BANCO CENTRAL DE COSTA RICA

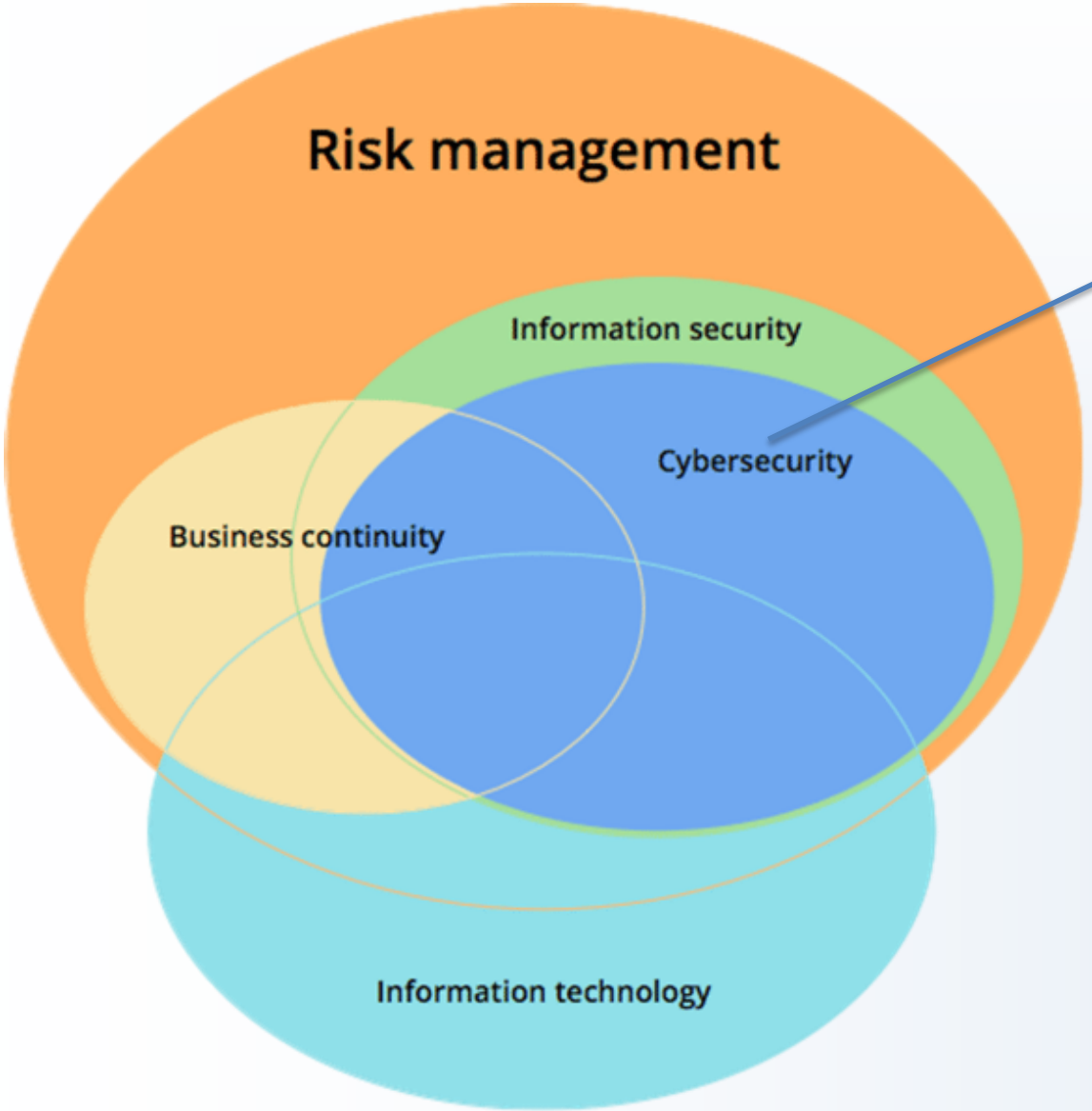
Ciberseguridad y Gestión Documental

Logros y Retos

Miguel Carballo Chavarría - Departamento de Ciberseguridad
División de Servicios Tecnológicos - Banco Central de Costa Rica

San José, Costa Rica
Noviembre, 2022

Ciberseguridad - Seguridad de la Información - Riesgo

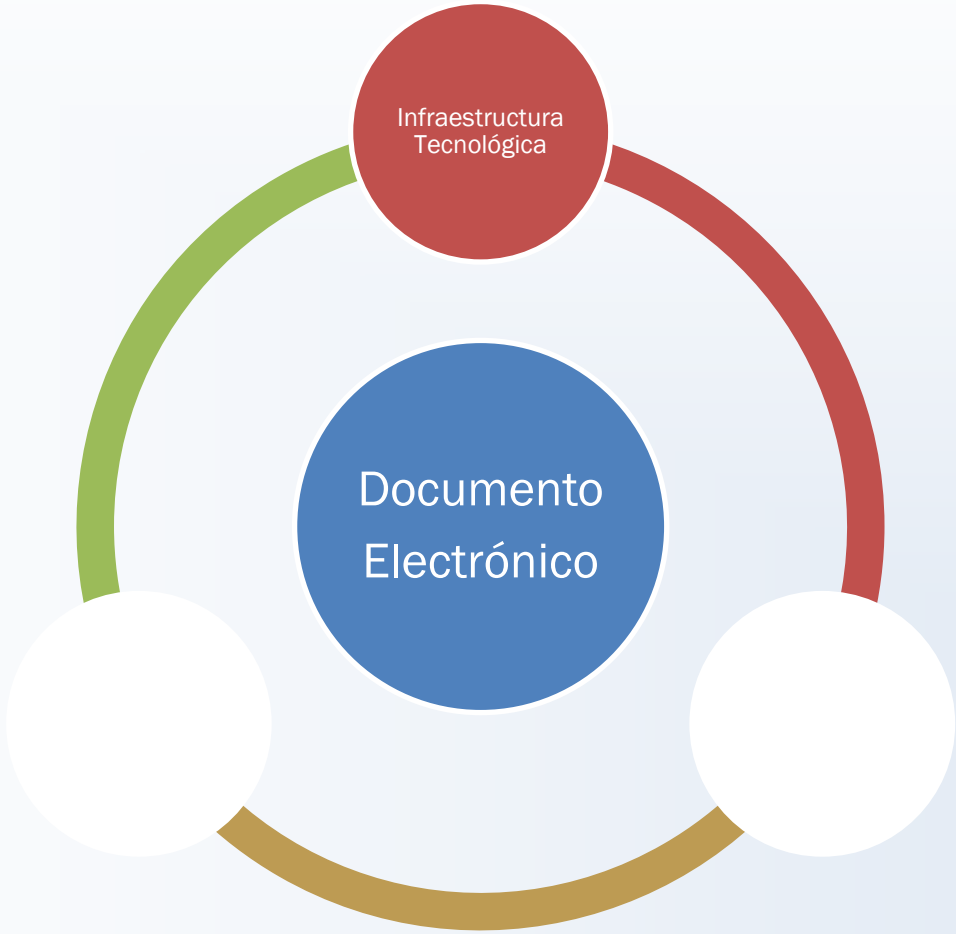


1. Aseguramiento
2. Identidad y Acceso
3. Protección y Control
4. Detección y Respuesta

https://advisera.com/27001academy/blog/2016/10/24/where-does-information-security-fit-into-a-company/

Seguridad de los Documentos Electrónicos

1. Infraestructura Tecnológica



Estándares y Marcos de Referencia

Controles fundamentales y avanzados para la infraestructura tecnológica:

- ✓ ISO 27002: Seguridad de la Información
- ✓ **Verizon: CRP Cyber Risk Program**
- ✓ NIST-CSF: Cybersecurity Framework
- ✓ CIS: Center for Internet Security

Controles Fundamentales para la Infraestructura de T.I.

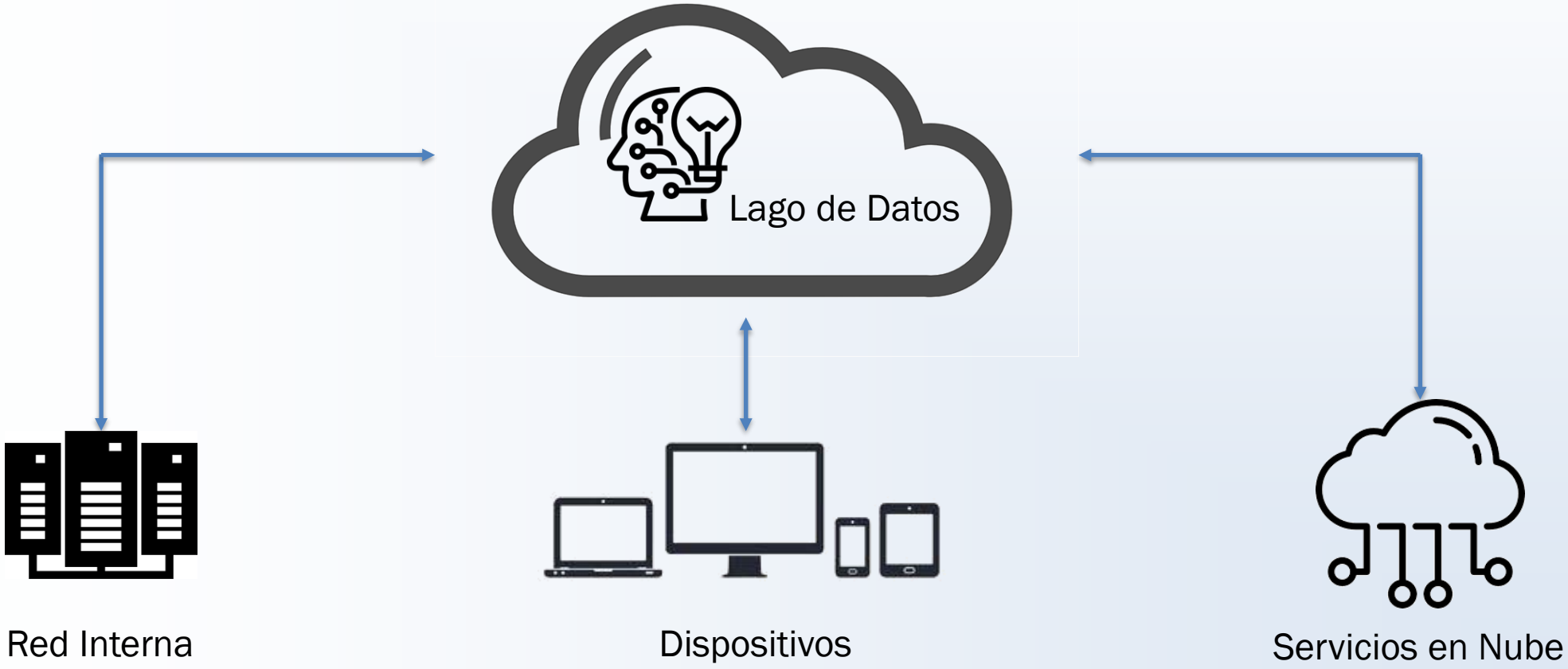
- ✓ Seguridad y segmentación de redes
- ✓ Arquitectura de Alta Disponibilidad
- ✓ Protección ante Ataques de Denegación (DDoS)
- ✓ Soluciones Anti-malware (Antivirus, EDR)
- ✓ Filtro de correo electrónico
- ✓ Filtro de navegación web
- ✓ Gestión de vulnerabilidades tecnológicas
- ✓ Actualizaciones y parches

Controles Avanzados para la Infraestructura de T.I.

- ✓ **Protección avanzada de Aplicaciones Web (WAF)**
  - Equipo especializado de inspección y bloqueo de tráfico malicioso
- ✓ **Control del acceso privilegiado (PAM + EPM)**
  - Estricto control y trazabilidad del acceso para labores de administración técnica, incluyendo grabación de sesiones, Elevación y bloqueo de privilegios por aplicación
- ✓ **Gestión y monitoreo constante de eventos (XDR + SIEM)**
  - Recopilación, correlación y análisis automático de eventos del sistema para monitorear umbrales y comportamiento anómalo
- ✓ **Protección y Auditoría de Bases de Datos (DBF)**
  - Monitoreo y bloqueo de transacciones sospechosas hacia las bases de datos utilizando equipo especializado
- ✓ **Cifrado Avanzado de Datos (Always encrypted + HSM)**
  - Cifrado permanente de la información sensible (utilizando equipo criptográfico especializado) de manera que ni siquiera el personal técnico que administra las bases de datos puede accederla
- ✓ **Infraestructura específica e independiente de telecomunicaciones**
  - Segmentación de la red y aislamiento de equipos

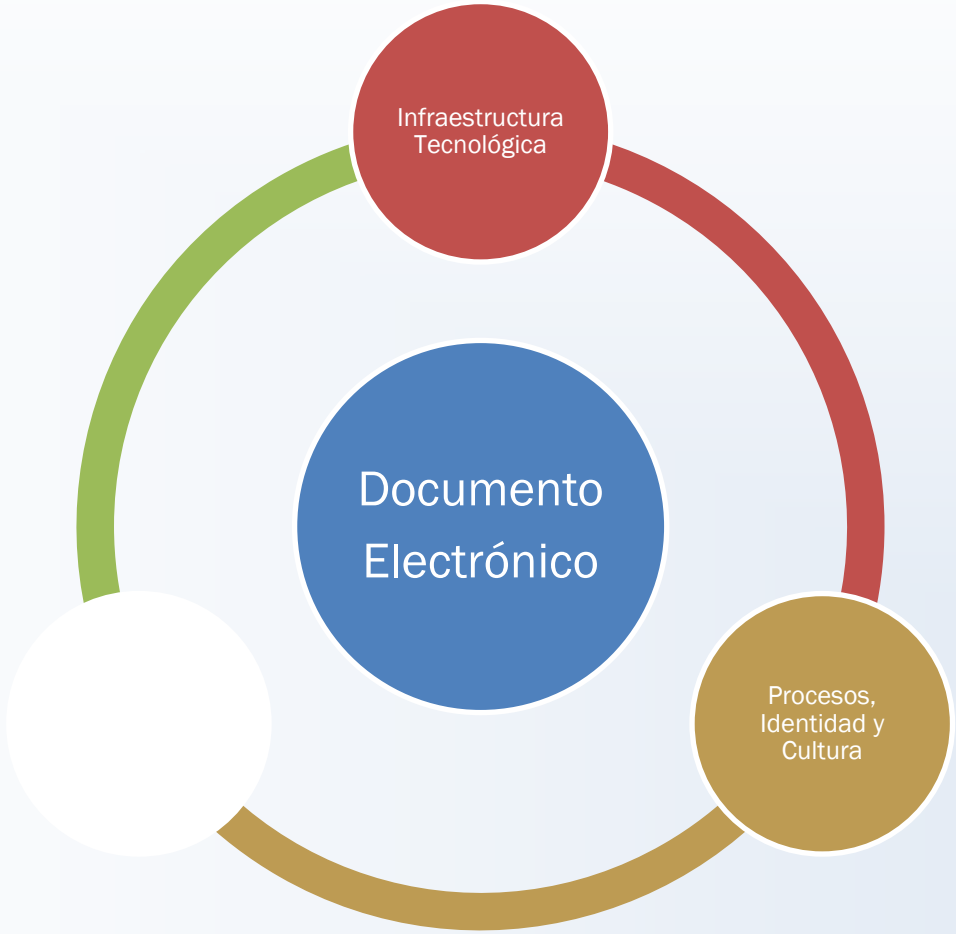
XDR – Detección y Respuesta

Servicios de análisis integral de datos para detección y respuesta

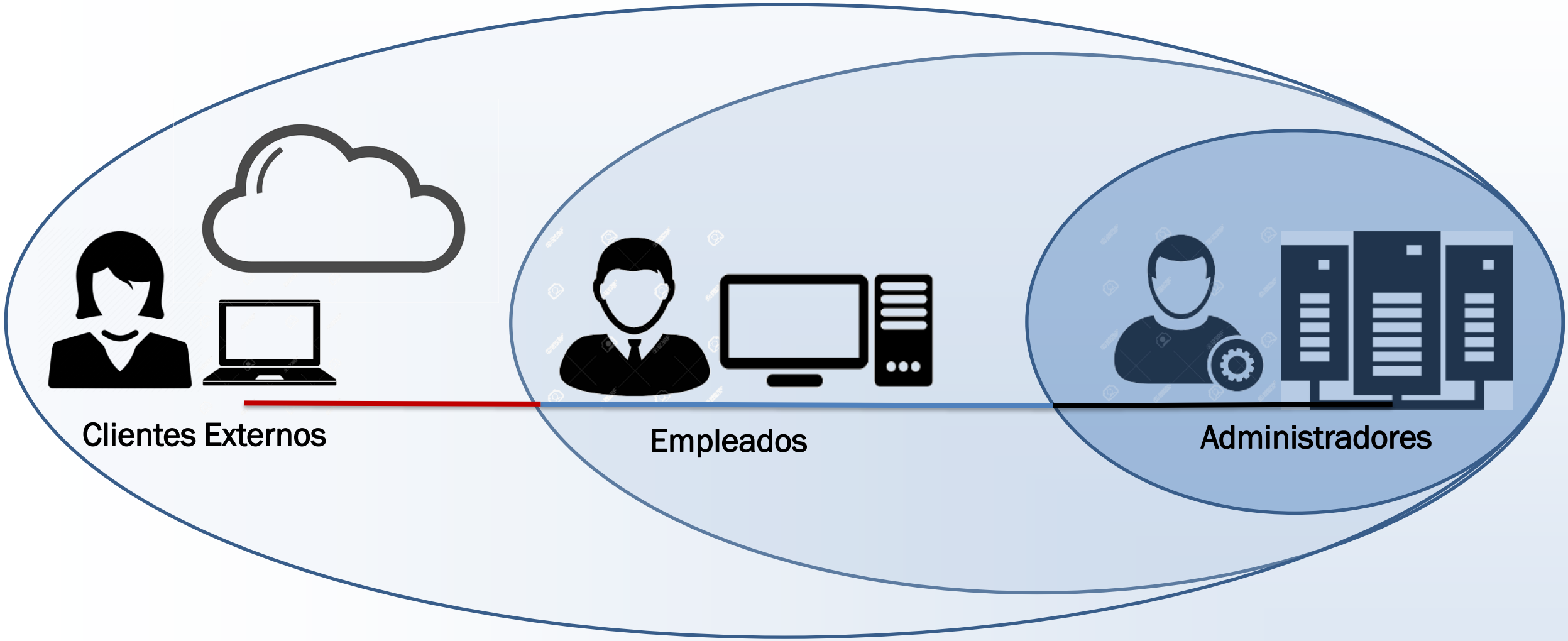


Seguridad de los Documentos Electrónicos

2. Procesos, Identidad y Cultura



Escenario Anterior



Escenario Actual

Clientes Externos

Empleados

Administradores

SaaS

La identidad es el nuevo perímetro

Programa de Concientización

Fortalecimiento y verificación del nivel de cultura en Ciberseguridad

- Curso Virtual para Funcionarios
- Charlas sobre temas relevantes
- Comunicados y boletines informativos
- Phishing Test – Verificación de cultura

Tendencia al click (Phish-Prone):
11,6% Institucional
5,5% Certificación

Controles Relacionados con la Gestión de Procesos

- ✓ Revisión continua de roles y permisos
- ✓ Identificación de Activos de Información Crítica
- ✓ Etiquetado de información
- ✓ Actividades de control, aprobación, supervisión
- ✓ Proceso de Continuidad de Negocio
- ✓ Gestión de Riesgo de los Procesos

Seguridad de los Documentos Electrónicos

3. Controles Inherentes al Documento

Firma Digital

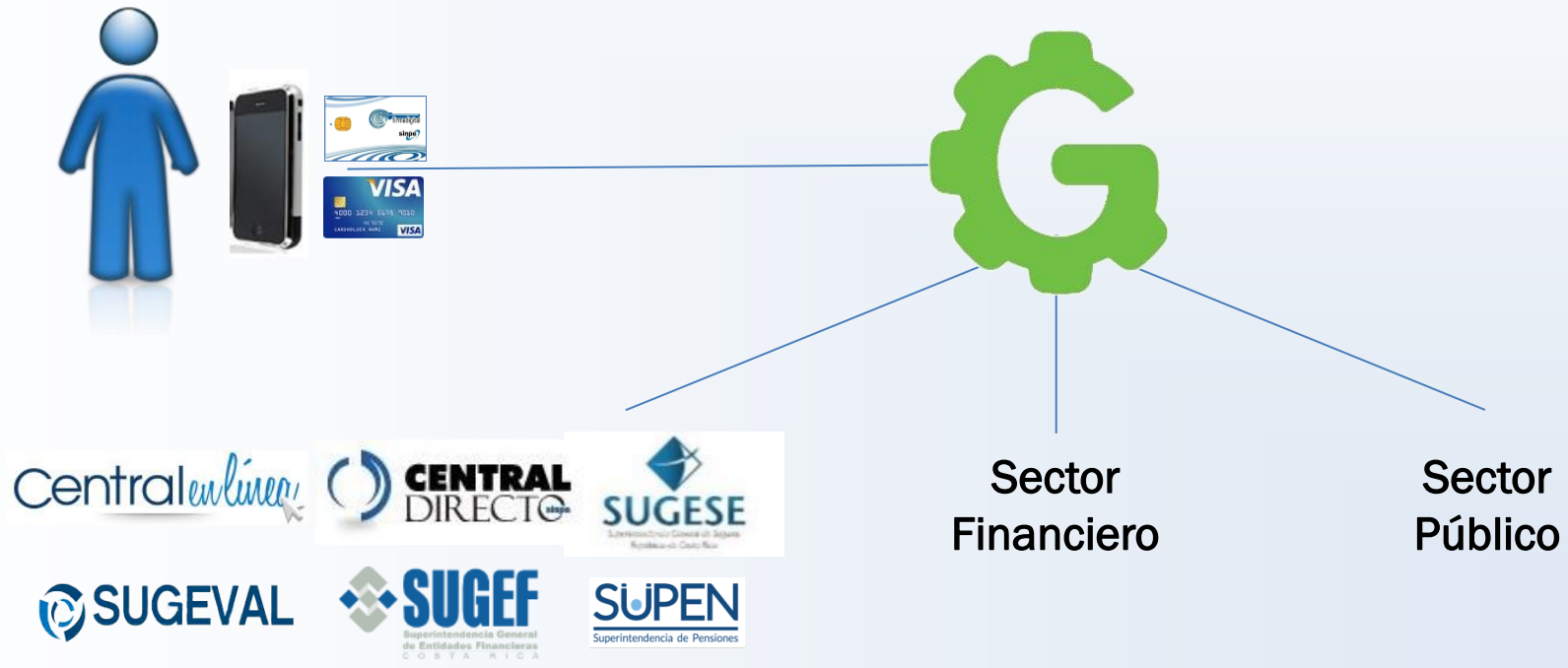
Ley 8454 – Certificados, Firmas Digitales y Documentos Electrónicos

- ✓ Identidad Digital y Firma Digital
- ✓ Mecanismo de Autenticación Robusta
- ✓ Equivalencia funcional con la firma autógrafa
- ✓ Compromiso jurídico en medios electrónicos
- ✓ Garantía de Integridad y Autenticidad
- ✓ No Repudio

Gaudí – Banco Central de Costa Rica

Gaudí – Gestor de Autenticación y Firma Digital

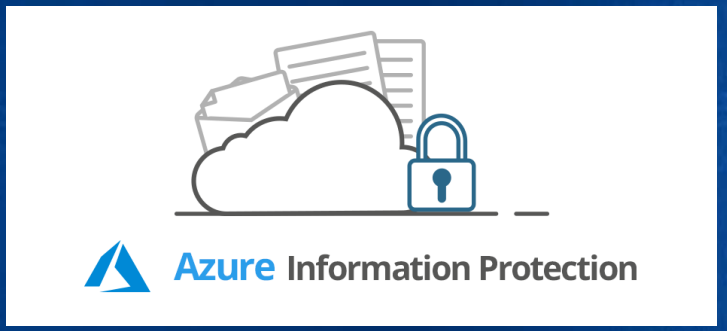
- ✓ Servicio central de identidad digital y firma digital (alcance país)
- ✓ Robustez técnica que sustenta el compromiso jurídico en medios electrónicos

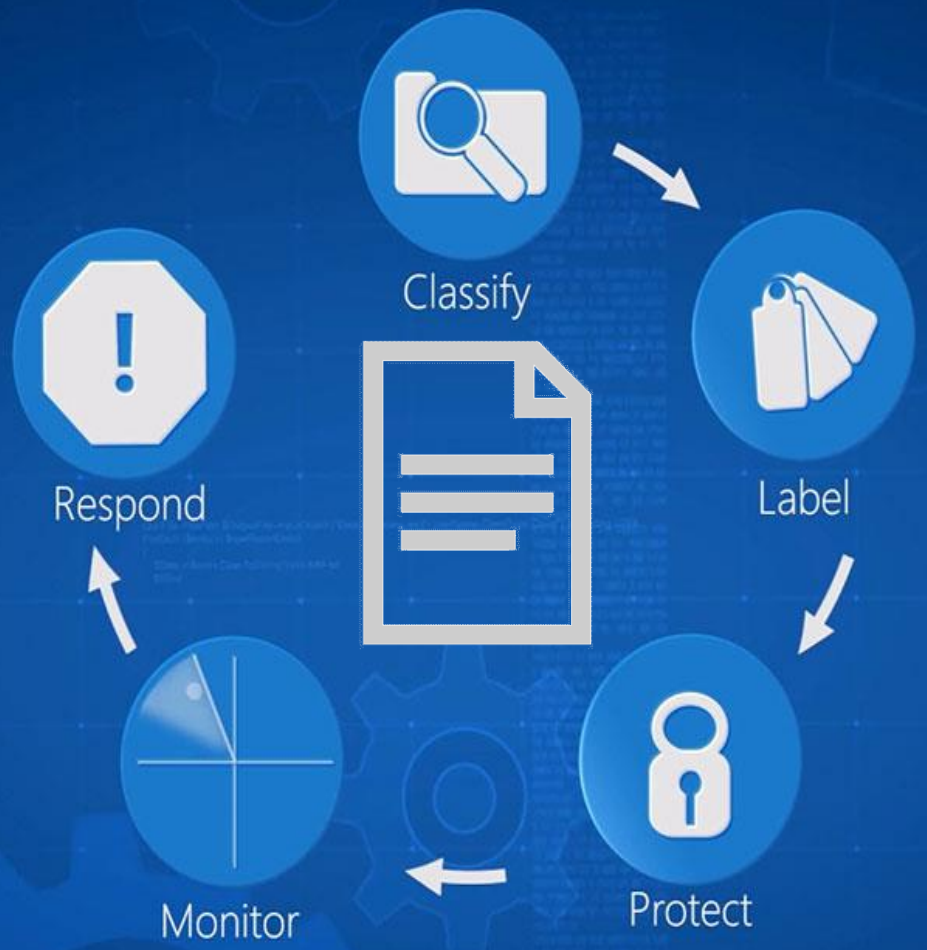


Etiquetado y Protección Activa de Documentos Electrónicos

Etiquetas de Sensibilidad – MS AIP

- ✓ Protección implementada en el documento
- ✓ Capacidad de cifrado del contenido
- ✓ Protección de la Confidencialidad
- ✓ Capacidad de monitoreo y respuesta





Protection Process

Seguridad de los Documentos Electrónicos

¿Cómo sabemos si estamos bien?

Certificación de Seguridad

- ✓ **VERIZON**
  - Líder mundial en servicios de ciberseguridad
  - Certificación de reconocimiento internacional en sector finanzas, gov, salud
  - Auditores certificados, centro de investigación, servicio de alertas

- ✓ **Las certificaciones de Verizon son utilizadas y reconocidas en los siguientes sectores:**
  - **Sector Financiero**: Hardland Clarke, D+H, Fieldprint
  - **Sector Gobierno**: Colorado, Nebraska, Kansas, Virginia (FairFax County)
  - **Sector Seguros**: Liberty Mutual, NYCM Insurance, Cigna

- ✓ **Certificación obtenida a partir del 2007**
- ✓ **Alcance actual:** SINPE, Central Directo, Firma Digital, GAP y RTBF

- ✓ **Servicios críticos identificados por los negocios**
  - Valoración general de políticas, factor humano, ambiente físico, dispositivos, redes.

- ✓ **Impacto positivo y atención de hallazgos en toda la infraestructura tecnológica**

Verizon Cybertrust Security | CERTIFIED ENTERPRISE

verizon

Verizon - Cyber Risk Program

CRP: Nuevo programa basado en riesgo tecnológico

Assessment	
External Vulnerability Assessment (EVA)	Valoración de vulnerabilidades **desde Internet**
Firewall Assessment(FWA)	Valoración de vulnerabilidades en la **red interna**
Web Application Assessment (WAS)	Valoración de vulnerabilidades en las **aplicaciones web**
IP Reputational Assessment (IPA)	Valoración de la **reputación** en Internet
Netflow Assessment (NFA)	Valoración del **tráfico institucional** en Internet
Internal Vulnerability Assessment (IVA - DMZ)	Valoración de vulnerabilidades en la **red de salida**
Internal Vulnerability Assessment (IVA - LAN)	Valoración de vulnerabilidades en la **red interna**
Email Filter Check Assessment (EFC)	Valoración de filtro de **correo electrónico**
Endpoint Risk Assessment (EPA)	Valoración de los equipos – **computadores y servidores**
Phishing Assessment (PHA)	Valoración del riesgo de **phishing**
Physical Assessment (PA)	Valoración del riesgo de **acceso físico**
Wireless Assessment (WA)	Valoración de las **redes inalámbricas**
Policy, Process and Procedures Assessment (PPP)	Valoración de **políticas, procesos, procedimientos**

Verizon - Cyber Risk Program

CRP: Nuevo programa basado en riesgo tecnológico

Para efectos de cálculo de la calificación general los valores de riesgo son truncados (puntuación de riesgo)
Actualmente se utiliza el valor promedio de riesgo de la Institución

Resultados

Evaluación de Vulnerabilidades Externa	Evaluación del Firewall	Evaluación de aplicaciones web	Evaluación de vulnerabilidades DMZ	Evaluación de vulnerabilidades interna
Bajo	Bajo	Bajo	Moderado	Moderado
Rango de riesgo 1.00 (Línea base)	Rango de riesgo 1.96 (Línea base)	Puntuación de Rango del Riesgo 1.00 (Disminución)	Rango de riesgo 2.37 (Línea base)	Rango de riesgo 2.92 (Línea base)

Evaluación de Endpoints	Physical Assessment	Wireless Assessment
Moderado	Low	Low
Rango de riesgo 2.17 (Línea base)	Risk Range Score 1.75 (Baseline)	Risk Range Score 1.87 (Baseline)

Nivel de Riesgo	Rango de Riesgo	Puntuación de Riesgo
Muy Alto	≥5.00	5
Alto	4.00 a 4.99	4
Alto Moderado	3.00 a 3.99	3
Moderado	2.00 a 2.99	2
Bajo	≤1.99	1

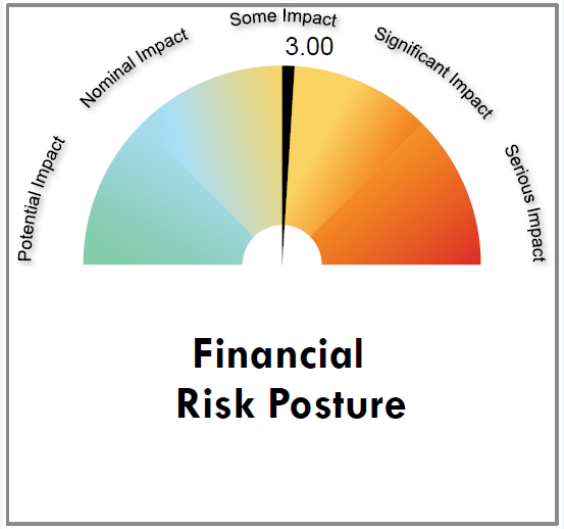
Verizon - Cyber Risk Program

CRP: Calificación general referenciada al sector financiero

Postura General de Riesgo: Valoración del riesgo potencial de explotación o brecha según la industria relacionada

Overall Risk Posture – Reality of Potential Exploit or Breach

The Overall Risk Posture is a portrayal of the risk and potential of a breach that has been identified from the 12 Cyber Risk Program assessments. Information is then aggregated based on the Verizon Data Breach Investigation report to show the organization's overall posture to a data breach based on the industry vertical.



Nivel de Riesgo	Rango de Riesgo	Puntuación de Riesgo
Muy Alto	≥5.00	5
Alto	4.00 a 4.99	4
Alto Moderado	3.00 a 3.99	3
Moderado	2.00 a 2.99	2
Bajo	≤1.99	1

Calificación = **94,5%**

Ciberseguridad
Principales Retos

- Contratación, formación y retención de personal calificado
- Certificación de alcance Institucional
- Extensión y coordinación con sectores asociados
- Implementación de controles y prácticas de siguiente generación

Aporte de la Ciberseguridad a la Gestión Documental:

Buenas prácticas, controles y herramientas tecnológicas

BANCO CENTRAL DE COSTA RICA

Ciberseguridad y Gestión Documental

¿Preguntas?

San José, Costa Rica
Noviembre, 2022