

**ISACA Full Day**  
**BUENOS AIRES**



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

Últimas actualizaciones e  
implicancias.

Marcela Pallero  
11 de diciembre de 2025

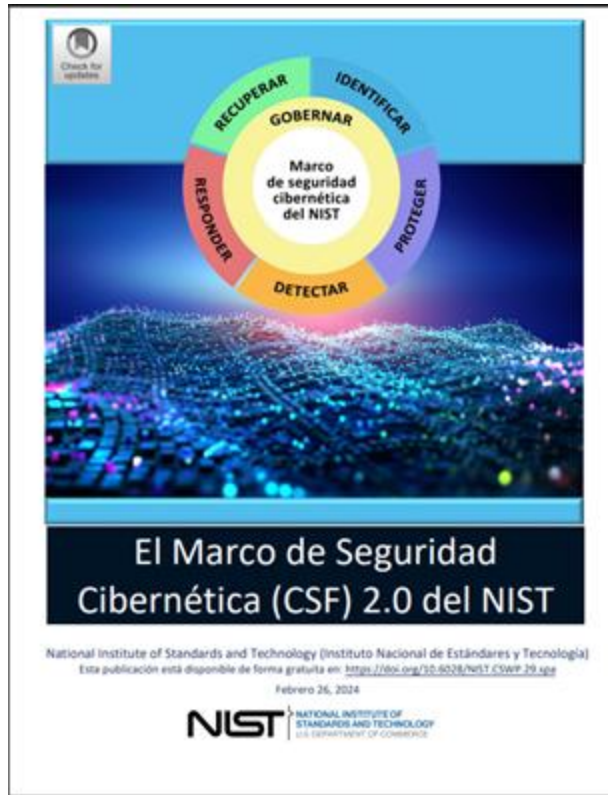
## Temas:

- 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.

# 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.



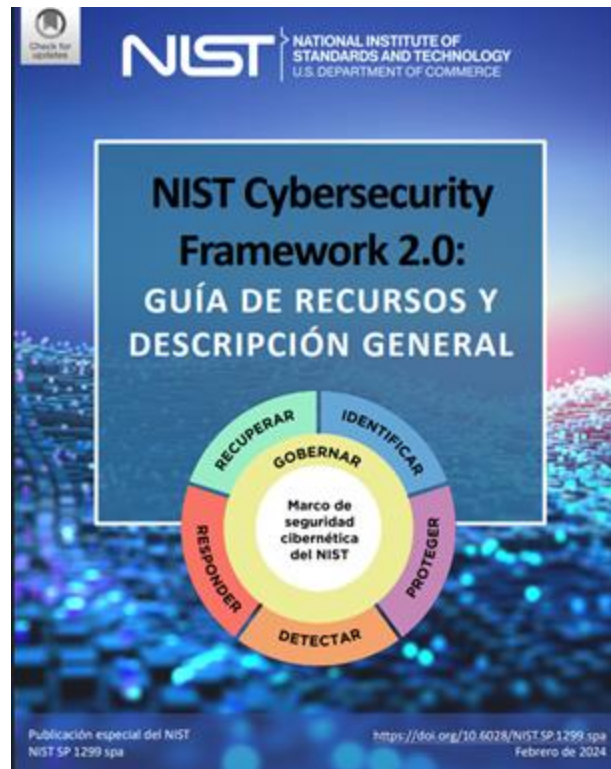
# Contexto

## 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



## 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

#### 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

M. PALLERO

#### 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

Publicada en  
2022

4 Categorías,  
93 controles

Se mapea  
con el CSF  
de NIST

## CONTROLES DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PRIVACIDAD

ISO/IEC 27002: 2022

### CONTROLES SOBRE LAS PERSONAS

#### ANTES DE LA CONTRATACIÓN Y EN EL INGRESO

- 6.1 Investigación de antecedentes
- 6.2 Términos y condiciones del empleo.

#### DURANTE LA CONTRATACIÓN

- 6.3 Concienciación, educación y capacitación en seguridad de la información
- 6.4 Proceso disciplinario

#### AL FINALIZAR LA CONTRATACIÓN

- 6.5 Responsabilidades ante la finalización o cambio de empleo
- 6.6 Acuerdos de confidencialidad o no divulgación

#### TELETRABAJO

- 6.7 Teletrabajo

#### REPORTE DE EVENTOS

- 6.8 Reporte de eventos de seguridad de la información

M. PALLERO

ISO/IEC 27002: 2022

### CONTROLES FÍSICOS

#### EDIFICIOS, OFICINAS

- 7.1 Perímetro de seguridad física
- 7.2 Controles de entrada en entorno físicos
- 7.3 Seguridad de oficinas, despachos y recursos
- 7.4 Monitoreo de la seguridad física
- 7.5 Prot. contra las amenazas del entorno y físicas
- 7.6 El trabajo en áreas seguras

#### ESCRITORIOS Y PANTALLAS LIMPIAS

- 7.7 Política de escritorios y pantalla limpia

#### EQUIPOS E INFRAESTRUCTURAS

- 7.8 Ubicación y protección de equipos
- 7.9 Seguridad de los equipos fuera de las instalaciones
- 7.10 Medios de almacenamiento
- 7.11 Provisión de servicios públicos.
- 7.12 Seguridad del cableado
- 7.13 Mantenimiento de los equipos
- 7.14 Reutilización o eliminación segura de equipos



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 Criptografía

#### 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

#### 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

#### 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

# ISO/IEC 27002: 2022

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

## Aspectos que incluyen los 4 dominios

M. Pallero





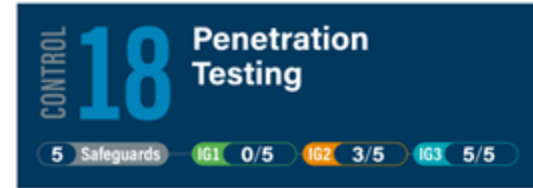
# Controles del Centro de Seguridad de Internet Controles CIS

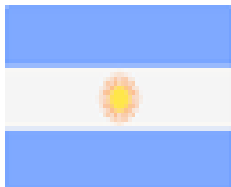
<b>CONTROL 01</b> Inventory and Control of Enterprise Assets 5 Safeguards 101 2/5 102 4/5 103 5/5	<b>CONTROL 02</b> Inventory and Control of Software Assets 7 Safeguards 101 3/7 102 6/7 103 7/7	<b>CONTROL 03</b> Data Protection 14 Safeguards 101 6/14 102 12/14 103 14/14
<b>CONTROL 04</b> Secure Configuration of Enterprise Assets and Software 12 Safeguards 101 7/12 102 11/12 103 12/12	<b>CONTROL 05</b> Account Management 6 Safeguards 101 4/6 102 6/6 103 6/6	<b>CONTROL 06</b> Access Control Management 8 Safeguards 101 5/8 102 7/8 103 8/8
<b>CONTROL 07</b> Continuous Vulnerability Management 7 Safeguards 101 4/7 102 7/7 103 7/7	<b>CONTROL 08</b> Audit Log Management 12 Safeguards 101 3/12 102 11/12 103 12/12	<b>CONTROL 09</b> Email and Web Browser Protections 7 Safeguards 101 2/7 102 6/7 103 7/7
<b>CONTROL 10</b> Malware Defenses 7 Safeguards 101 3/7 102 7/7 103 7/7	<b>CONTROL 11</b> Data Recovery 5 Safeguards 101 4/5 102 5/5 103 5/5	<b>CONTROL 12</b> Network Infrastructure Management 8 Safeguards 101 1/8 102 7/8 103 8/8
<b>CONTROL 13</b> Network Monitoring and Defense 11 Safeguards 101 0/11 102 6/11 103 11/11	<b>CONTROL 14</b> Security Awareness and Skills Training 9 Safeguards 101 8/9 102 9/9 103 9/9	<b>CONTROL 15</b> Service Provider Management 7 Safeguards 101 1/7 102 4/7 103 7/7
<b>CONTROL 16</b> Applications Software Security 14 Safeguards 101 0/14 102 11/14 103 14/14	<b>CONTROL 17</b> Incident Response Management 9 Safeguards 101 3/9 102 8/9 103 9/9	<b>CONTROL 18</b> Penetration Testing 5 Safeguards 101 0/5 102 3/5 103 5/5



## 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.





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



# Brasil

Guia do Framework de Privacidade e  
Segurança da Informação

## SUMÁRIO

<b>AVISO PRELIMINAR E AGRADECIMENTOS</b>	<b>12</b>
<b>INTRODUÇÃO</b>	<b>14</b>
<b>1. FUNDAMENTAÇÃO E ESTRUTURAÇÃO DOS CONTROLES</b>	<b>16</b>
<b>1.1 Normas Legais de Conformidade</b>	<b>16</b>
1.1.1 LGPD	17
1.1.2 Publicações da ANPD	18
1.1.3 Normativos do GSI	18
1.1.4 PNSI	19
<b>1.2 Estruturação básica de gestão em privacidade e segurança da informação</b>	<b>19</b>
<b>1.3 Abordagem de controles e implementação de cibersegurança</b>	<b>21</b>
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
<b>1.4 Abordagem de controles e implementação de privacidade</b>	<b>26</b>
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

**PROGRAMA DE  
PRIVACIDADE E  
SEGURANÇA DA  
INFORMAÇÃO  
(PPSI)**

Versão 1.1.4

Brasília, dezembro de 2024



Brasil

De la  
Secretaría  
de  
Gobierno  
Digital



**PPSI 2.0**

**NOVA  
VERSÃO**

A **nova portaria** já foi publicada e as inovações entram em vigor no dia 1º de janeiro de 2026

MINISTÉRIO DA  
GESTÃO E DA INOVAÇÃO  
DO GOVERNO FEDERAL

GOVERNO DO  
**BRASIL**  
30 de junho de 2025



## PPSI 2.0

El Programa de Privacidad y Seguridad de la Información (PPSI), actualmente en su segunda versión, es la principal herramienta del SGD para alcanzar los objetivos del SISP en este ámbito.

Según lo estipulado en el artículo 14 de la Ordenanza SGD/MGI n.º 9.511, de 28 de octubre de 2025, las agencias y entidades deben adoptar el *Marco PPSI*, que consiste en un conjunto de controles y medidas para la privacidad y la seguridad de la información, cuya gestión está a cargo de la estructura de gobernanza del PPSI.

Obtenga más información sobre PPSI 2.0





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.



Chile

**LEY 21663** | **LEY MARCO DE CIBERSEGURIDAD**  
MINISTERIO DEL INTERIOR Y SEGURIDAD PÚBLICA



Generar url corta



Promulgación: 26-MAR-2024

Publicación: 08-ABR-2024

Versión: Última Versión - 01-MAR-2025

Materias: Ciberseguridad, Organismos Estatales, Organismos del Estado, Agencia Nacional de Ciberseguridad (ANCI)

Resumen: La presente ley tiene por objeto regular la normativa general aplicable a las acciones de ciberseguridad de l ... [ver más >>](#)

MODIFICACION

CONCORDANCIA

REGLAMENTO

## 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.



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.



Chile

## **DECRETO 7** | ESTABLECE NORMA TÉCNICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD CONFORME LA LEY N° 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



Colombia



# 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

**Documento Maestro de Los  
Lineamientos del Modelo de  
Seguridad y Privacidad de la  
Información**

Ministerio de tecnologías de la información y las comunicaciones

**MSPI**





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.



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

# Colombia



## Guías y documentación para la implementación



[01. Documento Maestro MSPi](#)



[02. Roles y Responsabilidades](#)



[03. Indicadores de Gestión de Seguridad de la Información](#)



[04. Inventario y Clasificación de Activos de Información e Infraestructura Crítica Cibernética Nacional](#)



[05. Modelo Nacional de Gestión de Riesgos de Seguridad de la Información en Entidades Públicas](#)



[06. Relación con Proveedores de Tecnologías de la Información y Las Comunicaciones](#)



[07. Seguridad de la información para el uso de servicios en la nube](#)



[08. Identificación de las infraestructuras críticas cibernéticas](#)



[1. Política general de seguridad](#)



[2. Manual de políticas del MSPi](#)



[3. Plan estratégico de seguridad](#)



[3. Autodiagnóstico MSPi](#)



[2. Activos de Información MSPi](#)



[3. Riesgos de seguridad de la información MSPi](#)



[4. Servicios Nube MSPi](#)



**EGSI**

ESQUEMA  
GUBERNAMENTAL  
DE SEGURIDAD  
DE LA INFORMACIÓN

EGSI versión 3

Hoja de ruta

Registro OSI



## Esquema Gubernamental de Seguridad de la Información (EGSI)

Buscamos preservar el activo más importante del Estado ecuatoriano, la información.



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)**



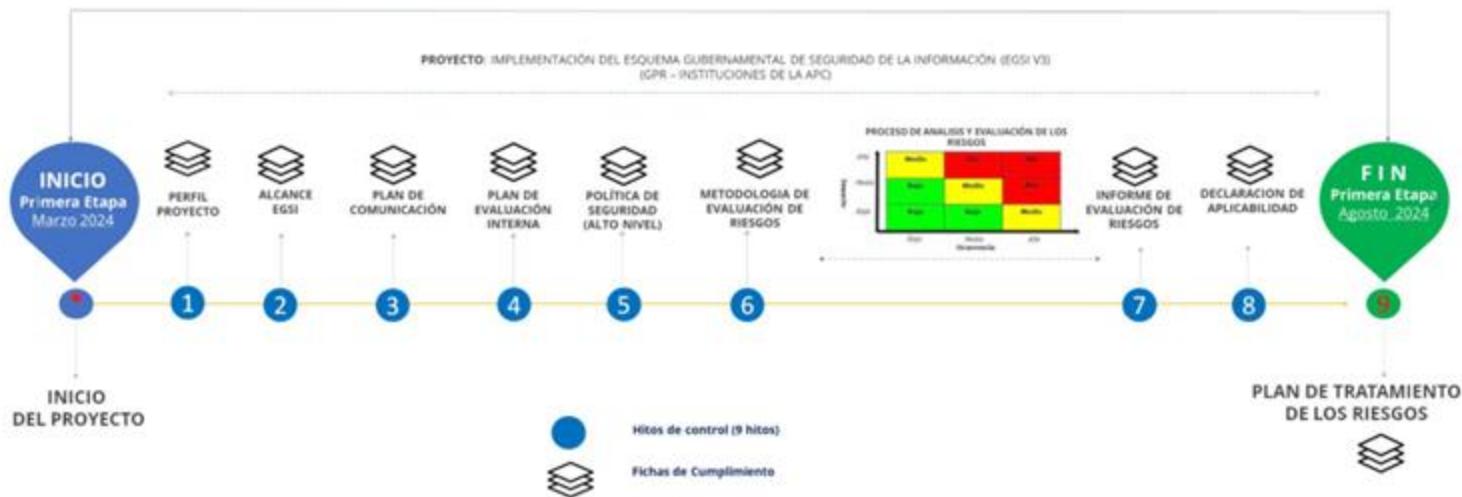


## Implementación del EGSi versión 3.0

### 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)



## Paraguay



La Resolución MITIC N° 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;



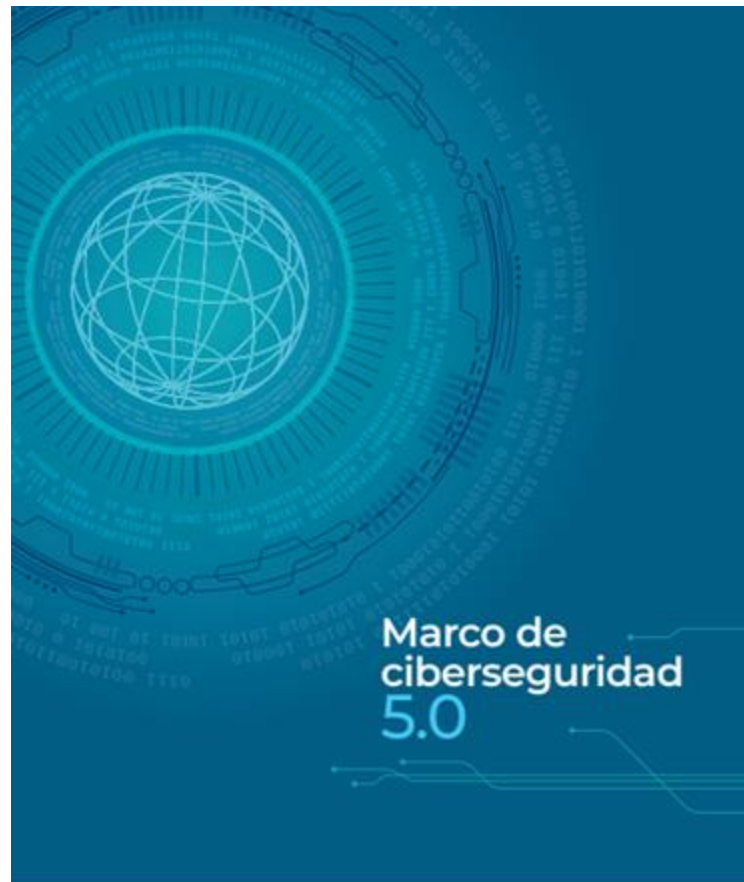
Uruguay



## Seguridad de la Información

Versión 5.0 Agosto de 2025

Basado y adaptado en CSF 2.0  
de NIST



Presidencia  
Uruguay



# Uruguay



## Modelo de Madurez

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



## 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.

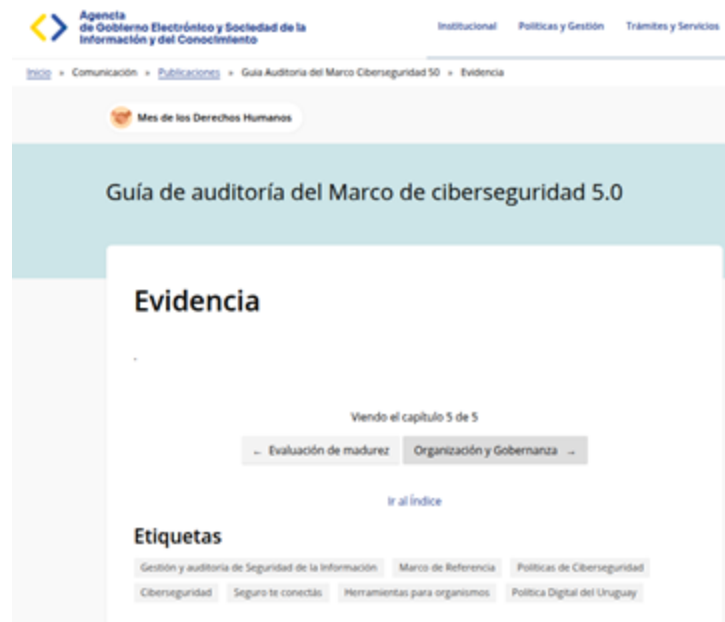


# Uruguay



## 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.



## 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.

**¡Muchas gracias!**

Marcela Pallero