UNIVERSIDAD MARIANO GÁLVEZ DE GUATEMALA

FACULTAD DE INGENIERÍA EN SISTEMAS DE INFORMACIÓN

PROGRAMA DE POSGRADOS

JM-104-2021

Autor:

Guerrero Hernandez, Diego Guerrero – dguerreroh@miumg.edu.gt

Profesor

Evelyn Yesenia Lobos Barrera

Curso

Marco legal y regulatorio – Tercer Trimestre - 2025

Guatemala, junio 2025

1) Implementación JM-104 y NIST CSF 2.0

Capítulo JM-104-2021	Resultado que debes lograr	NIST CSF 2.0
II. Organización para la administración del riesgo tecnológico	Política y apetito de riesgo TI aprobados por Junta; roles (CISO), comités, manual y métricas	GV para estrategia/roles; ID.RA (evaluación de riesgo)
III. Infraestructura, SI, BD y servicios TI	Inventario/CMDB, segmentación, WAF/IDS/IPS, obsolescencia y soporte	ID.AM (activos), PR.PT/PR.AC (protección técnica/acceso), DE.CM (monitoreo)
IV. Seguridad de TI	Clasificación de información, controles físicos/lógicos, respaldos, SIEM	PR.DS/PR.AC/PR.IP/PR.MA, DE.CM
V. Ciberseguridad	Gestión de vulnerabilidades, pruebas, SOC/Use-Cases, hardening	PR.IP/DE.CM, RS.MI (mitigación)
VI. DRP	BIA, RTO/RPO, sitio alterno, pruebas y mejora	RC.RP/RC.IM (recuperación y mejora)
VII. Procesamiento/almacenamiento de información	Protección de datos en tránsito/ reposo, retención/depuración	PR.DS/PR.IP

2) Esfuerzos actuales

- MFA, hardening y segmentación con evidencias para PR.AC, PR.PT
- SIEM, casos de uso con alertas y DE.CM (monitoreo)
- Gestión de parches y vulnerabilidades con PR.IP/RS.MI, obliga a llevar bitácoras y reportes a comité.
- DRP con RTO/RPO definidos con RC.RP/RC.IM
- Gobernanza de ciber (comité, CISO, métricas) y GV función nueva en CSF

3) Cómo evitar duplicar esfuerzos

- Catálogo único de controles, usar los resultados del CSF 2.0 y mapear cada control a los artículos/capítulos de JM-104 (un control y varias evidencias).
- Perfil de comunidad, documentar “perfil bancario-JM104” para que proyectos/áreas reusen el mismo conjunto mínimo de controles.
- Repositorio de evidencias (GRC/Confluence/Drive): política, diagrama, acta y registro una sola vez y referencia cruzada.
- RACI por resultados (GV, ID, PR, DE, RS, RC): evita que TI, Riesgos y Seguridad repitan tareas. nvlpubs.nist.gov
- Métricas/KRIs integradas al tablero del comité, miden resultados del CSF y demuestran cumplimiento normativo

4) Cambios “grandes” a priorizar

1. Aprobación de alto nivel: Política de Riesgo Tecnológico firmados por Junta directiva y calendario de reportes.
2. Manual de Riesgo Tecnológico con procedimientos (operativos y de evidencias) alineados a CSF.
3. Inventario (CMDB) de activos/servicios/datos con criticidad y dueños.
4. Gestión de vulnerabilidades con SLA por criticidad y pruebas periódicas.
5. SOC/Use-Cases orientados a riesgos del negocio
6. DRP probado (BIA→RTO/RPO→pruebas→mejoras) y sitio alterno.
7. Terceros: due diligence y cláusulas de ciber en contratos.

5) Hoja de ruta 90 días (mínimo viable de cumplimiento)

- Días 0–30 (Gobernanza & Alcance): aprobar política y apetito, definir RACI y levantar perfil JM-104.
- Días 31–60 (Controles base): CMDB e inventarios críticos, MFA/segregación, SOPs de backup/restauración, catálogo de casos de uso SIEM, proceso de parches con SLA.
- Días 61–90 (Prueba & Demostración): simulacro de incidente y post-mortem, prueba de DRP con RTO/RPO, informe de avance al Comité/Junta con KPIs