Registro de Incidente de Ciberseguridad

Completar desde el primer minuto — Un registro por incidente

Ley 21.663: si eres operador de importancia vital, tienes 3 horas para reportar a la ANCI. Resto de empresas: 24 horas. Reportar a csirt@anci.gob.cl

1. IDENTIFICACIÓN DEL INCIDENTE

ID del incidente (ej: INC-2026-001):

Fecha y hora de detección:

Detectado por (nombre y cargo):

Fecha y hora de notificación a TI:

Empresa / Unidad afectada:

Responsable del seguimiento:

Tipo de incidente (marcar todos los que apliquen):

- ☐ Ransomware / cifrado de datos
- ☐ Acceso no autorizado a sistemas
- ☐ Compromiso de cuenta de usuario
- ☐ DDoS / interrupción de servicio
- ☐ Pérdida o robo de dispositivo
- ☐ Phishing / ingeniería social
- ☐ Robo o exfiltración de datos
- ☐ Malware / virus
- ☐ Fraude (BEC, factura falsa)
- ☐ Otro:

2. DESCRIPCIÓN DEL INCIDENTE

Descripción inicial (qué ocurrió, cómo se detectó, síntomas observados):

Sistemas / equipos afectados:

IP / hostname (si aplica):

Datos potencialmente comprometidos:

Nro. aprox. de personas afectadas:

Gravedad estimada:

[ ] Crítica (servicio interrumpido, datos expuestos)

[ ] Alta (riesgo inminente)

[ ] Media (contenida, sin impacto externo)

[ ] Baja (anomalía menor)

3. CRONOLOGÍA DE ACCIONES

Fecha / Hora	Acción tomada	Responsable	Resultado

4. CONTENCIÓN Y MEDIDAS TOMADAS

- [ ] Sistemas afectados desconectados de la red (no apagados)
- [ ] Cuentas comprometidas bloqueadas / contraseñas restablecidas
- [ ] Backups verificados: intactos [ ] Sí [ ] No [ ] No verificado
- [ ] Evidencia preservada (logs, capturas de pantalla, memoria RAM)
- [ ] Proveedor externo de respuesta a incidentes contactado
- [ ] Comunicación a clientes/terceros afectados iniciada

5. REPORTES REGULATORIOS

¿Se debe reportar a la ANCI? [ ] Sí (completar abajo) [ ] No (justificar):_____

Reporte enviado a ANCI (fecha/hora):

Nro. de referencia ANCI:

¿Hay datos personales expuestos? [ ] Sí [ ] No

Titulares notificados (fecha):

6. RECUPERACIÓN

Vector de entrada identificado:

Fecha resolución del incidente:

Acciones de erradicación realizadas:

Lecciones aprendidas / mejoras a implementar:

7. CIERRE Y FIRMAS

Responsable TI (firma y fecha):

Gerencia (V°B° y fecha):