Función	Categoría	Subcategoría	Madurez subcat.	Madurez promedio
			Nivel	
TIF IC	**Gestión de Activos (ID.GA.)** Los datos, personal, dispositivos, sistemas e instalaciones que permiten a la organización alcanzar sus objetivos de negocio, se identifican y gestionan según su importancia relativa	ID.GA-1. Los dispositivos físicos y los sistemas de la organización están inventariados	2	0,5
		ID.GA-2. Las plataformas de software y las aplicaciones de la organización están inventariadas	0	
		ID.GA-3. Está mapeada toda la comunicación y los flujos de datos que existen dentro de la organización	0	
		ID.GA-4. Los sistemas externos de información que se utilizan en la organización están identificados y catalogados	0	
		ID.GA-5. Los activos (hardware, dispositivos, datos, tiempo, personal y software) se priorizan en base a su clasificación, criticidad y valor para el negocio	1	
		ID.GA-6. Están establecidos los roles y responsabilidades de ciberseguridad para todo el personal y terceros (proveedores, clientes, socios)	0	
	Ambiente del negocio (ID.AN.) La misión de la organización, sus objetivos, interesados y actividades son comprendidos y priorizados; esta información es utilizada para apoyar la toma de decisiones sobre roles,	ID.AN-1. El rol de la organización en la cadena global de suministros está identificado y es comunicado		1,3
		ID.AN-2. El lugar que ocupa la organización en la infraestructura crítica y en su sector de industria está identificado y es comunicado		
		ID.AN-3. Se han establecido y se comunican las prioridades para la misión de la organización, sus objetivos y actividades	1	
		ID.AN-4. Se han definido las dependencias y funciones críticas para la entrega de los servicios críticos	0	
		ID.AN-5. Se han establecido los requerimientos de resiliencia para soportar la entrega de los servicios críticos en cualquier situación operativa (bajo presión o ataque, en recuperación o en normalidad)	3	
	Gobernanza (ID.GO.) Las políticas, procedimientos y procesos para gestionar y monitorear los requisitos regulatorios, legales, ambientales y operativos de la organización, son comprendidos y la gestión	ID.GO-1. La política de seguridad de la información está establecida y es comunicada	2	0,5
		ID.GO-2. Los roles y las responsabilidades de ciberseguridad están coordinados y se alinean con roles internos y socios externos	0	
		ID.GO-3. Los requisitos legales y regulatorios sobre la ciberseguridad, incluyendo las obligaciones de privacidad y las libertades civiles son comprendidos y se gestionan	0	
		ID.GO-4. Los procesos de gobernanza y gestión del riesgo toman en consideración los riesgos de ciberseguridad	0	
	Evaluación de Riesgos (ID.ER.) La organización comprende cuales son los riegos de ciberseguridad que enfrentan sus operaciones (incluyendo misión, funciones, imagen o reputación), activos e individuos.	ID.ER-1. Se identifican y documentan las vulnerabilidades de los activos	2	1,0
		ID.ER-2. Se recibe de parte de grupos, foros y fuentes especializadas, información e inteligencia sobre ciberamenazas	1	
		ID.ER-3. Se identifican y documentan las amenazas, tanto internas como externas	1	
		ID.ER-4. Se han identificado los impactos potenciales sobre el negocio y sus probabilidades de ocurrencia	0	
		ID.ER-5. Las amenazas, vulnerabilidades, probabilidad de ocurrencia e impactos, se utilizan para determinar el riesgo	0	
		ID.ER-6. Se han identificado y priorizado las respuestas ante los riesgos	2	
	Estrategia de gestión de riesgos (ID. GR.) Se establecen las prioridades, restricciones, tolerancia al	ID.GR-1. Los procesos de gestión de riesgos están establecidos, son gestionados y son aprobados por todos los interesados de la organización	1	0,7
		ID.GR-2. La tolerancia de la organización ante el riesgo está determinada y claramente expresada	1	
		ID.GR-3. La tolerancia de la organización ante el riesgo considera su rol dentro de la infraestructura crítica así como la evaluación de riesgos específicos del sector al que pertenece.	0	
	Gestión del riesgo en la cadena de suministros (ID.CS.) Las prioridades, restricciones, tolerancia al riesgo y supuestos	ID.CS-1. Los procesos de gestión del riesgo de la cibercadena de suministros están identificados, establecidos, evaluados, gestionados y acordados por todas las partes interesadas de la organización.	0	0,8
		ID.CS-2. Los proveedores de sistemas, componentes y servicios de información así como también otros terceros vinculados, están identificados y priorizados y son evaluados mediante un proceso de evaluación del riesgo en la cibercadena de suministros.	3	
		ID.CS-3. Se utilizan los contratos con proveedores y otros terceros vinculados, para implementar medidas apropiadas destinadas a cumplir con los objetivos del programa de ciberseguridad de la organización y con su plan de gestión de riesgos en la cibercadena de suministros.	1	

		ID.CS-4. Los proveedores y otros terceros vinculados son evaluados rutinariamente mediante auditorías, resultados de pruebas u otras formas de evaluación, para confirmar que están en cumplimiento de sus obligaciones contractuales.	**0**	
		ID.CS-5. Las pruebas de los planes de respuesta y recuperación involucran a proveedores y otros terceros vinculados.	**0**	
EG ER	**Gestión de Identidad, Autenticación y Control de Acceso (PR.CA.)** El acceso a los activos físicos y lógicos e instalaciones	PR.CA-1. Las identidades y credenciales para usuarios, dispositivos y procesos autorizados son creadas, gestionadas, verificadas, revocadas y auditadas.	**1**	0,4
		PR.CA-2. Se gestiona y protege el acceso físico a los activos.	**2**	
		PR.CA-3. Se gestiona el acceso remoto.	**0**	
		PR.CA-4. Los permisos de acceso y las autorizaciones son gestionados, incorporando los principios de menor privilegio y segregación de funciones.	**0**	
		PR.CA-5. Se protege la integridad de la red aplicando segregación y segmentación cuando es apropiado	**0**	
		PR.CA-6. Las identidades son verificadas y vinculadas a las credenciales, y se les reconfirma durante las interacciones.	**0**	
		PR.CA-7. Los usuarios, dispositivos y demás activos son autenticados de forma acorde (uno o más factores) al riesgo de la transacción (seguridad y riesgos de privacidad del individuo y otros riesgos organizacionales).	**0**	
	Concientización y formación (PR.CF.) El personal de la organización y socios de negocios, reciben entrenamiento y concientización sobre ciberseguridad. Están adecuadamente entrenados para cumplir con sus obligaciones	PR.CF-1. Todos los usuarios están entrenados e informados	**1**	1,2
		PR.CF-2. Los usuarios privilegiados comprenden sus roles y responsabilidades	**4**	
		PR.CF-3. Interesados externos (proveedores, clientes, socios) comprenden sus roles y responsabilidades	**0**	
		PR.CF-4. La gerencia ejecutiva comprende sus roles y responsabilidades	**0**	
		PR.CF-5. El personal de seguridad física y de ciberseguridad comprende sus roles y responsabilidades	**1**	
	Seguridad de los datos (PR.SD.) La información y los registros (datos) se gestionan de acuerdo con la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	PR.SD-1. Los datos en reposo se encuentran protegidos	**1**	0,1
		PR.SD-2. Los datos en tránsito se encuentran protegidos	**0**	
		PR.SD-3. Los activos se manejan formalmente durante su retiro de servicio, transferencia o eliminación definitiva	**0**	
		PR.SD-4. Se mantiene una adecuada capacidad para asegurar la disponibilidad	**0**	
		PR.SD-5. Se implementan medidas de protección contra fuga de datos	**0**	
		PR.SD-6. Se realizan chequeos de integridad para verificar software, firmware e integridad de la información	**0**	
		PR.SD-7. Los entornos de desarrollo y pruebas están separados del entorno de producción	**0**	
		PR.SD-8. Se utilizan mecanismos de verificación de integridad sobre el hardware.	**0**	
	Procesos y procedimientos para la protección de la información (PR.PI.) Las políticas (con propósito, alcance, roles, responsabilidades,	PR.PI-1. Existe una configuración básica para los sistemas de información y de control industrial, la misma es mantenida e incorpora principios de seguridad (concepto de mínima funcionalidad).	**0**	1,0
		PR.PI-2. Se implementa un ciclo de vida de desarrollo para gestionar los sistemas	**0**	
		PR.PI-3. Existen procesos de gestión del cambio para las configuraciones	**1**	
		PR.PI-4. Se realizan y mantienen respaldos de la información y se les verifica regularmente	**4**	
		PR.PI-5. Se cumple con las políticas y reglamentaciones relacionadas con el medio ambiente físico operativo de los activos de la organización.	**0**	
		PR.PI-6. Los datos son eliminados de acuerdo a las políticas de seguridad	**0**	

		PR.PI-7. Existe una mejora continua para los procesos de protección.	0	
		PR.PI-8. La eficacia de las tecnologías de protección se comparte con las partes apropiadas	0	
		PR.PI-9. Existen y se gestionan planes de respuesta a incidentes (Respuesta a Incidentes y Continuidad del Negocio) y planes de recuperación (Recuperación de incidentes y Recuperación de Desastres)	4	
		PR.PI-10. Los planes de respuesta y recuperación se testean regularmente	2	
		PR.PI-11. La ciberseguridad está considerada en las prácticas de RRHH (desvinculaciones, revisión de antecedentes).	0	
		PR.PI-12. Existe un plan de gestión de vulnerabilidades	1	
	Mantenimiento (PR.MA.) El mantenimiento y las reparaciones de los componentes de los sistemas de información y de control industrial (si los hay) se llevan a cabo en consonancia con las políticas y	PR.MA-1. El mantenimiento y las reparaciones de los activos de la organización se llevan a cabo y es registrado en forma oportuna con herramientas aprobadas y controladas	2	1,0
		PR.MA-2. El mantenimiento a distancia de los activos de la organización se aprueba, registra y lleva a cabo de forma tal que se impide el acceso no autorizado	0	
	Tecnología de protección (PR.TP.) Las soluciones técnicas de seguridad se gestionan para garantizar la seguridad y resistencia de los sistemas y activos de la organización, en consonancia con las políticas,	PR.TP-1. Los registros de auditoría (logs) están determinados, se documentan, implementan, y se revisan de acuerdo con la política	0	0,6
		PR.TP-2. Los medios extraíbles se encuentran protegidos y se restringe su uso de acuerdo con las políticas	0	
		PR.TP-3. Se incorpora el principio de mínima funcionalidad mediante la configuración de los sistemas de modo que brinden únicamente sus funciones esenciales	1	
		PR.TP-4. Las redes de comunicaciones y control se encuentran protegidas	2	
		PR.TP-5. Se implementan mecanismos (falla segura, balanceo de carga, hot swap) para cumplir con los requerimientos de resiliencia, tanto en casos de normalidad como en situaciones adversas.	0	
CT AR	**Anomalías y eventos (DE.AE.)** La actividad anómala se detecta de forma oportuna y es claramente comprendido por la organización el potencial impacto de los eventos.	DE.AE-1. Se establece y gestiona una línea base esperada de operaciones de red y flujos de datos tanto para usuarios como para sistemas	0	0,0
		DE.AE-2. Los eventos detectados son analizados para entender los objetivos y los métodos de ataque	0	
		DE.AE-3. Se recopilan y correlacionan datos de eventos provenientes de múltiples fuentes y sensores	0	
		DE.AE-4. Se determina el impacto de los eventos	0	
		DE.AE-5. Se establecen los umbrales de alerta de incidentes	0	
	Monitoreo continuo de la seguridad (DE.MC.) Los sistemas y activos de información son monitoreados para	DE.MC-1. Se monitorea la red para detectar potenciales eventos de ciberseguridad	0	1,3
		DE.MC-2. Se monitorea el ambiente físico para detectar potenciales eventos de ciberseguridad.	2	
		DE.MC-3. Se monitorea la actividad del personal para detectar potenciales eventos de ciberseguridad.	0	
		DE.MC-4. Se detecta el código malicioso.	0	
		DE.MC-5. Se detecta el código móvil no autorizado.	0	
		DE.MC-6. Se controla la actividad de los proveedores de servicios externos para detectar posibles eventos de ciberseguridad	2	
		DE.MC-7. Se realiza monitoreo para detectar personas, conexiones, dispositivos y software sin autorización.	1	
		DE.MC-8. Se realizan escaneos de vulnerabilidades.	5	
	Procesos de detección (DE.PD.) Se mantienen procesos y procedimientos de detección y se les prueba para asegurar una adecuada concientización sobre eventos anómalos.	DE.PD-1. Los roles y las responsabilidades de detección se encuentran definidos de forma tal de asegurar la imputabilidad.	2	0,8
		DE.PD-2. Las actividades de detección cumplen con todos los requisitos aplicables.	2	
		DE.PD-3. Los procesos de detección son probados.	0	

		DE.PD-4. La información de la detección de eventos es comunicada a las partes pertinentes	0	
		DE.PD-5. Los procesos de detección son mejorados continuamente	0	
RESPONDER (RE)	**Planificación de la respuesta (RE.PR.)** Los procesos y procedimientos de respuesta se ejecutan y se mantienen de manera que se garantiza una respuesta oportuna ante los eventos de ciberseguridad detectados.	RE.PR-1. El plan de respuesta se ejecuta durante o luego de un incidente	2	2,0
	Comunicaciones (RE.CO.) Las actividades de respuesta se coordinan con las partes interesadas internas y externas, según corresponda	RE.CO-1. El personal conoce sus roles y el orden de las operaciones cuando es necesaria una respuesta	0	0,6
		RE.CO-2. Los incidentes son reportados consistentemente con los criterios establecidos	0	
		RE.CO-3. La información se comparte de acuerdo con los planes de respuesta	0	
		RE.CO-4. La coordinación con las partes interesadas se realiza consistentemente con los planes de respuesta	0	
		RE.CO-5. Se realiza intercambio de información voluntaria con partes interesadas externas para alcanzar una conciencia de ciberseguridad más amplia	3	
	Análisis (RE.AN.) Se efectúa análisis para asegurar una respuesta adecuada y para dar soporte a las actividades de recuperación.	RE.AN-1. Se investigan las notificaciones de los sistemas de detección	2	0,8
		RE.AN-2. El impacto del incidente es comprendido	1	
		RE.AN-3. Se realiza análisis forense	0	
		RE.AN-4. Los incidentes son categorizados de acuerdo con los planes de respuesta	1	
		RE.AN-5. Existen procedimientos para recibir, analizar y responder a vulnerabilidades reveladas a la organización por fuentes internas y/o externas (pruebas internas, boletines o investigadores de seguridad)	0	
	Mitigación (RE.MI.) Se ejecutan actividades para prevenir la expansión de un evento, mitigar sus efectos y erradicar el incidente	RE.MI-1. Los incidentes son contenidos	2	1,3
		RE.MI-2. Los incidentes son mitigados	2	
		RE.MI-3. Las nuevas vulnerabilidades identificadas o bien se mitigan o se documentan como riesgos aceptados	0	
	Mejoras (RE.ME.) Las actividades de respuesta de la organización son mejoradas mediante la incorporación de lecciones aprendidas a partir de las actividades de detección y respuesta actuales y	RE.ME-1. Los planes de respuesta incorporan lecciones aprendidas	2	1,0
		RE.ME-2. Las estrategias de respuesta se actualizan	0	
RECUPERAR (RC)	**Planificación de la recuperación (RC. PR.)** Los procesos y procedimientos de recuperación son ejecutados y mantenidos para asegurar la restauración oportuna de los sistemas o activos afectados por eventos de ciberseguridad.	RC.PR-1. El plan de recuperación se ejecuta durante o luego de un evento	2	2,0
	Mejoras (RC.ME.) Se mejoran los planes y procesos de recuperación incorporando las lecciones aprendidas en actividades futuras.	RC.ME-1. Los planes de recuperación incorporan lecciones aprendidas	4	3,0
		RC.ME-2 Las estrategias de recuperación se actualizan	2	
	Comunicaciones (RC.CO.) Las actividades de recuperación se coordinan con las partes interesadas internas y externas, tales como centros de coordinación, proveedores de servicios de Internet,	RC.CO-1. Se gestionan las relaciones públicas	2	2,0
		RC.CO-2. Se repara la reputación luego del evento	2	
		RC.CO-3. Se comunican las actividades de recuperación a las partes interesadas internas y externas, así como también a los equipos ejecutivos y de gestión	2	