Ley 21.663

Ley Marco de Ciberseguridad

Informática Legal y Derecho Informático
INF300 - 2025-2

Toledo Correa, Pedro

Departamento de Informática
Universidad Técnica Federico Santa María

22 de octubre de 2025 - v1.0

Tabla de contenidos

Tabla de contenidos

Tabla de contenidos

Definiciones - Artículo 2

1. **Activo informático**
   Toda información almacenada en una red y sistema informático que tenga valor para una persona u organización
2. **Agencia**
   La Agencia Nacional de Ciberseguridad, que se conocerá en forma abreviada como ANCI
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

Definiciones - Artículo 2

4. **Autenticación**
   Propiedad de la información que da cuenta de su origen legítimo
5. **Ciberataque**
   Intento de destruir, exponer, alterar, deshabilitar, o exfiltrar u obtener acceso o hacer uso no autorizado de un activo informático
6. **Ciberseguridad**
   Preservación de la confidencialidad e integridad de la información y de la disponibilidad y resiliencia de las redes y sistemas informáticos, con el objetivo de proteger a las personas, la sociedad, las organizaciones o las naciones de incidentes de ciberseguridad

Definiciones - Artículo 2

7. **Confidencialidad**
   Propiedad que consiste en que la información no es accedida o entregada a individuos, entidades o procesos no autorizados
8. **Disponibilidad**
   Propiedad que consiste en que la información está disponible y es utilizable cuando es requerida por un individuo, entidad o proceso autorizado
9. **Equipo de Respuesta a Incidentes de Seguridad Informática o CSIRT**
   Centros multidisciplinarios que tienen por objeto prevenir, detectar, gestionar y responder a incidentes de ciberseguridad o ciberataques, en forma rápida y efectiva, y que actúan conforme a procedimientos y políticas predefinidas, ayudando a mitigar sus efectos

Definiciones - Artículo 2

10. **Incidente de ciberseguridad**
    Todo evento que perjudique o comprometa la confidencialidad o integridad de la información, la disponibilidad o resiliencia de las redes y sistemas informáticos, o la autenticación de los procesos ejecutados o implementados en las redes y sistemas informáticos
11. **Integridad**
    Propiedad que consiste en que la información no ha sido modificada o destruida sin autorización
12. **Red y sistema informático**
    Conjunto de dispositivos, cables, enlaces, enrutadores u otros equipos de comunicaciones o sistemas que almacenen, procesen o transmitan datos digitales

Definiciones - Artículo 2

13. **Resiliencia**
    Capacidad de las redes y sistemas informáticos para seguir operando luego de un incidente de ciberseguridad, aunque sea en un estado degradado, debilitado o segmentado, y la capacidad de las redes y sistemas informáticos para recuperar sus funciones después de un incidente de ciberseguridad
14. **Riesgo**
    Posibilidad de ocurrencia de un incidente de ciberseguridad; la magnitud de un riesgo es cuantificada en términos de la probabilidad de ocurrencia del incidente y del impacto de las consecuencias del mismo
15. **Vulnerabilidad**
    Debilidad de un activo o control que puede ser explotado por una o más amenazas informáticas

Tabla de contenidos

Principios - Artículo 3

1. **Principio de control de daños**
   Frente a un ciberataque o a un incidente de ciberseguridad siempre se deberá actuar coordinada y diligentemente, y adoptar las medidas necesarias para evitar la escalada del ciberataque o del incidente de ciberseguridad y su posible propagación a otros sistemas informáticos
2. **Principio de cooperación con la autoridad**
   Para resolver los incidentes de ciberseguridad se deberá prestar la cooperación debida con la autoridad competente y, si es necesario, cooperar entre diversos sectores, teniendo en cuenta la interconexión y la interdependencia de los sistemas y servicios

Principios - Artículo 3

3. **Principio de coordinación**
   De conformidad a lo dispuesto por el inciso segundo del artículo 5º de la ley Nº 18.575, orgánica constitucional de Bases Generales de la Administración del Estado, la Agencia y las autoridades sectoriales deberán cumplir sus cometidos coordinadamente, propender a la unidad de acción y evitar la duplicación o interferencia de funciones
4. **Principio de seguridad en el ciberespacio**
   Es deber del Estado resguardar la seguridad en el ciberespacio. El Estado velará por que todas las personas puedan participar de un ciberespacio seguro, otorgando especial protección a las redes y sistemas informáticos que contengan información de aquellos grupos de personas que suelen ser en mayor medida objeto de ciberataques

Principios - Artículo 3

5. **Principio de respuesta responsable**
   La aplicación de medidas para responder a la realización o el apoyo a operaciones ofensivas
6. **Principio de seguridad informática**
   Toda persona tiene derecho a adoptar las medidas técnicas de seguridad informática que considere necesarias, incluyendo el cifrado

Principios - Artículo 3

7. **Principio de racionalidad**
   Las medidas para la gestión de incidentes de ciberseguridad, las obligaciones de ciberseguridad y el ejercicio de las facultades de la Agencia deberán ser necesarias y proporcionales al grado de exposición a los riesgos y al eventual impacto social y económico
8. **Principio de seguridad y privacidad por defecto y desde el diseño**
   Los sistemas informáticos, aplicaciones y tecnologías de la información deben diseñarse, implementarse y gestionarse teniendo en cuenta la seguridad y la privacidad de los datos personales que procesan

Tabla de contenidos

Ámbito de Aplicación

- Organismos de la Administración del Estado, como Ministerios y Municipalidades
- Empresas del Estado y sociedades con participación mayoritaria estatal
- Prestadores de servicios esenciales y operadores de importancia vital

Órganos autónomos - Artículo 53

- Senado
- Cámara de Diputados
- Poder Judicial
- Contraloría General de la República
- Banco Central
- Ministerio Público
- Servicio Electoral
- Consejo Nacional de Televisión

Clasificación de los Servicios Esenciales

- Aquellos provistos por organismos públicos
- Servicios prestados bajo concesión pública, como agua potable y energía
- Servicios privados de sectores críticos como telecomunicaciones, banca, salud, y transporte

Operadores de Importancia Vital

- Instituciones o servicios cuya afectación tendría un impacto significativo en la seguridad o el orden público
- **Criterios para clasificación**
  - Dependencia de redes y sistemas informáticos críticos
  - Impacto potencial de su interrupción o daño en la seguridad nacional o en la provisión de servicios esenciales

Tabla de contenidos

Tabla de contenidos

Agencia Nacional de Ciberseguridad (ANCI)

- **Propósito**
  Coordinar y supervisar las acciones de ciberseguridad en organismos del Estado y sector privado.
- **Funciones principales**
  - Asesorar al Presidente en materias de ciberseguridad
  - Proteger los intereses nacionales en el ciberespacio
  - Coordinar y supervisar la acción de los organismos de la Administración del Estado en ciberseguridad
  - Velar por el derecho a la seguridad informática

Consejo Multisectorial sobre Ciberseguridad

- **Propósito**
  Asesorar y formular recomendaciones a la Agencia en el análisis y revisión periódica de la situación de ciberseguridad
- **Regulación**
  Un reglamento del Ministerio encargado de la seguridad pública

Red de Conectividad Segura del Estado (RCSE)

- **Propósito**
  Proveer servicios de interconexión y conectividad segura entre los organismos de la Administración del Estado
- **Regulación**
  Un reglamento del Ministerio encargado de la seguridad pública y visado por el Ministerio de Hacienda define el funcionamiento de la RCSE y las obligaciones de los organismos usuarios

Equipos de Respuesta a Incidentes de Seguridad Informática Institucionales

- **Propósito**
  Responder a vulnerabilidades y amenazas en los sistemas de ciberseguridad de las instituciones de defensa nacional
- **Coordinación**
  Actúan en línea con el CSIRT de la Defensa Nacional, bajo la normativa del Ministerio de Defensa

Equipo Nacional de Respuesta a Incidentes de Seguridad Informática (CSIRT Nacional)

- **Propósito**
  Responder a ciberataques o incidentes de ciberseguridad de impacto significativo
- **Funciones principales**
  - Respuesta a incidentes
  - Coordinación de acciones en casos de ciberseguridad críticos
  - Fortalecer la seguridad cibernética en los sectores públicos y privados

Equipo de Respuesta a Incidentes de Seguridad Informática de la Defensa Nacional (CSIRT de la Defensa)

- **Propósito**
  Coordinar y asegurar la ciberseguridad de las redes y sistemas del Ministerio de Defensa y operadores esenciales para la defensa nacional
- **Dependencia**
  Estado Mayor Conjunto, Ministerio de Defensa Nacional

Tabla de contenidos

Atribuciones de la Agencia Nacional de Ciberseguridad

- La Agencia Nacional de Ciberseguridad (ANCI) coordina la seguridad en el ciberespacio, protegiendo los intereses nacionales y supervisando los organismos públicos y privados en su cumplimiento de normativas de ciberseguridad
- **Principales atribuciones**
  - Asesorar al Presidente en políticas y estrategias de ciberseguridad
  - Emitir protocolos, estándares y normas obligatorias para organismos y empresas
  - Coordinar y supervisar el CSIRT Nacional y otros organismos de ciberseguridad del Estado

Atribuciones de Fiscalización

- Realizar inspecciones y auditorías en organismos regulados
- Exigir información y documentación para verificar el cumplimiento de normas
- Evaluar la efectividad de los planes de ciberseguridad y continuidad operativa

Información y acceso - Artículo 11.j

- La Agencia puede solicitar a los organismos públicos y privados información necesaria para
  - Prevenir incidentes de ciberseguridad
  - Gestionar incidentes ya ocurridos
- **Requerimientos**
  - **Información solicitada**
    Los registros de actividad de redes y sistemas
  - **Criterio**
    Debe ser una instrucción particular y debidamente fundamentada

Información y acceso - Artículo 11.j
Protección de Datos Personales

- La Agencia debe anonimizar los datos personales, siempre que ello sea compatible con la gestión de incidentes
- Los datos personales deben manejarse conforme a la Ley N.º 19.628 sobre protección de la vida privada
- La dirección IP no se considera un dato personal en el contexto de la ciberseguridad

Tabla de contenidos

Tabla de contenidos

Paso 1: Notificación de Solicitud de Acceso

- La Agencia Nacional de Ciberseguridad (ANCI) solicita acceso a redes y sistemas informáticos de una institución privada
- La notificación se envía al correo electrónico registrado de la institución privada
- La institución tiene el derecho de oponerse formalmente, suspendiendo la solicitud de acceso hasta que un tribunal revise el caso

Paso 2: Presentación de la Oposición

- La institución privada presenta su oposición ante la solicitud de la ANCI, indicando que no autoriza el acceso inmediato a sus redes y sistemas informáticos
- La oposición bloquea temporalmente el acceso de la ANCI, quien deberá obtener autorización judicial para continuar

Paso 3: Solicitud de Autorización Judicial

- La ANCI solicita autorización a un Ministro de la Corte de Apelaciones de Santiago, debidamente fundamentada en hechos específicos que justifiquen el acceso
- Anualmente, el Presidente de la Corte designa dos Ministros encargados de revisar estas solicitudes

Paso 4: Audiencia Breve y Decisión Judicial

- El tribunal fija una audiencia en el plazo más breve posible para escuchar a ambas partes
- El Ministro de la Corte decide si permite o rechaza la solicitud de acceso
- La decisión debe estar basada en la justificación de la necesidad y urgencia del acceso solicitado por la ANCI

Plazos y Recursos Adicionales

- La resolución debe dictarse en un plazo preferencial y extraordinario; si es necesario, el tribunal puede sesionar de manera extraordinaria
- La decisión del Ministro puede ser apelada ante la misma Corte de Apelaciones de Santiago, la cual priorizará su resolución al día siguiente o en sesión extraordinaria en caso de inhabilidad

Tabla de contenidos

Determinación de Servicios Esenciales

- Son **Servicios Esenciales** aquellos cuya afectación puede impactar gravemente la seguridad pública, el orden social, o la continuidad de servicios críticos
- **Ejemplos**
  - Energía (generación, transmisión, distribución)
  - Suministro de agua potable y saneamiento
  - Telecomunicaciones e infraestructura digital
  - Banca y medios de pago

Proceso de Calificación de Servicios Esenciales

- La Agencia Nacional de Ciberseguridad puede calificar servicios como esenciales mediante resolución fundada, si su afectación puede causar daños graves a la población o al orden público
- La calificación debe someterse a un proceso de consulta pública, conforme a la ley 19.880

Calificación de Operadores de Importancia Vital

- Son **Operadores de Importancia Vital** aquellos cuya interrupción afectaría significativamente la seguridad, orden público o la provisión continua de servicios esenciales
- **Requisitos**
  - Dependencia en redes y sistemas informáticos críticos
  - Impacto significativo en caso de interrupción en el ámbito público o en la continuidad de servicios esenciales

Proceso de Calificación de Operadores de Importancia Vital

- La Agencia solicita un informe de organismos públicos competentes sobre potenciales operadores vitales (Informe sectorial)
- La Agencia elabora una lista preliminar de operadores de importancia vital, sometida a consulta pública (solo instituciones privadas)
- Tras la consulta pública, se publica la lista definitiva mediante resolución exenta

Plazos en el Proceso de Calificación de Operadores de Importancia Vital

- **Informe sectorial**
  30 días para responder
- **Consulta pública**
  30 días corridos
- **Informe final de la Agencia**
  30 días después de la consulta

Tabla de contenidos

Notificación Inicial de Incidentes de Ciberseguridad

- **Procedimiento**
  Toda institución afectada debe enviar una alerta temprana al CSIRT Nacional al tener conocimiento del incidente
- **Plazo**
  Máximo de 3 horas desde que se detecta un incidente con posible impacto significativo

Actualización de Información sobre el Incidente

- **Procedimiento**
  Las instituciones afectadas deben proporcionar una actualización con una evaluación inicial de gravedad, impacto e indicadores de compromiso
- **Plazo**
  - Máximo de 72 horas desde la notificación inicial
  - Si afecta a un operador de importancia vital, la actualización debe entregarse en 24 horas

Informe Final del Incidente

- **Procedimiento**
  Elaborar y entregar un informe final detallando la gravedad, el impacto, el tipo de amenaza y las medidas de mitigación aplicadas
- **Plazo**
  - Máximo de 15 días corridos desde la alerta temprana
  - Si el incidente continúa después de este plazo, se debe entregar un informe actualizado sobre la situación

Plan de Acción para Operadores de Importancia Vital

- **Procedimiento**
  Los operadores de importancia vital deben formular un plan de acción para mitigar el incidente y reportarlo al CSIRT Nacional
- **Plazo**
  Máximo de 7 días corridos desde que se detecta el incidente

Tabla de contenidos

Tabla de contenidos

Reglamentos

- **275/2024 - Funcionamiento del comité interministerial**
- **276/2024 - Funcionamiento del consejo multisectorial**
- **483/2025 - Estructura interna de la ANCI**
- **295/2024 - Reporte de incidentes**
- **285/2024 - Procedimiento de clasificación**
- **293/2024 - Red de conectividad segura del Estado**

Tabla de contenidos

Agencia Nacional de Ciberseguridad

- Director Ejecutivo: **Daniel Álvarez Valenzuela**
- **Sitio web oficial**
- **Reporte de incidentes para regulados**
- **Reporte de incidentes para público general (CSIRT)**
- **CSIRT Nacional**

Agencia Nacional de Ciberseguridad

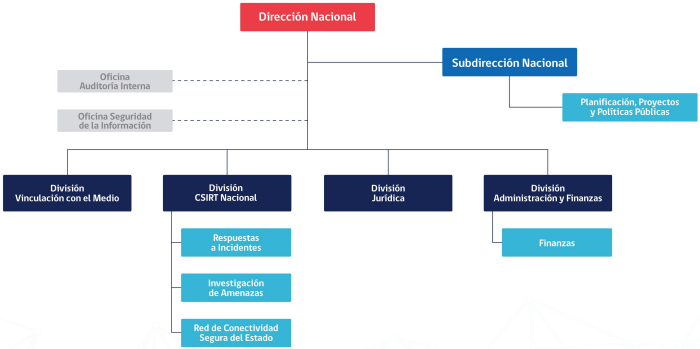

Figura 1: Organigrama de la Agencia Nacional de Ciberseguridad[1]

[1] Fuente: https://anci.gob.cl/quienes-somos/organigrama/

¿Preguntas?

Fotografía de fondo:
https://prensa.presidencia.cl/fotografia.aspx?id=282688
Plantilla del tema:
https://github.com/ptoledo-teaching/pt-slides