence)**



- Compartir información.
- Participación en foros.
- Automatización de la compartición y la distribución.
- Permite identificar nuevas amenazas

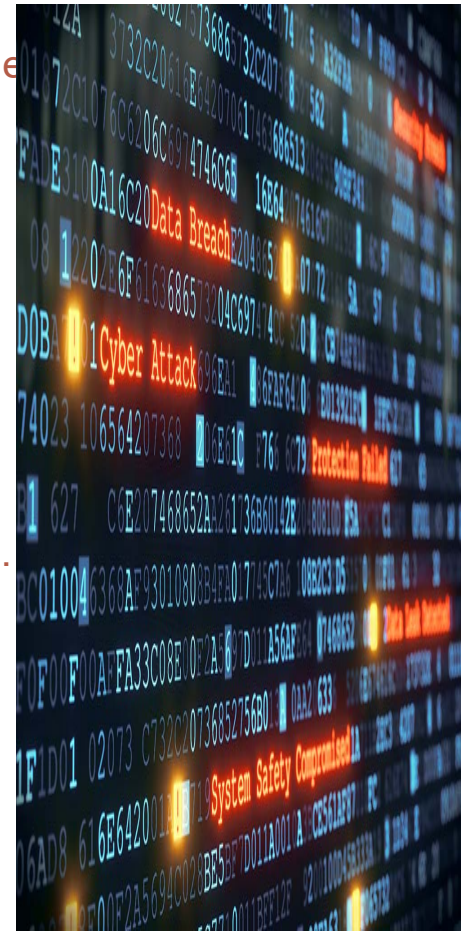
- **Protección de marca**
  - Gestión de cuentas corporativas en redes sociales
- **Gestión de vulnerabilidades**
  - Red Team vs Blue Team
  - Escáner de vulnerabilidades
  - Gestión ágil de parches
- **Gestión de información y eventos de seguridad**
  - Implantación de un Sistema de Gestión de Eventos de Seguridad (SIEM)

- **Pruebas de ciberseguridad**
  - Pruebas de intrusión (Penetration Tests) sobre infraestructuras, aplicaciones y dispositivos.
  - Participación en ciber-ejercicios integrales con otras organizaciones.
- **Respuesta ante incidentes**
  - Priorización de incidentes en función de su impacto
  - Procedimientos de escalado para tipos de ataque
  - Estrategias de contención (aislamiento de equipos infectados)
  - Comunicación interna y externa (CERT/CSIRT)
- **Preparación ante incidentes y crisis**
  - Plan de Gestión de Crisis de Sistemas de Información.
- **Gestión de la continuidad de negocio**
  - Desarrollo de escenarios de ciberataque
  - Definición e implementación del plan de continuidad en escenarios de ciberataque
  - Simulacros de continuidad en escenarios de ciberataque



5. FORMACIÓN Y CONCIENCIACIÓN

- **Implicación de las áreas de negocio**
  - La ciberseguridad **NO** es sólo una responsabilidad del Departamento de Sistemas de Información.
  - Análisis de Criticidad:
    - *Las áreas de negocio son responsables de definir el nivel de criticidad de los sistemas de información de su propiedad.*
    - *Considerando la relevancia de la información procesada y almacenada en función de su confidencialidad, integridad y disponibilidad.*
- **Desarrollo de una cultura de la ciberseguridad**
  - Objetivo: alcanzar el nivel de madurez general adecuado en ciberseguridad.
  - Potenciar la implicación de la alta dirección en la cultura de la seguridad corporativa.
- **Plan de formación y concienciación**
  - Dirigido a todos los empleados
  - Especial atención a la alta dirección (objetivo preferente de los atacantes)
  - Campañas informativas
- **Medición de la eficiencia de la formación y concienciación**
  - Simulaciones de “spear phishing”



- **Directiva NIS de la Unión Europea**
  - Medidas para garantizar un elevado nivel de seguridad común de las redes y sistemas de información de la UE.
  - Cooperación y coordinación

- **Protección de Infraestructuras Críticas**

- **Esquema Nacional de Seguridad (ENS)**
  - Recoge el conjunto de principios básicos y requisitos mínimos requeridos a los sistemas de información del Sector Público.
  - Autoevaluaciones anuales y auditorías independientes cada dos años.

BANCO DE ESPAÑA
Eurosistema

GRACIAS POR SU ATENCIÓN

AUDITORIA INTERNA