Checklist operativo de cumplimiento

Medidas obligatorias para reducir el impacto y la propagación de un incidente de ciberseguridad.

Instrucción general n°4 — ANCI. Conforme al artículo 8 literal e) de la Ley N° 21.663

Prey Inc.

Introducción

La Instrucción General N°4 de la Agencia Nacional de Ciberseguridad (ANCI) no introduce nuevas recomendaciones. Introduce obligaciones operativas inmediatas.

Su foco no está en políticas, sino en capacidad real de contención:

- Restringir accesos comprometidos
- Aislar sistemas afectados
- Suspender integraciones y servicios expuestos
- Gestionar identidades privilegiadas bajo plazo
- Implementar segmentación efectiva
- Registrar decisiones y resguardar evidencia

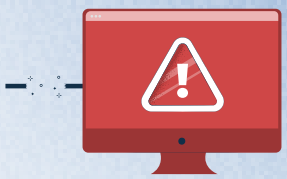
Algunas medidas deben ejecutarse dentro de las primeras **3 horas desde la detección del incidente**. Esto transforma la respuesta a incidentes desde una función reactiva hacia una capacidad operativa medible.

Este documento te permite evaluar, de forma rápida y objetiva, si tu organización está realmente preparada para cumplir.

Instrucciones Generales

Artículo 1:

Restricción y aislamiento inmediato



Obligación normativa	Qué significa realmente para TI	Acción concreta que debes poder ejecutar	Cómo validarlo hoy	¿Cumple?
Restringir accesos comprometidos	Cortar privilegios y accesos activos del atacante	• Deshabilitar cuentas sospechosas • Revocar tokens/ sesiones activas • Bloquear acceso a sistemas críticos	¿Sabes qué cuentas tienen privilegios hoy?	☐ Sí ☐ No ☐ Parcial
Aislar sistemas afectados	Separar activos comprometidos del resto de la red	• Aislar endpoints de forma remota • Desconectar VMs • Bloquear tráfico entre segmentos	¿Puedes aislar un equipo en menos de 10 minutos?	☐ Sí ☐ No ☐ Parcial
Suspender funcionalidades/ integraciones	Cortar puentes de propagación	• Pausar APIs • Deshabilitar accesos remotos • Detener sincronizaciones	¿Tienes mapeadas todas las integraciones críticas?	☐ Sí ☐ No ☐ Parcial
Interrumpir servicios si es necesario	Apagar para contener	• Suspender sitio web o servicio expuesto • Publicar aviso mitigatorio	¿Tienes protocolo de “apagado controlado”?	☐ Sí ☐ No ☐ Parcial

Artículo 2:

Gestión crítica de identidades (plazo 3 horas)

Obligación normativa	Qué significa para TI	Acción requerida	Validación interna	¿Cumple?
Cambiar contraseñas admin inmediatamente	Reset masivo de credenciales privilegiadas	• Cambiar passwords de cuentas admin • Revocar accesos privilegiados	¿Puedes listar todas las cuentas admin en minutos?	☐ Sí ☐ No ☐ Parcial
Eliminar cuentas genéricas/no usadas	Reducir vectores invisibles	• Auditar cuentas • Eliminar cuentas sin dueño activo	¿Cuántas cuentas genéricas existen hoy?	☐ Sí ☐ No ☐ Parcial
Ejecutar dentro de 3 horas e informar	Operar bajo deadline regulatorio	• Registrar cuentas modificadas • Reportar en alerta temprana	¿Tienes procedimiento documentado de 3 horas?	☐ Sí ☐ No ☐ Parcial
Revisión preventiva cada 6 meses	Higiene obligatoria	• Auditoría semestral de privilegios	¿Tienes calendario formal?	☐ Sí ☐ No ☐ Parcial

Artículo 3:

Accesos remotos y exposición pública

Obligación normativa	Qué implica	Acción técnica	Validación	¿Cumple?
Revisar exposición pública	Identificar puertas abiertas a Internet	• Escaneo de puertos • Inventario de servicios expuestos	¿Sabes qué está expuesto ahora mismo?	☐ Sí ☐ No ☐ Parcial
Bloquear en máximo 3 horas	Cerrar vectores de entrada	• Deshabilitar RDP/ SSH públicos • Cerrar paneles admin	¿Puedes hacerlo sin intervención física?	☐ Sí ☐ No ☐ Parcial
Permitir solo VPN o IP específicas	Acceso controlado	• Restringir por IP • Validar configuración VPN	¿Tu VPN soporta segmentación adecuada?	☐ Sí ☐ No ☐ Parcial
Aplicar MFA si es factible	Agregar capa adicional	• Activar MFA en accesos remotos	¿Todos los accesos críticos tienen MFA?	☐ Sí ☐ No ☐ Parcial
Deshabilitar tras finalizar tarea	Eliminar accesos temporales	• Bajar credenciales temporales	¿Tienes control sobre accesos excepcionales?	☐ Sí ☐ No ☐ Parcial

Artículo 4:

Protección de servicios expuestos

Mantenimiento

Obligación normativa	Qué significa	Acción operativa	Validación	¿Cumple?
Suspender servicios ante riesgo activo	Contener explotación	• Apagar portal público • Suspender transacciones	¿Tienes criterio claro de suspensión?	☐ Sí ☐ No ☐ Parcial
Informar suspensión como medida mitigatoria	Transparencia controlada	• Banner de mantenimiento de seguridad	¿Tienes mensaje preaprobado?	☐ Sí ☐ No ☐ Parcial
Redireccionar a entornos seguros	Minimizar exposición	• Redirigir a entornos internos protegidos	¿Existen entornos alternativos?	☐ Sí ☐ No ☐ Parcial
Usar cifrado robusto	Evitar interceptación	• Validar TLS • Revisar certificados	¿Has auditado tu configuración TLS?	☐ Sí ☐ No ☐ Parcial

Artículo 5:

Herramientas de detección y contención

Obligación normativa	Qué exige realmente	Acción técnica	Validación	¿Cumple?
Identificar dispositivos/ cuentas comprometidas	Visibilidad real	• Inventario actualizado • Telemetría activa	¿Tienes inventario en tiempo real?	☐ Sí ☐ No ☐ Parcial
Bloquear/aislar remoto	Contención sin desplazamiento físico	• Remote lock • Aislamiento de red • Deshabilitar cuenta	¿Puedes hacerlo en minutos?	☐ Sí ☐ No ☐ Parcial
Monitorear evolución y propagación	Seguimiento activo del ataque	• Alertas de movimiento lateral	¿Puedes detectar propagación?	☐ Sí ☐ No ☐ Parcial

Artículo 6:

Firewalls y bloqueo por defecto

Obligación normativa	Qué implica	Acción técnica	Validación	¿Cumple?
Instalar y operar firewalls adecuados	Perímetro activo	• Firewall configurado y monitoreado	¿Se revisan reglas periódicamente?	☐ Sí ☐ No ☐ Parcial
Bloqueo entrante por defecto (whitelisting)	Deny by default	• Regla base: bloquear todo salvo permitido	¿Tus reglas permiten más de lo necesario?	☐ Sí ☐ No ☐ Parcial
Supervisión periódica	Gobernanza técnica	• Auditoría de reglas	¿Existe revisión formal?	☐ Sí ☐ No ☐ Parcial

Artículo 7:

Segmentación y contención lateral

Obligación normativa	Qué significa	Acción operativa	Validación	¿Cumple?
Segmentación lógica/física	Red no plana	• Separar productivo, respaldo, admin	¿Tu red está segmentada realmente?	☐ Sí ☐ No ☐ Parcial
Aislar segmentos comprometidos	Confinar propagación	• Cortar tráfico entre zonas	¿Puedes hacerlo rápido?	☐ Sí ☐ No ☐ Parcial
Proteger respaldos	Backup fuera de alcance	• Separar red de backups	¿Backups están aislados?	☐ Sí ☐ No ☐ Parcial
Suspender credenciales/ integraciones compartidas	Eliminar puentes laterales	• Deshabilitar cuentas de servicio compartidas	¿Existen credenciales compartidas?	☐ Sí ☐ No ☐ Parcial

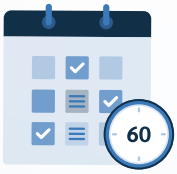
Artículo 8:

Registro, evidencia y coordinación

Obligación normativa	Qué implica	Acción operativa	Validación	¿Cumple?
Registrar decisiones	Bitácora formal	• Documentar cada acción tomada	¿Tienes plantilla estándar?	☐ Sí ☐ No ☐ Parcial
Resguardar evidencia	Integridad forense	• Guardar logs y evidencias de forma segura	¿La evidencia está protegida?	☐ Sí ☐ No ☐ Parcial
Comunicación continua con ANCI	Coordinación obligatoria	• Canal definido de reporte	¿Quién es responsable del contacto?	☐ Sí ☐ No ☐ Parcial
Informar a nivel directivo	Gobernanza ejecutiva	• Reporte ejecutivo inmediato	¿Existe protocolo de escalamiento?	☐ Sí ☐ No ☐ Parcial

Artículo 9:

Vigencia y adecuación



Obligación normativa	Qué implica	Acción estratégica	Validación	¿Cumple?
60 días desde calificación como OIV	Ventana limitada de cumplimiento	• Plan de adecuación técnica • Roadmap de implementación	¿Tienes plan con responsables y fechas?	☐ Sí ☐ No ☐ Parcial

Cómo aporta Prey en este contexto

Prey permite fortalecer tres capacidades clave alineadas con las exigencias regulatorias:

Visibilidad centralizada de endpoints

Inventario actualizado de dispositivos, ubicación, estado de seguridad y asignación por usuario o área.

Contención remota inmediata

Bloqueo de pantalla, borrado seguro, control de acceso y acciones ejecutables desde un panel centralizado.

Trazabilidad de acciones

Registro de actividades y medidas aplicadas sobre cada dispositivo, facilitando la documentación del incidente.

La normativa no exige una tecnología específica. Exige que puedas ejecutar contención en minutos y demostrarlo.

Agenda una conversación con nuestro equipo y revisemos juntos cómo mejorar el control y la gestión de tu flota de dispositivos frente a los nuevos estándares regulatorios.

Solicita tu demo personalizada

Sobre Prey

Nacimos en 2009 con una misión clara: devolverle a las personas el control sobre su tecnología. Hoy, Prey ha evolucionado en una **plataforma integral de gestión y seguridad para flotas globales**. Más allá del rastreo, empoderamos a las empresas con herramientas avanzadas para el manejo de software, cumplimiento de políticas y protección de datos.

Somos el aliado estratégico que ayuda a administrar y proteger entornos de trabajo remoto, facilitando el cumplimiento normativo. Un equipo comprometido con la continuidad de tu operación.

Prey para: **Personas** | **Organizaciones** | **Escuelas y Universidades**