Estándares y buenas prácticas de Ciberseguridad en las Administraciones públicas de LATAM.

Últimas actualizaciones e implicancias.

Marcela Pallero
11 de diciembre de 2025

Temas:

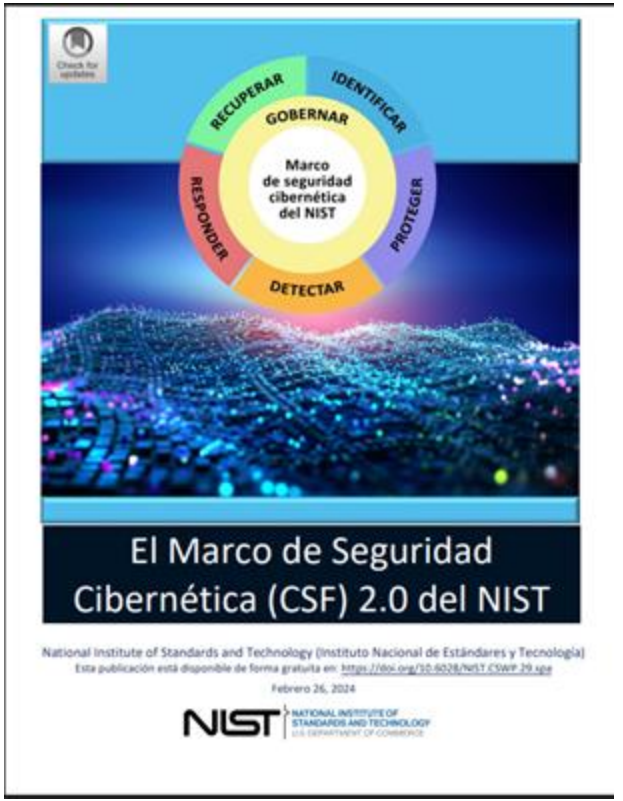
- Estándares y buenas prácticas
  - Marco de referencia de ciberseguridad de NIST
  - Familia ISO/IEC
  - Controles CIS
- Adopción en Países de América del Sur: Argentina, Brasil, Chile, Colombia, Ecuador, Paraguay, Uruguay.

ISACA
ADACSI | Buenos Aires Chapter

Contexto

Cyberframework de NIST 2.0

- Publicado en febrero de 2024
- Actualizado con la función: Gobernar
- Una característica principal es su extensión a todas las organizaciones, independientemente de tamaño, sector o madurez, convirtiéndolo en un estándar universal.

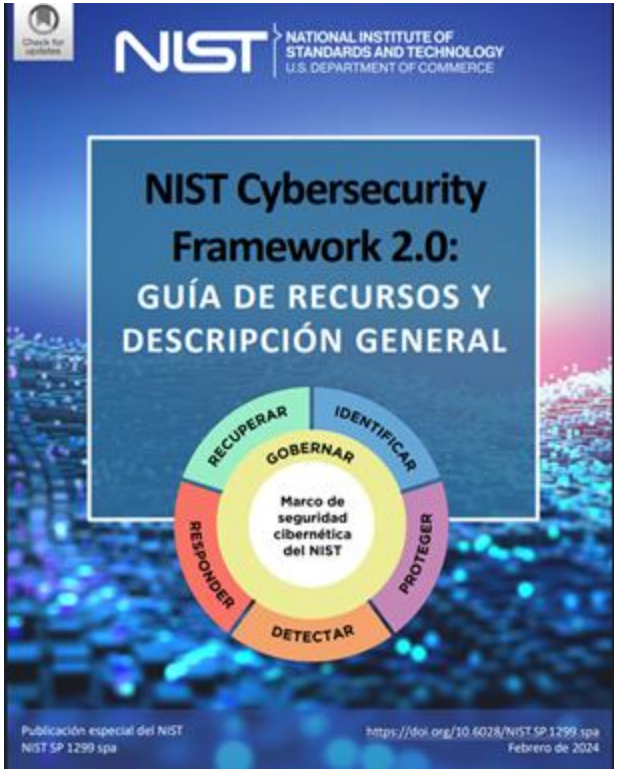


Contexto

Cyberframework de NIST 2.0

- 6 Funciones, 106 Subcategorías y 4 niveles de madurez para el gobierno y la gestión de los riesgos de ciberseguridad.

Fig. 4. Los niveles de los CSF para el gobierno y la gestión de los riesgos de seguridad cibernética



ISACA
ADACSI | Buenos Aires Chapter

Publicada en 2022

4 Categorías,

93 controles

CONTROLES DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PRIVACIDAD

ISO/IEC 27002:2022

CONTROLES ORGANIZACIONALES

GESTIÓN Y ENTORNO
5.1 Políticas de seguridad de la información
5.2 Roles y responsabilidades en seguridad de la información
5.3 Segregación de tareas
5.4 Responsabilidades de gestión
5.5 Contacto con las autoridades
5.6 Contacto con grupos de interés especial

AMENAZAS
5.7 Inteligencia de Amenazas

PROYECTOS
5.8 Seguridad de la información en la gestión de proyectos

INFORMACIÓN
5.9 Inventario de información y otros activos asociados
5.10 Uso aceptable de la información y otros activos asociados
5.11 Devolución de activos
5.12 Clasificación de la información
5.13 Etiquetado de la información
5.14 Transferencia de información

ACCESOS
5.15 Control de acceso
5.16 Gestión de identidades
5.17 Información de autenticación
5.18 Derechos de acceso

M. PALLERO

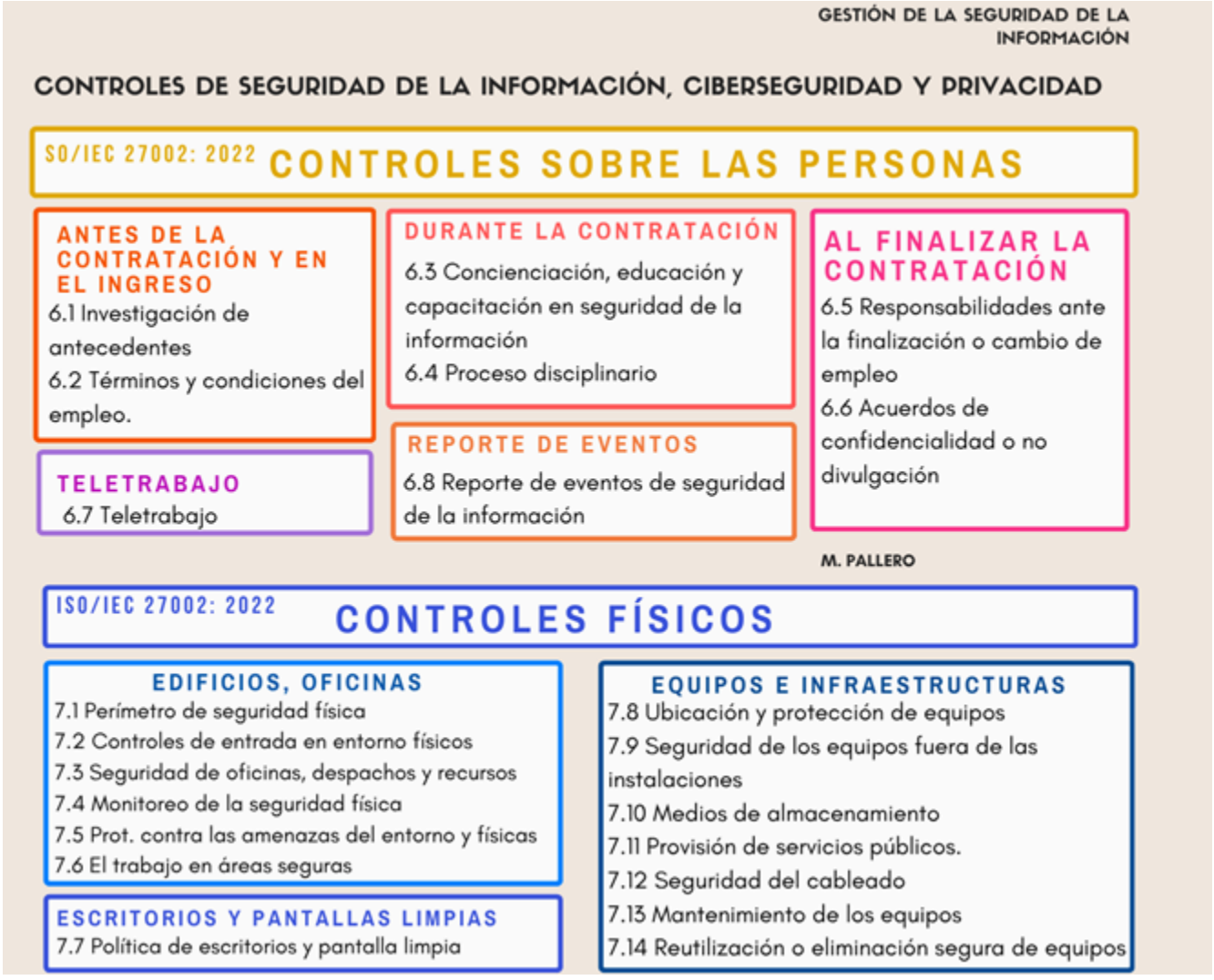
PROVEEDORES
5.19 Política de seguridad de la información en las relaciones con los proveedores
5.20 Abordar la seguridad de la información dentro de los acuerdos con los proveedores
5.21 Gestión de la seguridad de la información en la cadena de suministro TIC
5.22 Monitoreo, revisión y gestión del cambio en los proveedores de servicios
5.23 Seguridad de la información en el uso de servicios en la nube

GESTIÓN DE INCIDENTES Y SEGURIDAD EN LA CONTINUIDAD
5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información
5.25 Evaluación y decisión sobre los eventos de seguridad de información
5.26 Respuesta a incidentes de seguridad de la información
5.27 Aprendizaje de los incidentes de seguridad de la información
5.28 Recopilación de evidencias
5.29 Seguridad de la información durante una disrupción.
5.30 Preparación TIC para la continuidad del negocio

REQUERIMIENTOS LEGALES Y CUMPLIMIENTO
5.31 Identificación de requerimientos legales, estatutarios, regulatorios y contractuales
5.32 Derechos de Propiedad Intelectual (DPI)
5.33 Protección de los registros de la organización
5.34 Protección y privacidad de la información de carácter personal
5.35 Revisión independiente de la seguridad de la información
5.36 Cumplimiento con políticas y estándares para la seguridad de la información
5.37 Procedimientos operacionales documentados

ISACA
ADACSI | Buenos Aires Chapter

Se mapea con el CSF de NIST



ISACA
ADACSI | Buenos Aires Chapter

Incluye Dominios, y como atributos: Capacidades Operativas, entre otros.

CONTROLES DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PRIVACIDAD

ISO/IEC 27002: 2022 CONTROLES TÉCNICOS

ENDPOINT
8.1 Seguridad en los dispositivos finales.

ACCESOS
8.2 Gestión de privilegios de acceso
8.3 Restricción del acceso a la información

INFORMACIÓN
8.10 Eliminación de información
8.11 Enmascaramiento de datos
8.12 Prevención de la fuga de datos
8.13 Copias de seguridad de la información
8.14 Redundancia de las instalaciones de procesamiento de información

CRIPTOGRAFÍA
8.24 Uso de Critografía

CAMBIOS
8.32 Gestión del cambio

FUENTES AUTENTICACIÓN CAPACIDADES
8.4 Control de acceso al código fuente de los programas
8.5 Procedimientos autenticación seguros
8.6 Gestión de capacidades

EN EL EQUIPO DEL USUARIO
8.15 Inicio de Sesión
8.16 Monitoreo de actividades
8.17 Sincronización del reloj
8.18 Uso de aplicaciones con usuarios privilegiados
8.19 Instalación de software en sistemas operativo
8.23 Filtrado Web

LA RED
8.20 Seguridad de las redes
8.21 Seguridad de los servicios de red
8.22 Segregación en redes

MALWARE-VULNERABILIDADES
8.7 Controles contra el código malicioso
8.8 Gestión de vulnerabilidades técnicas
8.9 Gestión de las configuraciones

M. PALLERO

DESARROLLO
8.25 Seguridad en el ciclo de vida del desarrollo
8.26 Requerimientos de seguridad en aplicaciones
8.27 Principios de ingeniería y arquitectura de sistemas seguros
8.28 Codificación Segura
8.30 Desarrollo tercerizado

SEGURIDAD EN LAS PRUEBAS (EN DESARROLLO)
8.29 Pruebas de seguridad en el desarrollo y aceptación
8.31 Separación de ambientes de desarrollo, prueba y producción
8.33 Protección de los datos de prueba
8.34 Controles durante la auditoría de sistemas de información

ISACA
ADACSI | Buenos Aires Chapter

ISO/IEC 27002: 2022

93 Controles de Seguridad de la información, ciberseguridad protección de la privacidad.

Aspectos que incluyen los 4 dominios

M. Pallero

- GOBIERNO DE SEGURIDAD DE LA INFORMACIÓN & GESTIÓN DEL RIESGO
- GESTIÓN DE LA CIBERSEGURIDAD DEL ECOSISTEMA (INCLUYE PARTES INTERESADAS INTERNAS Y EXTERNAS)
- ARQUITECTURA DE SEGURIDAD DE TI
- ADMINISTRACIÓN DE SEGURIDAD DE TI
- GESTIÓN DE ACCESOS E IDENTIDADES
- MANTENIMIENTO DE LA SEGURIDAD DE TI
- SEGURIDAD FÍSICA Y MEDIOAMBIENTAL
- DETECCIÓN
- GESTIÓN DE INCIDENTES DE SI
- GESTIÓN DE CRISIS
- CONTINUIDAD DE LAS OPERACIONES

ISACA
ADACSI | Buenos Aires Chapter

CIS. Center for Internet Security

25 YEARS

Controles del Centro de Seguridad de Internet

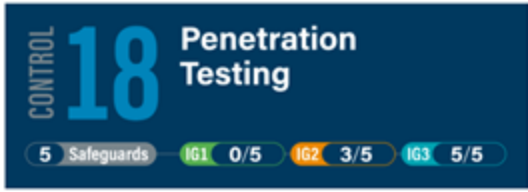
Controles CIS

ISACA
ADACSI | Buenos Aires Chapter

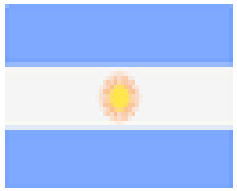
CIS Center for Internet Security 25 YEARS

Características de los Controles CIS:

- Son abiertos y gratuitos.
- Brinda niveles de implementación.
- Cuenta con documentación, foros para discutir y consultar.
- Es más conocido entre la comunidad técnica.
- El marco de gestión de riesgo está tratado en otro documento.



ISACA
ADACSI | Buenos Aires Chapter



Argentina

DA 641/2021- Obligatoria para el Sector Público Nacional.
Basada en la Norma ISO 27001 (ISO 27001: 2013)

Contiene 14 Directrices.

De la Normativa: Para la elaboración del documento se han tomado como referencia estándares nacionales e internacionales reconocidos, tales como las Normas IRAM-ISO/IEC 27001, 27002 y 20000-1

ISACA
ADACSI | Buenos Aires Chapter

Brasil

SUMÁRIO

AVISO PRELIMINAR E AGRADECIMENTOS ____ *12*

INTRODUÇÃO ____ *14*

1. FUNDAMENTAÇÃO E ESTRUTURAÇÃO DOS CONTROLES ____ *16*

1.1 Normas Legais de Conformidade ____ 16
1.1.1 LGPD ____ 17
1.1.2 Publicações da ANPD ____ 18
1.1.3 Normativos do GSI ____ 18
1.1.4 PNSI ____ 19

1.2 Estruturação básica de gestão em privacidade e segurança da informação ____ 19

1.3 Abordagem de controles e implementação de cibersegurança ____ 21
1.3.1 CIS Controls - Cibersegurança ____ 22
1.3.2 CIS Guia Complementar de Privacidade ____ 23
1.3.3 Grupos de Implementação ____ 23
1.3.4 NIST Cybersecurity Framework ____ 24

1.4 Abordagem de controles e implementação de privacidade ____ 26
1.4.1 ISO/IEC 29100:2011 ____ 27
1.4.2 ISO/IEC 29151:2017 ____ 27
1.4.3 ABNT NBR ISO/IEC 27701:2019 ____ 28
1.4.4 ISO/IEC 27018:2014 ____ 29
1.4.5 ISO/IEC 29134:2017 ____ 29
1.4.6 ABNT NBR ISO/IEC 29184:2021 ____ 30
1.4.7 NIST Privacy Framework ____ 30
1.4.8 Guias Orientativos da ANPD ____ 33

Guia do Framework de Privacidade e Segurança da Informação

PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO (PPSI)

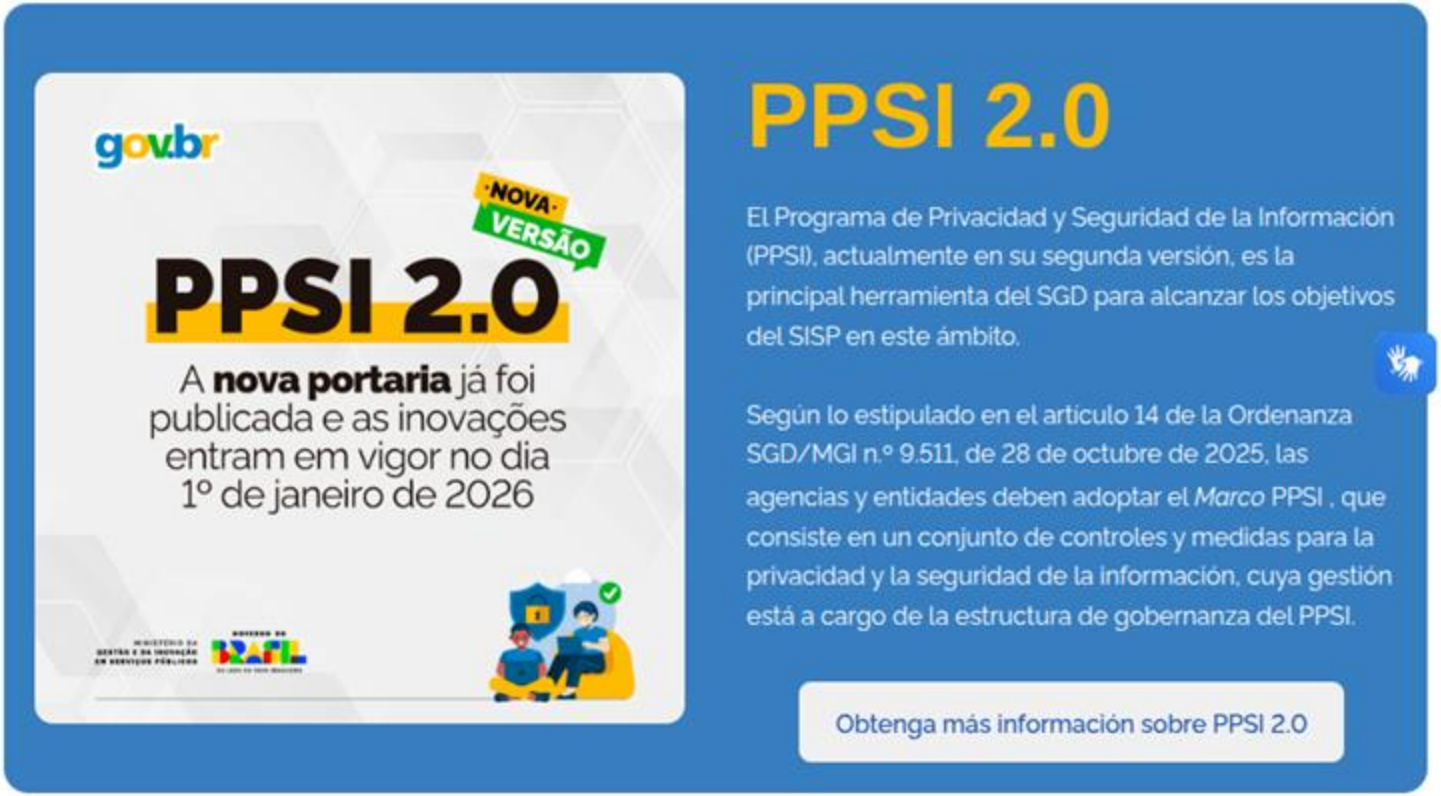
Versão 1.1.4

Brasília, dezembro de 2024

ISACA
ADACSI | Buenos Aires Chapter

Brasil

De la Secretaría de Gobierno Digital



ISACA
ADACSI | Buenos Aires Chapter

Brasil

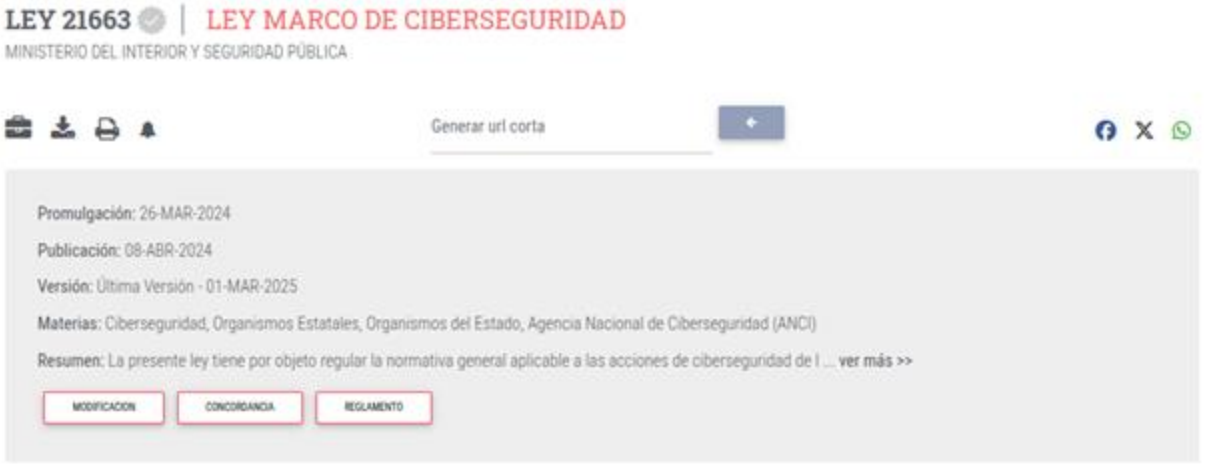
El Programa de Privacidad y Seguridad de la Información aborda:

- La gobernanza
- Cuenta con un modelo de madurez con ciclos de monitoreo.
- Una metodología de implementación.
- Las habilidades de las personas para ponerlo en práctica.
- Tecnologías implicadas.
- Cuenta con herramientas de autoevaluación.

ISACA
ADACSI | Buenos Aires Chapter

Chile

Ley Marco de Ciberseguridad



3. Auditorías de seguridad: procesos de control destinados a revisar el cumplimiento de las políticas y procedimientos que se derivan del Sistema de Gestión de la Seguridad de la Información.

ISACA
ADACSI | Buenos Aires Chapter

Chile

Ley Marco de Ciberseguridad, abril de 2024

Artículo 8º. Deberes específicos de los operadores de importancia vital. Todos los operadores de importancia vital deberán:

a) Implementar un sistema de gestión de seguridad de la información continuo con el fin de determinar aquellos riesgos que puedan afectar la seguridad de las redes, sistemas informáticos y datos, y la continuidad operacional del servicio.

Este sistema deberá permitir evaluar tanto la probabilidad como el potencial impacto de un incidente de ciberseguridad.

b) Mantener un registro de las acciones ejecutadas que compongan el sistema de gestión de seguridad de la información, de conformidad a lo que señale el reglamento.

ISACA
ADACSI | Buenos Aires Chapter

Chile

DECRETO 7 | ESTABLECE NORMA TÉCNICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD CONFORME LA LEY Nº 21.180

MINISTERIO SECRETARÍA GENERAL DE LA PRESIDENCIA

Establece un conjunto de definiciones y funciones para los órganos de la Administración del Estado, a saber:

- Función de identificación
- Función de protección
- Función de detección
- Función de respuesta
- Función de recuperación

Mayo 2023

ISACA
ADACSI | Buenos Aires Chapter

Colombia

TIC

Colombia cuenta con el Modelo de Seguridad y Privacidad de la Información - MSPI

Versión 5, 21/4/2025. Ministerio TIC. Res. 500/2021.

Ilustración 1 Ciclo del Modelo de Seguridad y Privacidad de la Información

ISACA
ADACSI | Buenos Aires Chapter

Colombia

Colombia cuenta con el Modelo de Seguridad y Privacidad de la Información - MSPI

- Brinda lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales,
- Con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital.

ISACA
ADACSI | Buenos Aires Chapter

Colombia

Colombia cuenta con el Modelo de Seguridad y Privacidad de la Información - MSPI

Listado de tablas

Tabla 1 Estructura de los controles..... 44
Tabla 2: Controles del Anexo A del estándar ISO/IEC 27001:2022 y dominios a los que pertenece..... 52

ISACA
ADACSI | Buenos Aires Chapter

Colombia

Guías y documentación para la implementación

ISACA
ADACSI | Buenos Aires Chapter

Ecuador

ISACA
ADACSI | Buenos Aires Chapter

Ecuador

Ciclo de Deming (PDCA)

Implementación del EGSI

El Esquema Gubernamental de Seguridad de la Información - EGSI-busca preservar la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos de seguridad de la información y la selección de controles para el tratamiento de los riesgos identificados.

- Normativa vigente

  Acuerdo Ministerial No. 0003-2024, las instituciones tienen un plazo de 12 meses para implementar o actualizar el EGSI versión 3.0

PLAN (Planificar)

DO (Hacer)

CHECK (Verificar)

ACT (Actuar)

ISACA
ADACSI | Buenos Aires Chapter

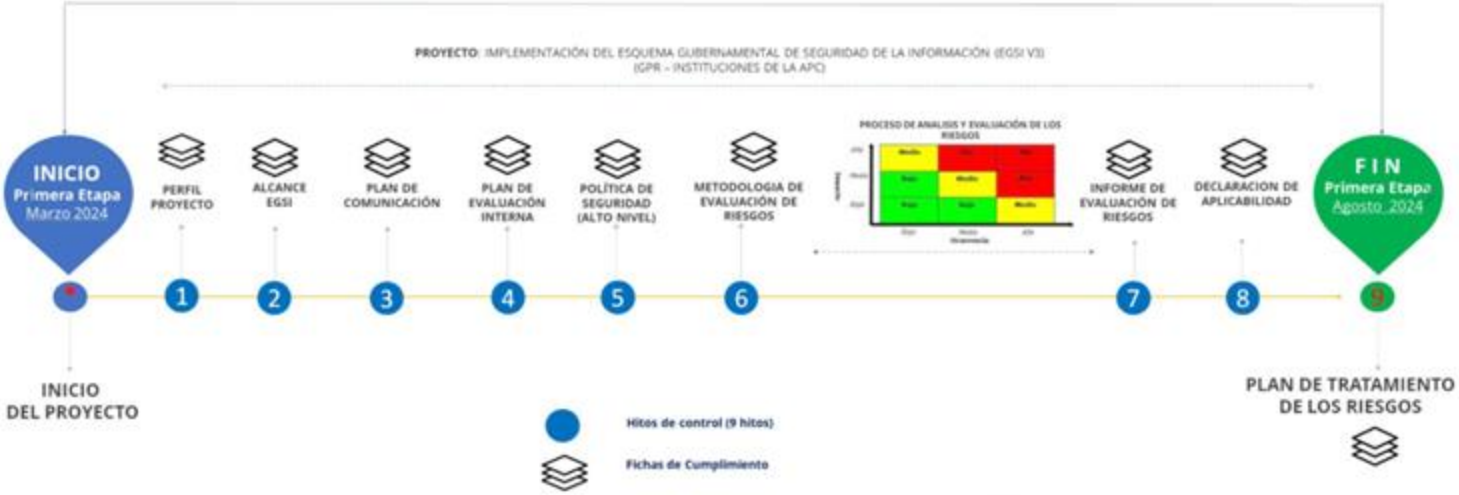
Ecuador

Implementación del EGSI versión 3.0

Hoja de ruta - Implementación EGSI versión 3.0

PRIMERA ETAPA - REQUISITOS DEL SISTEMA DE GESTIÓN (6 MESES)

PROGRAMA: GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LAS INSTITUCIONES DEL SECTOR PÚBLICO - EGSI V3 (GPR - MINTEL)



ISACA
ADACSI | Buenos Aires Chapter

Paraguay

La Resolución MITIC Nº 277/2020, que establece el estándar adoptado por el Gobierno, la Guía de Controles Críticos de Ciberseguridad (CIS Controls) con estándares mínimos de protección para los sistemas de información del Estado, asegurando que las organizaciones mejoren sus niveles de madurez en ciberseguridad implementando medidas de seguridad eficaces;

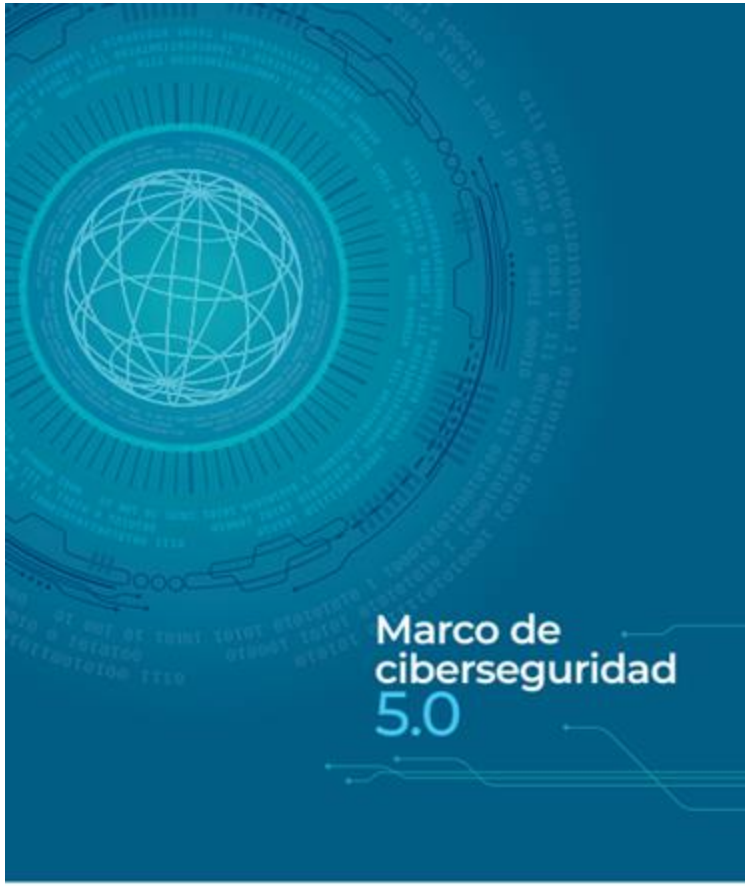
ISACA
ADACSI | Buenos Aires Chapter

Uruguay

Seguridad de la Información

Versión 5.0 Agosto de 2025

Basado y adaptado en CSF 2.0 de NIST



Presidencia Uruguay | agesic

ISACA
ADACSI | Buenos Aires Chapter

Uruguay

Material de Ciberseguridad

Marco de ciberseguridad 5.0

Marco de Referencia

02/12/2025

Compartir

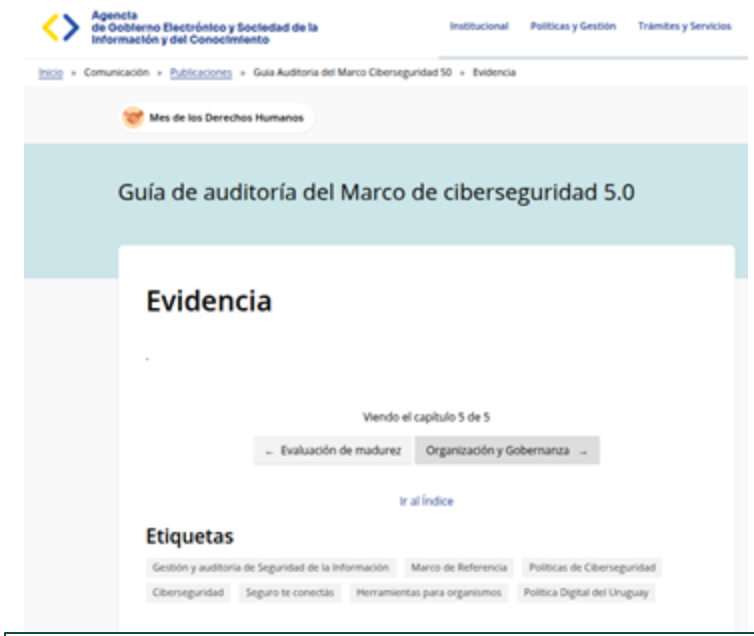
El Marco de ciberseguridad (MCU) 5.0 es una herramienta de referencia en materia de seguridad de la información y ciberseguridad. Proporciona un abordaje integral para reducir el riesgo vinculado a las amenazas que puedan comprometer la seguridad de la información en las organizaciones.

Modelo de Madurez

El modelo de madurez propuesto para la evaluación consta de cinco niveles, que se describen a continuación según sus requisitos.

ISACA
ADACSI | Buenos Aires Chapter

Uruguay



Contiene:

- 3 perfiles para adopción
- Guía de auditoría
- Herramienta de autodiagnóstico (sin fin de cumplimiento)
- Autoevaluación, para cumplimiento del decreto 66/2025

El **Decreto 66/2025** de Uruguay establece la obligatoriedad de implementar el **Marco de Ciberseguridad Nacional** para todas las entidades públicas y empresas privadas que proveen servicios esenciales o críticos al Estado.

ISACA
ADACSI | Buenos Aires Chapter

Reflexiones:

- Los Marcos de Referencias internacionales actualizados y se adaptan en los países.
- Abordan: Riesgos (PDCA) y Gobernanza.
- En los marcos para las administraciones públicas se integra la Seguridad de la información, la ciberseguridad y la PRIVACIDAD.

ISACA
ADACSI | Buenos Aires Chapter

¡Muchas gracias!

Marcela Pallero