CyberRisk 360: “Framework, controles, indicadores para una gestión efectiva de las Amenazas Cibernéticas”

Ing. Andrea Vera

Por qué un Framework 360?

Automatización
Agilidad en la ejecución de análisis de ciberseguridad.

Integración
Toda la información de controles de las distintas normativas, indicadores y amenazas desde un mismo software.

Visibilidad
Rapidez en la visualización del nivel de riesgo de ciberamenazas.

Trazabilidad
Seguimiento histórico disponible de manera permanente.

Componentes del Framework (1/2)

1 Inventario de Controles(SGSI)

2 Indicadores críticos Ciberseguridad

Mean Time To Attend & Analysis (MTTA&A) - *Minutes* ODM NX1	Mean Time To Remediate (MTTR) - *Hours* ODM NX2	Third Party Continuity Testing ODM NX3	Third-Party Cyber-Risk Engagement ODM NX4	Unassessed Third Parties ODM NX5
Discovered Cyber-Physical Systems ODM NX6	Endpoint Protection Coverage ODM NX7	OS Patching Time (Standard) ODM NX8	Ransomware Downtime and Workarounds ODM NX9	Ransomware Recovery (Mission-Critical) ODM NX10
Multifactor Authentication Coverage ODM NX11	Access Removal Time ODM NX12	Privileged Access Management (PAM) Coverage ODM NX13	Privileged Account Hygiene ODM NX14	Secure Software Development ODM NX15
Phishing Reporting Rates ODM NX16	Phishing Click-Throughs ODM NX17	Security Awareness Training ODM NX18	Cloud Security Coverage ODM NX19	Cloud Run - Time Visibility ODM NX20
Shadow IT ODM NX21	Expired Policy Exceptions ODM NX22	Technology Debt ODM NX23	Unassessed Gen AI Use-Cases ODM NX24	Data Classification Coverage ODM NX25
SGSI level: 3 ★★★ (Implantado / definido) ✔	SGSI level: 2 ★★ (Repetible o administrado)	SGSI level: 1 ★ (Inicial)	Application Vulnerabilities MTTR (Critical Threats) ODM NX26	Authorization Layer Maturity ODM NX27

Integración de Controles de diferentes Normativas y estándares como ISO 27001, PCI DSS, SOX, NIST, etc.

27 Indicadores estratégicos que garantizan la efectividad de los controles SGSI

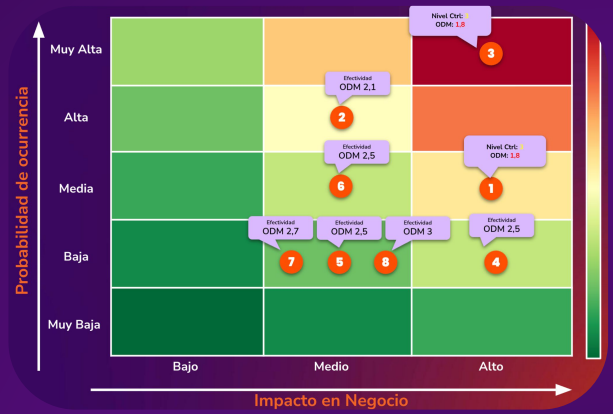
Componentes del Framework (2/2)

3 Amenazas críticas

AMENAZAS	RIESGO RESIDUAL
Cloud Security (Seguridad en la Nube)	Moderado
Compliance (Cumplimiento Normativo)	Significativo
Data Loss (Pérdida de Datos)	Intolerables
Denegación de Servicio (DDoS)	Moderado
Incident & Response (Capacidad de Respuesta a Incidentes)	Moderado
Insider Risk (Riesgo Interno)	Significativo
IoT/OT/ICS Security (Seguridad en Dispositivos Conectados)	Moderado
Ransomware/Malware	Moderado
Social Engineering (Ingeniería Social)	Tolerable/Bajo
Talent (Escasez de Talento)	Tolerable/Bajo
Tech Debt (Deuda Técnica)	Tolerable/Bajo
Third-Party Risk (Riesgo de Terceros)	Intolerables
Vulnerability Management (Gestión de Vulnerabilidades)	Moderado
Accesos no autorizados	Tolerable/Bajo

14 amenazas críticas

Nivel de riesgo residual en amenazas CRÍTICAS

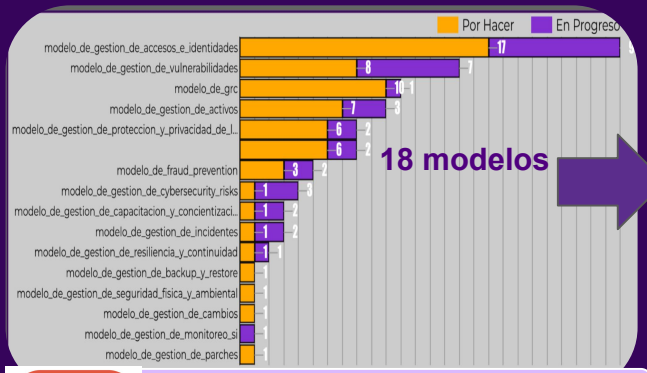


*Aumentar la madurez de controles SGSI, **reduce el nivel de riesgo** residual a amenazas críticas*

SGSI - Sistema de Gestión de Seguridad de la Información

Confidencialidad | **Integridad** | **Disponibilidad**

Modelos | **Políticas** | **Procedimientos** | **Controles** | **Metricas / ODMs**



New! 18. Modelo de Gestión de Inteligencia Artificial

Política de Control de Acceso

- **Procedimiento de ABM de Cuentas Privilegiadas**
  - **Control 1 -Accesos** → **ODM 1**
  - **Control 2 -Accesos** → **ODM 2**
- **Procedimiento de ABM de Cuentas Privilegiadas**
  - **Control N -Accesos** → **ODM N**

Un **control** se implementa para **reducir riesgos.**

Una **métrica** es un **indicador cuantitativo** que mide el desempeño, la efectividad o la eficiencia de un proceso, control.

Riesgos de Amenazas

Riesgo Amenazas = ((Nivel Ideal − Nivel Actual) × Probabilidad × Impacto) × (2 − Efectividad Métrica / ODM)

Vemos el framework automatizado

Muchas gracias!

Ing. Andrea Vera