



MES DE LA CIBERSEGURIDAD: EL ROL CLAVE DE LA ANCI

Michelle Bordachar Benoit
Directora Nacional (s)

UN NUEVO MARCO PARA UN **RIESGO QUE CAMBIÓ**

LA CIBERSEGURIDAD ES **CONTINUIDAD,**
CONFIANZA Y RESILIENCIA



UN ECOSISTEMA SEGURO PARA EL **DESARROLLO DEL PAÍS**



ÁMBITO DE APLICACIÓN Y OBLIGACIONES



SE PRESTADORES DE SERVICIOS ESENCIALES

Todos los **OAE** y las **instituciones privadas** que prestan servicios en:

- | | | |
|--------------------|-------------------------|----------------------------|
| Sector eléctrico | Combustibles | Agua y saneamiento |
| Telecomunicaciones | Infraestructura digital | Servicios y TI de terceros |
| Transporte | Banca y medios de pago | Seguridad social |
| Salud | Industria farmacéutica | Correos y mensajería |

OIV OPERADORES DE IMPORTANCIA VITAL

Instituciones públicas o privadas **calificadas por la ANCI** conforme al procedimiento que establece la ley.

SE Y OIV

Reportar incidentes
con efecto significativo

Deber general de ciberseguridad
prestar sus servicios de manera segura

Sin deberes adicionales

SOLO OIV

Deberes del art. 8

A FUTURO

Nuevas normas irán dando contenido concreto a los deberes generales

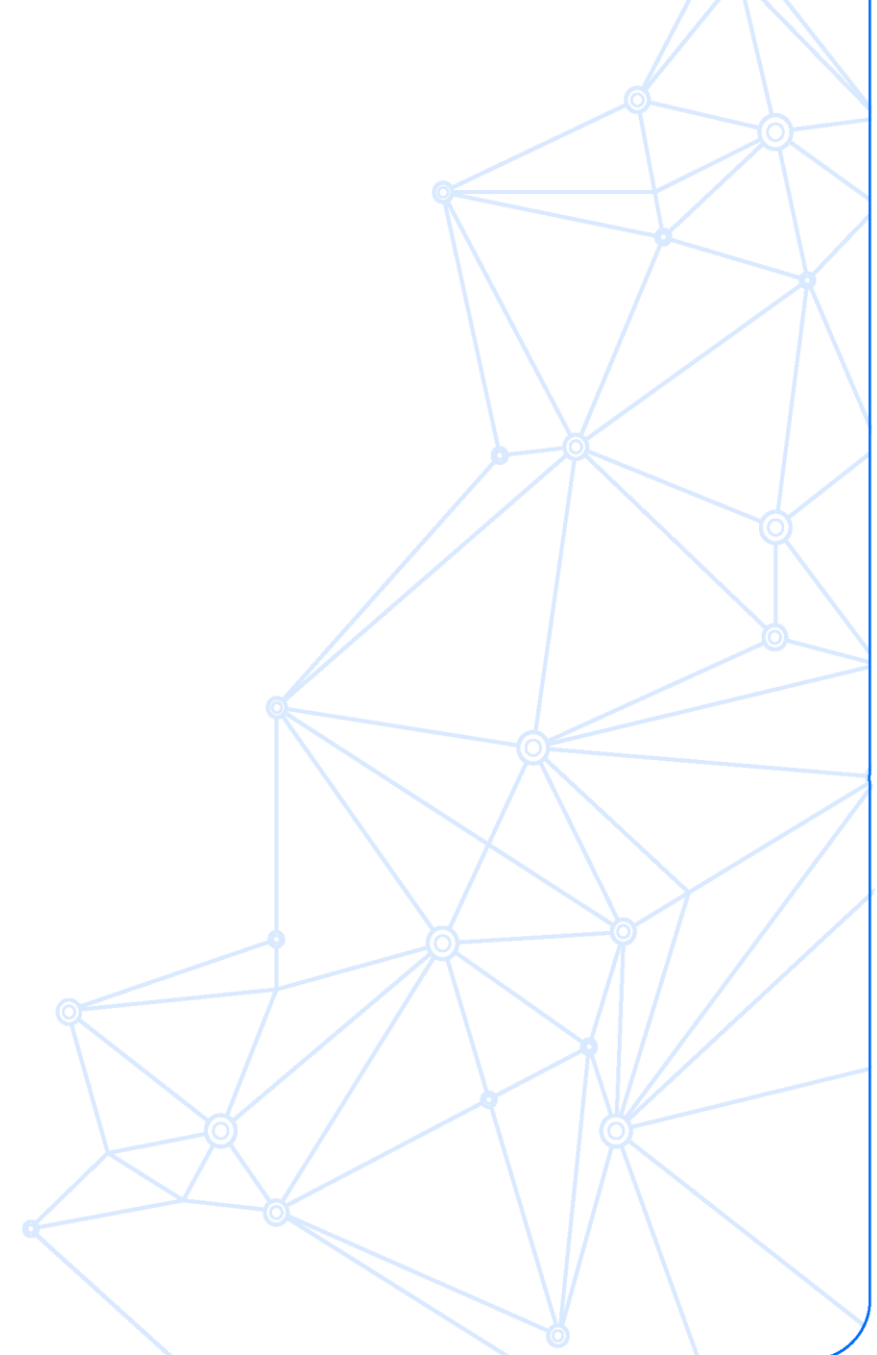
ROL AGENCIA NACIONAL DE CIBERSEGURIDAD

Prevenir, contener y gestionar incidentes de ciberseguridad.

Regular, fiscalizar y sancionar al sector público y privado.

Promover el desarrollo de una **cultura y capacidades** en ciberseguridad.

Proveer interconexión segura a OAE mediante la RCSE.



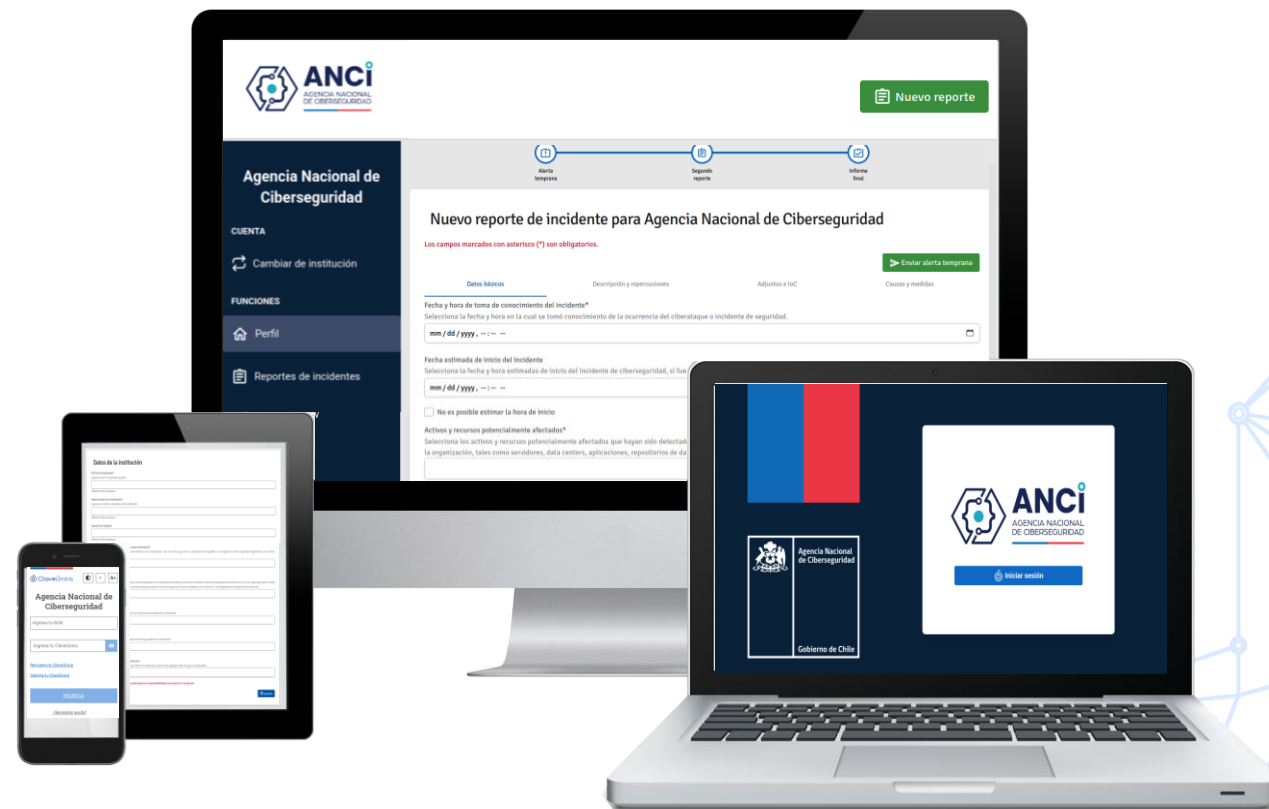
**REPORTAR PARA PREVENIR.
PREVENIR PARA PROTEGER.**



PORTAL DE REPORTE DE INCIDENTES



Plataforma oficial para reportar incidentes de ciberseguridad



El portal es el **punto de contacto** entre las instituciones y la Agencia

¿QUÉ REPORTAR?

Incidentes de efecto significativo:

- **Interrumpir** la continuidad de un servicio esencial.
- **Afectar** la integridad física o la salud de las personas.
- Afectar la **integridad** o confidencialidad de activos informáticos, o la disponibilidad de alguna red o sistema informático.
- **Utilizar** o ingresar sin autorización a redes o sistemas informáticos.
- Afectar sistemas informáticos que contengan **datos personales**.

Ante la duda, reporte.

Evite multas.



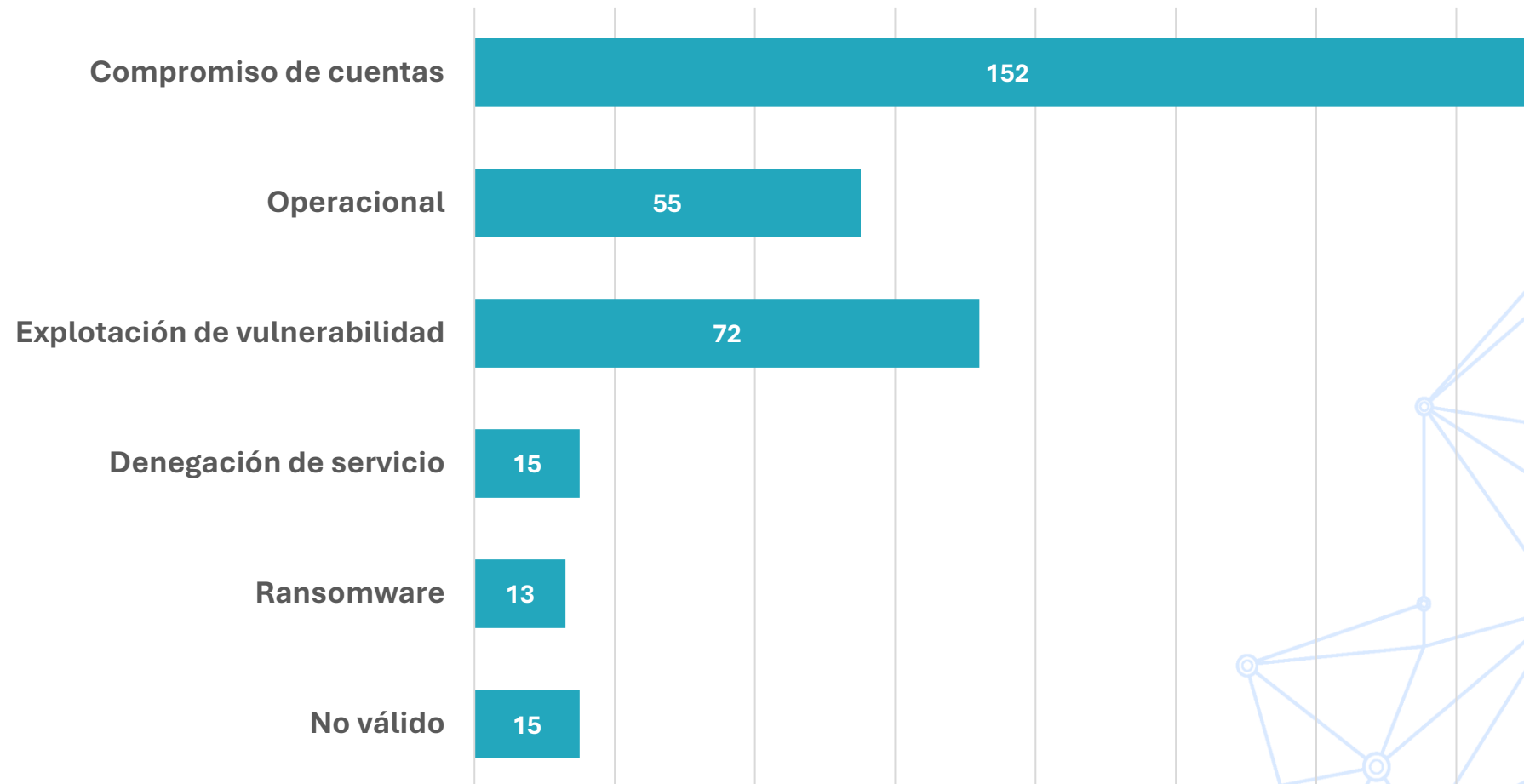
PRIMER SEMESTRE 2026

Durante el primer semestre, la ANCI recibió reportes de **324 reportes de incidentes** de efecto significativo en el país

1er trimestre: 128 incidentes

2do trimestre: 196 incidentes

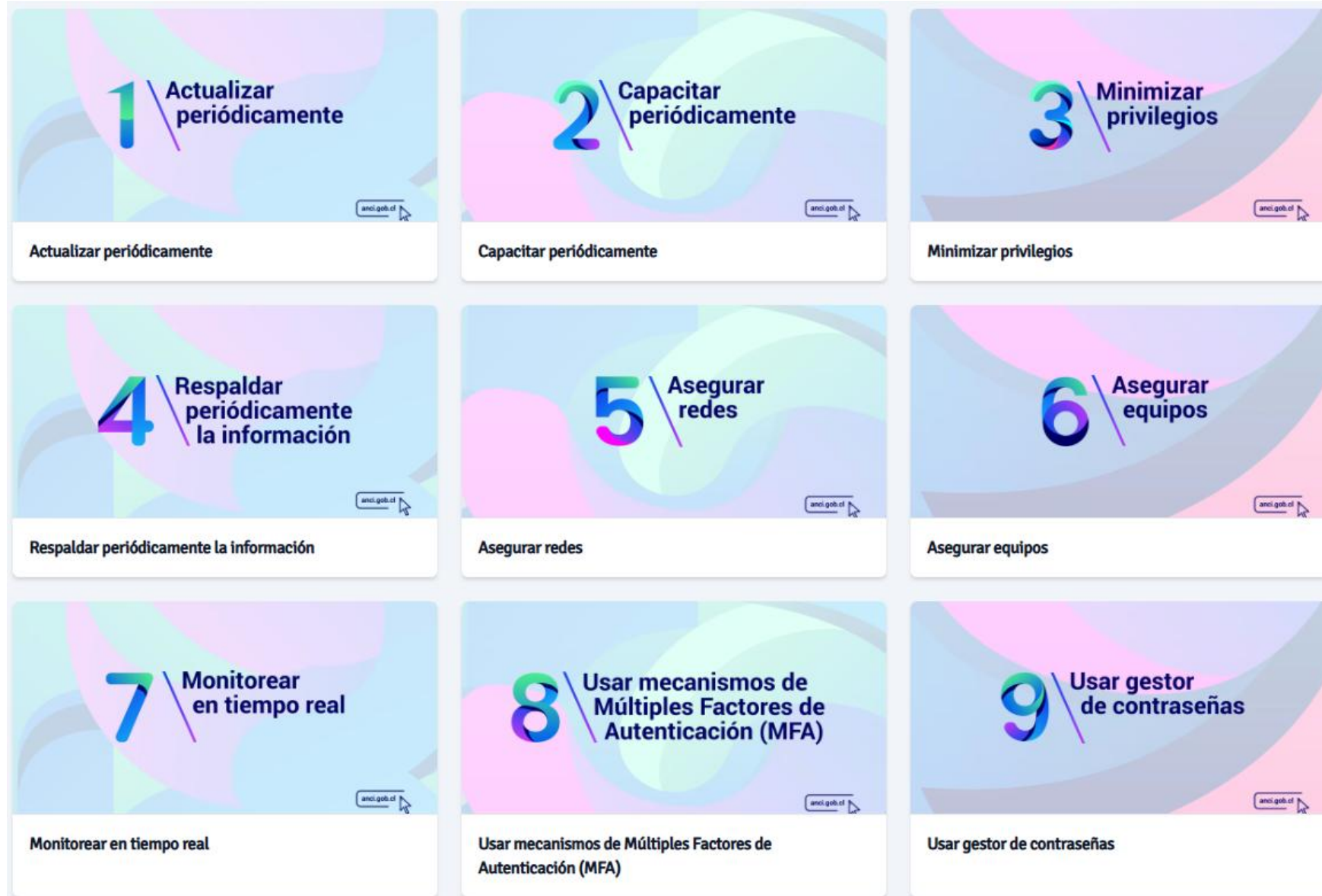
INCIDENTES 2026 POR TIPO



LOS REPORTE NOS PERMITEN HACER INVESTIGACIÓN DE AMENAZAS



9 BÁSICOS DE LA CIBERSEGURIDAD



CONSULTA BÁSICOS DE LA CIBERSEGURIDAD

1 / Actualizar
periódicamente

Actualizar periódicamente

2 / Capacitar
periódicamente

Capacitar periódicamente

4 / Respalda
periódicamente
la información

Respalda periódicamente la información

6 / Asegurar
equipos

Asegurar equipos

8 / Usar mecanismos de
Múltiples Factores de
Autenticación (MFA)

Usar mecanismos de Múltiples Factores de
Autenticación (MFA)

9 / Usar gestor
de contraseñas

Usar gestor de contraseñas

CONSULTA BÁSICOS DE LA CIBERSEGURIDAD



Se registraron **331 participantes** de organizaciones públicas y privadas de diversos sectores y tamaños.

Se recopiló un total de 395 observaciones durante el proceso llevado a cabo entre el **30 de mayo y el 29 de junio de 2026**.

Cerca del 80% de los participantes estima que requerirá un plazo razonable de entre 12 y 24 meses para implementar los seis controles propuestos.

CONTROL 8: USAR MECANISMOS DE MÚLTIPLES FACTORES DE AUTENTICACIÓN (MFA)

Más del 90% declara que el concepto y requisito del control es fácil de comprender.

Un 68,2% de las instituciones participantes indica tener el MFA completamente implementado.

El 63% percibe una complejidad relativa en su despliegue en comparación con otros controles más sencillos.



CONTROL 8: USAR MECANISMOS DE MÚLTIPLES FACTORES DE AUTENTICACIÓN (MFA)



PROTOCOLO N°1

IMPARTE ESTÁNDARES SOBRE LA IMPLEMENTACIÓN DE AUTENTICACIÓN MULTIFACTOR Y OTRAS MEDIDAS DE PREVENCIÓN DE INCIDENTES DE CIBERSEGURIDAD

A: LAS INSTITUCIONES QUE PRESTEN SERVICIOS CALIFICADOS COMO ESENCIALES SEGÚN LO ESTABLECIDO EN LOS INCISOS SEGUNDO Y TERCERO DEL ARTÍCULO 4° Y A AQUELLAS QUE SEAN CALIFICADAS COMO OPERADORES DE IMPORTANCIA VITAL, DE CONFORMIDAD CON LO DISPUESTO EN LOS ARTÍCULOS 5° Y 6°, TODOS DE LA LEY N°21.663.

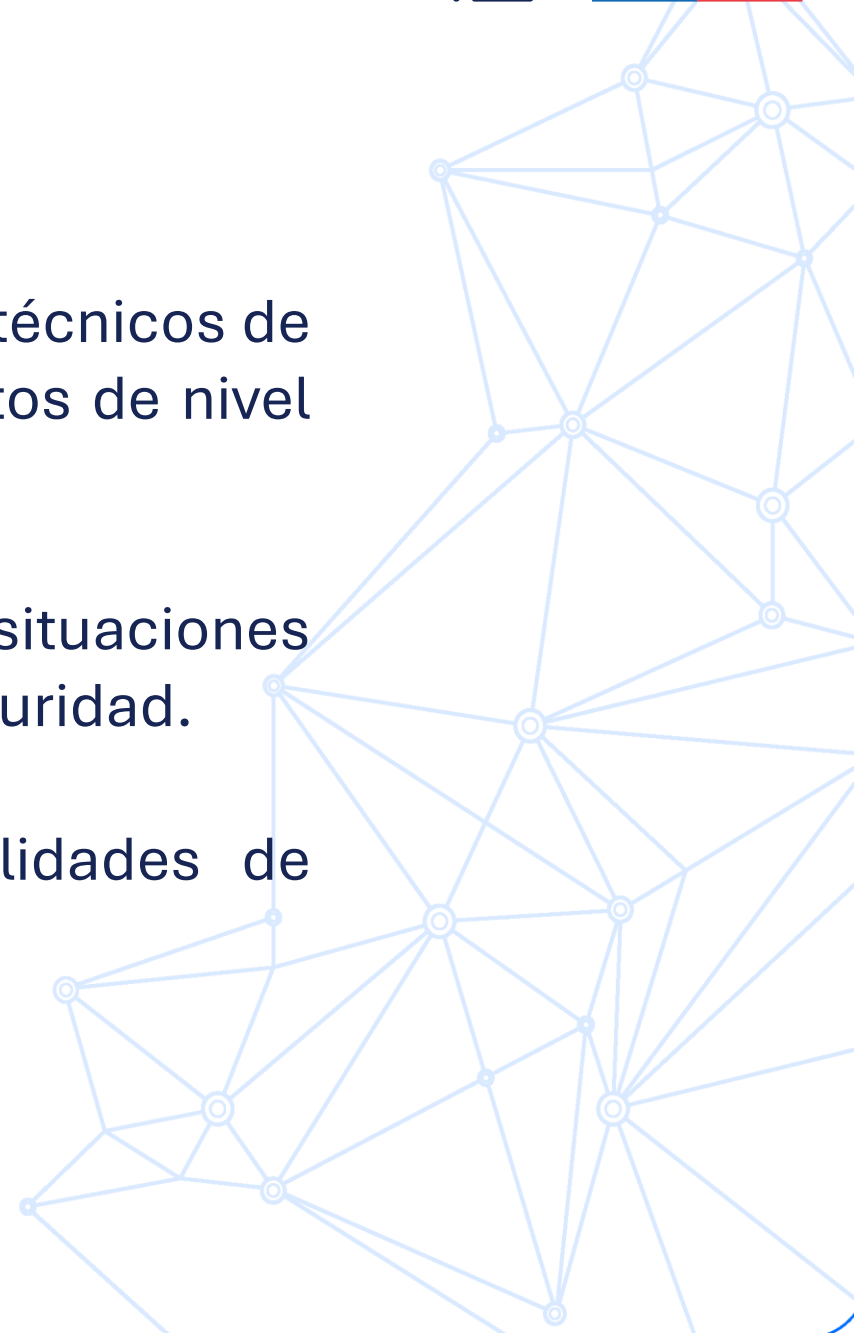
PRIMER EJERCICIO NACIONAL DE CIBERSEGURIDAD

Modalidad Capture the Flag (CTF)

Dirigido a encargados de ciberseguridad y equipos técnicos de instituciones públicas y privadas, con conocimientos de nivel intermedio.

Deberán resolver desafíos técnicos basados en situaciones que pueden presentarse en el ámbito de la ciberseguridad.

Cada desafío permitirá poner en práctica habilidades de análisis, investigación y resolución de problemas.



PORTAL DE REPORTE CIUDADANO



Gob.cl Sitio oficial del Gobierno de Chile ¿Cómo lo verifico?



Reportar

Programas de Bug Bounty Puerto Seguro Muro de la Fama Más Información

Te damos la bienvenida a la Plataforma de Reporte Ciudadano

Nuestra plataforma de Reporte Ciudadano permite reportar a la Agencia Nacional de Ciberseguridad indicios que ayuden a prevenir un incidente de ciberseguridad de forma rápida y segura.

Puedes acceder a la plataforma mediante un usuario anónimo o a través de ClaveÚnica. Esta última opción permite realizar el seguimiento de todos los reportes en un solo lugar, además de definir un pseudónimo para figurar en el Muro de la Fama.

Entrar con ClaveÚnica

Entrar anónimamente



Programas de Bug Bounty

Ver lista de programas activos

Revisa todos los programas de bug bounty activos y disponibles para reportar.



Puerto Seguro

Según Artículo 19

Usa esta opción para reportar indicios no contemplados en los programas activos.



Muro de la Fama

Lista de ciberinvestigadores destacados

Revisa la lista de ciberinvestigadores registrados con reportes validados.

LA AGENCIA LIDERA.

**LA CIBERSEGURIDAD LA CONSTRUIMOS
ENTRE TODOS**





anci.gob.cl