AguasdelCesar
S.A. E.S.P.

PROTOCOLO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN MSPI

Nombre completo de la entidad	Aguas del Cesar S.A E.S.P
NIT	900.149.163-8
Municipio / Departamento	Valledupar, Cesar
Dirección sede principal	Calle 28 Nº 6A – 15
Sitio web	https://aguasdelcesar.gov.co/
Correo de contacto TIC	**sistemas@aguasdelcesar.com.co**

Contenido

1. INTRODUCCIÓN

Las entidades públicas colombianas están permanentemente expuestas a eventos disruptivos que pueden comprometer la confidencialidad, integridad y disponibilidad de sus activos de información. Un incidente de seguridad de la información puede tener consecuencias operativas, legales, reputacionales y financieras de diverso impacto.

El presente documento establece el Protocolo de Gestión de Incidentes de Seguridad de la Información de **Aguas del Cesar S.A. E.S.P.**, con fundamento en la Guía No. 21 del MSPI MinTIC, la NTC-ISO/IEC 27035, el NIST SP 800-61 y el marco normativo colombiano aplicable. Define el ciclo de vida completo de respuesta a incidentes: Preparación → Detección y Análisis → Contención, Erradicación y Recuperación → Actividades Post-Incidente.

2. OBJETIVOS

2.1 Objetivo General

Establecer los lineamientos, procedimientos, roles y responsabilidades para detectar, analizar, contener, erradicar y recuperarse de incidentes de seguridad de la información en Aguas del Cesar S.A. E.S.P., minimizando su impacto en la operación institucional y garantizando el cumplimiento de las obligaciones legales de notificación.

2.2 Objetivos Específicos

- Definir roles y responsabilidades claros para la gestión de incidentes mediante la Matriz RACI.
- Establecer la clasificación, priorización y tiempos de respuesta para cada tipo de incidente.
- Definir estrategias de contención, erradicación y recuperación por categoría de incidente.
- Establecer los criterios y canales de notificación a entidades externas (ColCERT, SIC, CCP, Fiscalía).
- Definir los criterios para escalar un incidente a nivel de crisis y activar el PMU / Mesa de Crisis.
- Garantizar la recolección y preservación de evidencia digital con criterios forenses.
- Consolidar lecciones aprendidas para mejorar continuamente la postura de seguridad.
- Cumplir con los lineamientos del MSPI MinTIC, GEL, ISO/IEC 27001:2022 y la normativa colombiana vigente.

3. ALCANCE

Este protocolo aplica a todos los activos de información, sistemas, servicios tecnológicos, redes, instalaciones y personas (servidores públicos, contratistas y terceros) que hagan parte de la infraestructura tecnológica de Aguas del Cesar S.A. E.S.P., independientemente del medio o plataforma en que se encuentren (on-premise, nube pública, nube híbrida, dispositivos móviles).

Cubre los siguientes tipos de eventos:

- Incidentes de seguridad de la información (ciberataques, fugas de datos, código malicioso, accesos no autorizados).
- Incidentes tecnológicos con impacto en la disponibilidad de servicios críticos.
- Violaciones de datos personales con obligación de notificación a la SIC (Ley 1581/2012).
- Eventos que puedan derivar en una crisis institucional o reputacional.

Inicia con la detección del evento y finaliza con el cierre del incidente, el balance post-incidente y la actualización de controles y procedimientos.

4. MARCO NORMATIVO Y DE REFERENCIA

Norma / Instrumento	Referencia
Ley 1273 de 2009	Delitos Informáticos en Colombia — tipifica acceso abusivo, daño informático, interceptación de datos, etc.
Ley 1581 de 2012 + Decreto 1074/2015	Protección de datos personales — obligación de notificar brechas a la SIC.
Ley 1712 de 2014	Transparencia y acceso a la información pública.
Ley 1928 de 2018	Aprobación del Convenio de Budapest sobre Ciberdelincuencia.
CONPES 3854 de 2016	Política Nacional de Seguridad Digital.
Decreto 1008 de 2018	Política de Gobierno Digital — Marco de Referencia GEL.
Resolución MinTIC 000002 de 2021	Manual de Gobierno Digital (GEL).
MSPI	Modelo de Seguridad y Privacidad de la Información
NTC-ISO/IEC 27001:2022	Sistema de Gestión de Seguridad de la Información — Numeral 6.1.2 y Anexo A 5.24-5.28.
NTC-ISO/IEC 27002:2022	Controles 5.24–5.28: Gestión de incidentes, eventos y debilidades de seguridad.
NTC-ISO/IEC 27035:2016	Guía de gestión de incidentes de seguridad de la información.
NIST SP 800-61 Rev. 2	Computer Security Incident Handling Guide — referencia técnica internacional.
NTC-ISO 22301:2019	Gestión de continuidad del negocio — referencia para escenarios de crisis.
Guía MinTIC No. 21 (MSPI)	Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.

5. DEFINICIONES

Término	Definición
Evento de seguridad	Ocurrencia identificada en un sistema, servicio o red que indica una posible violación de la política de seguridad (ISO/IEC 27035).
Incidente de seguridad	Uno o más eventos de seguridad no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (ISO/IEC 27001).
Crisis	Materialización de un incidente que sale de control y afecta negativamente las personas, la operación, la información, la tecnología o la reputación de la Entidad (NTC-ISO 22301).
Indicador de compromiso (IoC)	Evidencia forense de que un sistema puede haber sido comprometido (huella digital, hash, IP maliciosa, patrón de tráfico anómalo).
CSIRT	Computer Security Incident Response Team — Equipo de Respuesta a Incidentes de Seguridad Informática, o el grupo que haga sus veces en la entidad.
ColCERT	Grupo de Respuesta a Emergencias Cibernéticas de Colombia — entidad de nivel nacional para reportar incidentes graves.
CCP / CCIT	Centro Cibernético Policial de la Policía Nacional — punto de contacto para denuncias de delitos informáticos.
SIC	Superintendencia de Industria y Comercio — autoridad de protección de datos que debe ser notificada ante brechas de datos personales.
PMU / Mesa de Crisis	Puesto de Mando Unificado — instancia de alta dirección activada ante incidentes críticos o crisis.
Mesa de Incidentes	Instancia operativa de coordinación que analiza el incidente y diseña el Plan de Acción.
Nivel de Prioridad	Clasificación del incidente según fórmula: (Impacto actual × 2,5) + (Impacto futuro × 2,5) + (Criticidad del sistema × 5).
RTO (Recovery Time Objective)	Tiempo máximo tolerable para restablecer un servicio tras un incidente.
RPO (Recovery Point Objective)	Punto en el tiempo al que se puede restaurar la información sin impacto inaceptable.
BIA	Business Impact Analysis — Análisis de Impacto al Negocio, que define los procesos y servicios críticos.
Evidencia digital	Información almacenada o transmitida en forma digital que puede ser utilizada en un proceso disciplinario, administrativo o penal.
Lecciones aprendidas	Registro de causas, acciones tomadas y mejoras identificadas tras el cierre de un incidente.
Breach (brecha de datos)	Incidente que conlleva la destrucción accidental o ilícita, pérdida, alteración, divulgación o acceso no autorizado a datos

	personales.

6. CLASIFICACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La clasificación depende de la infraestructura, los riesgos y la criticidad de los activos de Aguas del Cesar S.A. E.S.P. La siguiente tabla establece las categorías base, que deben revisarse y ajustarse según el contexto específico de la entidad.

Categoría	Tipo de Incidente	Ejemplos
Acceso no autorizado	Intrusión lógica o física sin autorización del propietario del activo.	Inicio de sesión con credenciales robadas, acceso físico a servidor sin permiso, escalada de privilegios.
Modificación no autorizada	Alteración de la integridad de información o sistemas sin autorización.	Defacement web, manipulación de registros en BD, alteración de logs, ransomware.
Código malicioso	Infección o propagación de software diseñado para causar daño.	Virus, gusano, troyano, ransomware, spyware, rootkit, exploit.
Denegación de servicio (DoS/DDoS)	Impedimento del uso autorizado de un activo o servicio.	SYN Flood, amplificación DNS/NTP, saturación de ancho de banda.
Fuga o pérdida de información	Divulgación no autorizada de información confidencial o datos personales.	Exfiltración de BD, envío de archivos por correo no autorizado, pérdida de dispositivo de almacenamiento.
Fraude / Ingeniería social	Engaño deliberado para obtener información o acceso.	Phishing, vishing, smishing, suplantación de identidad (Business Email Compromise).
Uso inapropiado de recursos	Violación de política de uso aceptable de los recursos TIC.	Minería de criptomonedas en servidores de la entidad, descarga masiva de contenido ilegal.
Vulnerabilidad explotada	Aprovechamiento de una debilidad técnica conocida o desconocida (0-day).	Explotación de CVE publicado, inyección SQL, XSS, SSRF.
Incidente de disponibilidad	Interrupción no planificada de un servicio crítico no asociada a ataque.	Fallo de hardware, corte de energía, error de configuración que deja el servicio inaccesible.
Amenaza interna (insider)	Acción deliberada o accidental de un usuario interno que compromete la seguridad.	Empleado que copia BD antes de renunciar, administrador que borra respaldos por error.
Multicomponente	Incidente que involucra más de una de las categorías anteriores.	Ransomware que exfiltra datos antes de cifrar (fuga + modificación + código malicioso).

Otros	Incidentes no clasificables en las categorías anteriores — monitorear para crear nueva categoría.	Actividad anómala no tipificada, señal de alerta sin causa aparente.

7. EVALUACIÓN Y PRIORIZACIÓN DE INCIDENTES

7.1 Niveles de Criticidad del Sistema Afectado

Nivel Criticidad	Valor	Definición
Inferior	0,10	Sistemas no críticos — estaciones de trabajo de usuarios con funciones no críticas.
Bajo	0,25	Sistemas que apoyan a una sola dependencia o proceso de la entidad.
Medio	0,50	Sistemas que apoyan más de una dependencia o proceso de la entidad.
Alto	0,75	Sistemas del área TIC y estaciones de trabajo de usuarios con funciones críticas.
Superior	1,00	Sistemas críticos definidos en el BIA — máxima prioridad de atención.

7.2 Niveles de Impacto (Actual y Futuro)

Nivel Impacto	Valor	Definición
Inferior	0,10	Impacto leve en uno de los componentes de cualquier sistema de información o estación de trabajo.
Bajo	0,25	Impacto moderado en uno de los componentes de cualquier sistema de información o estación de trabajo.
Medio	0,50	Impacto alto en uno de los componentes de cualquier sistema de información o estación de trabajo.
Alto	0,75	Impacto moderado en uno o más componentes de más de un sistema de información.
Superior	1,00	Impacto alto en uno o más componentes de más de un sistema de información.

7.3 Fórmula de Priorización

Una vez determinados los tres componentes, se calcula la prioridad del incidente con la siguiente fórmula:

Nivel Prioridad = (Impacto Actual × 2,5) + (Impacto Futuro × 2,5) + (Criticidad del Sistema × 5)

7.4 Niveles de Prioridad y Tiempos Máximos de Atención

Nivel Prioridad	Rango (fórmula)	T. Máx. Atención	Color / Severidad
Inferior	0,00 – 2,49	3 horas	Verde — Bajo riesgo, monitorear
Bajo	2,50 – 3,74	1 hora	Amarillo — Atención normal
Medio	3,75 – 4,99	30 minutos	Naranja — Atención prioritaria
Alto	5,00 – 7,49	15 minutos	Rojo — Respuesta inmediata
Superior	7,50 – 10,00	5 minutos	Rojo crítico — Activar PMU / Mesa de Crisis

Nota: Los tiempos expresados corresponden al tiempo máximo de atención inicial (primera respuesta), no al tiempo de solución definitiva, que varía según la complejidad del incidente.

Nivel Prioridad	T. Máx. Respuesta	Acción inmediata requerida
Superior	5 minutos	Notificar al Jefe TIC, activar CSIRT, aislar sistema afectado, notificar a la dirección.
Alto	15 minutos	Activar CSIRT, iniciar contención, notificar al Jefe TIC.
Medio	30 minutos	Asignar analista, iniciar diagnóstico, documentar en herramienta de gestión.
Bajo	1 hora	Registrar en Mesa de Servicios, asignar según disponibilidad.
Inferior	3 horas	Registrar, monitorear, resolver en ventana de mantenimiento si aplica.

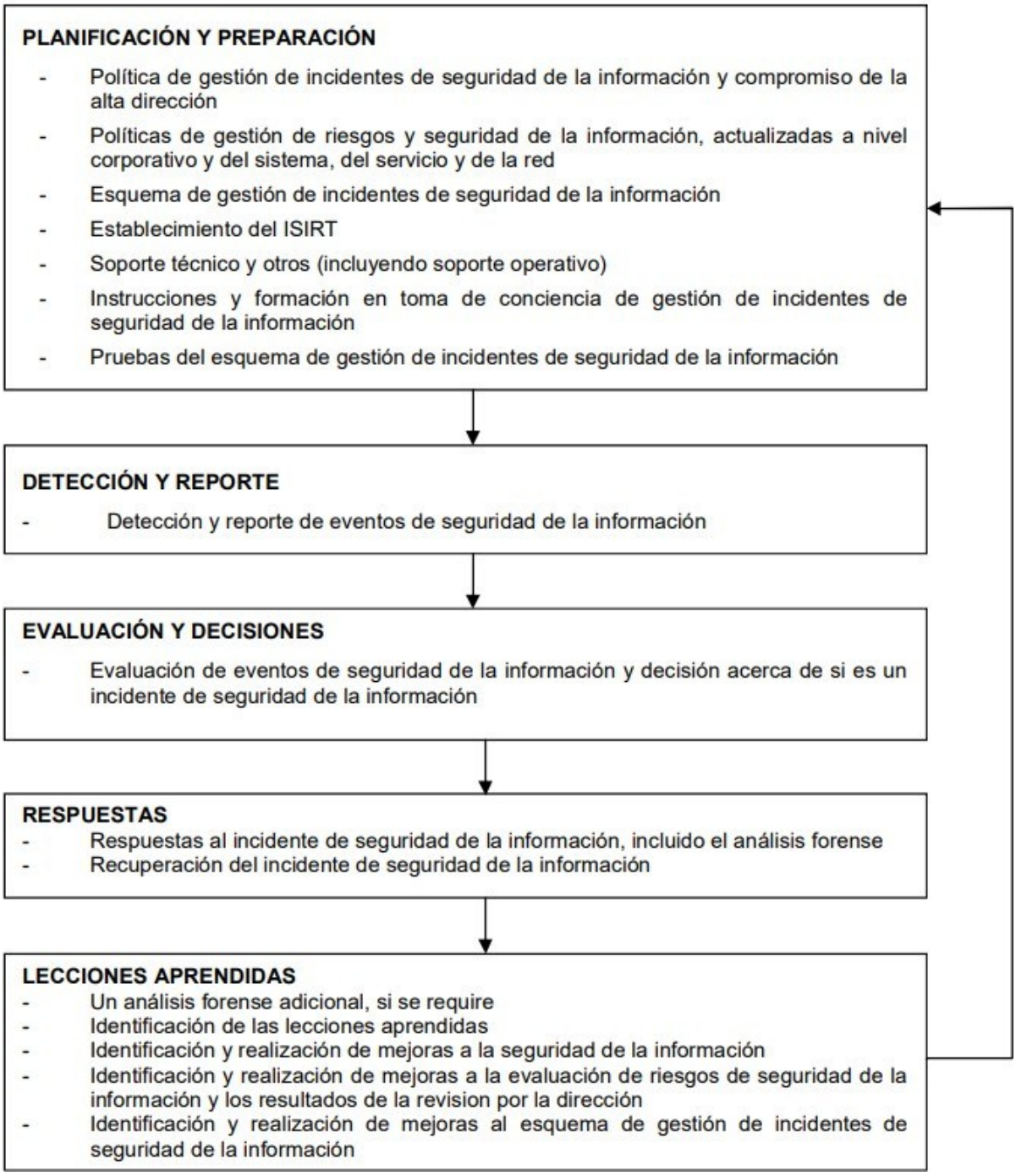
8. PROCEDIMIENTO — CICLO DE VIDA DEL INCIDENTE

En síntesis, el ciclo de vida del incidente sigue cuatro fases cíclicas alineadas con NIST SP 800-61 e ISO/IEC
27035: Preparación → Detección y Análisis → Contención, Erradicación y Recuperación → Post-Incidente.

No.	Fase	Descripción de la Actividad	Responsable	Tiempo Ref.
1	DETECCIÓN	El usuario, sistema de monitoreo, antivirus, SIEM o administrador detecta un evento anómalo (alerta, log sospechoso, reporte de usuario, caída de servicio).	Usuario / Sistema / Administrador	Continuo
2	REPORTE	El evento se notifica al Primer Punto de Contacto (Mesa de Servicios / Soporte) por cualquier canal disponible (teléfono, correo, aplicativo, presencial). Se diligencia el Formato de Reporte de Incidente.	Usuario / Administrador	Inmediato
3	REGISTRO Y CLASIFICACIÓN	El Primer Punto de Contacto registra el evento en la herramienta de gestión, verifica si corresponde a un incidente de seguridad (vs. requerimiento técnico) y aplica la tabla de clasificación (Sección 5). Asigna categoría y escala al CSIRT.	Primer Punto de Contacto	≤ 15 min
4	ANÁLISIS Y PRIORIZACIÓN	El CSIRT analiza los logs, alertas y evidencia inicial. Aplica la fórmula de prioridad: (Impacto actual × 2,5) + (Impacto futuro × 2,5) + (Criticidad del sistema × 5). Determina el nivel de prioridad y tiempo de respuesta (Sección 6).	CSIRT / Analista Seguridad	≤ 30 min
5	NOTIFICACIÓN INTERNA	El CSIRT / Jefe TIC notifica al Jefe TIC (si no lo inició) y a las áreas involucradas. Si es prioridad Alto o Superior: notificar inmediatamente a la Alta Dirección / PMU. Activar la Mesa de Incidentes si aplica.	CSIRT / Jefe TIC	Según prioridad
6	CONTENCIÓN	Se implementa la estrategia de contención definida para el tipo de incidente (Sección 8). Objetivo: evitar propagación y limitar el daño. Ejemplos: aislar sistema, bloquear IP, deshabilitar cuenta, revocar acceso. Documentar todas las acciones.	CSIRT / Administrador Sistema	Inmediato

7	RECOLECCIÓN DE EVIDENCIA	Antes de cualquier modificación: preservar logs, volcados de memoria, imágenes de disco, pcap de tráfico, capturas de pantalla. Aplicar principios de cadena de custodia. Si hay posibilidad de acción legal: activar Analista Forense.	CSIRT / Analista Forense	Simultáneo a contención
8	ERRADICACIÓN	Eliminar la causa raíz del incidente: desinstalar malware, cerrar vulnerabilidades, revocar accesos comprometidos, aplicar parches, restaurar configuraciones seguras. Verificar que el vector de ataque ha sido eliminado.	CSIRT / Administrador Sistema	Variable
9	RECUPERACIÓN	Restaurar los sistemas y servicios afectados a condiciones normales de operación, utilizando backups limpios o configuraciones validadas. Activar BCP/DRP si el impacto lo requiere. Monitorear activamente post-restauración.	CSIRT / Administrador / Jefe TIC	Según RTO

10	NOTIFICACIÓN EXTERNA	Según la naturaleza y gravedad: (a) ColCERT si se compromete infraestructura crítica o hay ciberataque grave; (b) SIC si hay brecha de datos personales (Ley 1581/2012); (c) CCP Policía Nacional si hay evidencia de delito informático (Ley 1273/2009); (d) Ciudadanos/usuarios si aplica.	Jefe TIC / CSIRT / Área Jurídica	≤ 72 h para brecha datos
11	CIERRE DEL INCIDENTE	El Jefe TIC declara el cierre cuando el incidente ha sido controlado, los servicios están restablecidos y la causa raíz ha sido eliminada. Notificar a todas las partes involucradas. Registrar cierre en la herramienta de gestión.	Jefe TIC / CSIRT	Post-recuperación
12	BALANCE POST-INCIDENTE (Lecciones Aprendidas)	Reunión del equipo involucrado para analizar: ¿qué ocurrió?, ¿cuándo?, ¿cómo se gestionó?, ¿qué se puede mejorar? Documentar lecciones aprendidas, actualizar procedimientos, políticas y controles. Registrar en base de conocimiento.	CSIRT / Jefe TIC / Áreas involucradas	≤ 5 días hábiles post-cierre


PLANIFICACIÓN Y PREPARACIÓN
- Política de gestión de incidentes de seguridad de la información y compromiso de la alta dirección
- Políticas de gestión de riesgos y seguridad de la información, actualizadas a nivel corporativo y del sistema, del servicio y de la red
- Esquema de gestión de incidentes de seguridad de la información
- Establecimiento del ISIRT
- Soporte técnico y otros (incluyendo soporte operativo)
- Instrucciones y formación en toma de conciencia de gestión de incidentes de seguridad de la información
- Pruebas del esquema de gestión de incidentes de seguridad de la información
DETECCIÓN Y REPORTE
- Detección y reporte de eventos de seguridad de la información
EVALUACIÓN Y DECISIONES
- Evaluación de eventos de seguridad de la información y decisión acerca de si es un incidente de seguridad de la información
RESPUESTAS
- Respuestas al incidente de seguridad de la información, incluido el análisis forense
- Recuperación del incidente de seguridad de la información
LECCIONES APRENDIDAS
- Un análisis forense adicional, si se require
- Identificación de las lecciones aprendidas
- Identificación y realización de mejoras a la seguridad de la información
- Identificación y realización de mejoras a la evaluación de riesgos de seguridad de la información y los resultados de la revision por la dirección
- Identificación y realización de mejoras al esquema de gestión de incidentes de seguridad de la información

9. ESTRATEGIAS DE CONTENCIÓN, ERRADICACIÓN Y RECUPERACIÓN POR TIPO DE INCIDENTE

Categoría Incidente	Ejemplo	Estrategia de Contención	Estrategia de Erradicación / Recuperación
Acceso no autorizado (login)	Sucesivos intentos fallidos de login	Bloqueo de cuenta / IP; habilitar MFA	Resetear credenciales; revisar logs de acceso; parche si aplica
Acceso no autorizado (root/admin)	Compromiso del usuario root	Apagado del sistema o desconexión de red	Reinstalación del OS; restaurar desde backup limpio; auditoría forense
Código malicioso (virus/gusano)	Infección con virus o gusano en red	Desconexión de la red del equipo afectado; cuarentena antivirus	Corrección de efectos; restauración de backups; actualizar firmas AV
Ransomware	Cifrado masivo de archivos	Aislar segmento de red; detener servicios compartidos; desconectar NAS/File Server	Restaurar desde backup previo al incidente; reformatear equipos; notificar ColCERT / SIC
DoS / DDoS	SYN Flood / amplificación DNS	Activar reglas de filtrado en firewall / WAF; escalar a proveedor de conectividad	Restitución del servicio; ajustar reglas; implementar scrubbing center
Defacement web	Modificación no autorizada de sitio web	Desconectar o poner sitio en mantenimiento	Restaurar contenido desde repositorio Git/backup; revisar accesos CMS
Phishing / BEC	Correo fraudulento con credenciales falsas	Bloquear dominio remitente; retirar correo de buzones	Resetear credenciales afectadas; revisar reglas de correo; sensibilizar usuarios
Fuga de datos (exfiltración)	Copia no autorizada de BD a exterior	Bloquear IP destino; revocar accesos del usuario involucrado	Análisis forense; notificar SIC (brecha de datos personales); notificar afectados
Reconocimiento / Scanning	Escaneo de puertos desde IP externa	Incorporar reglas de filtrado en firewall; bloquear IP origen	Revisar exposición de servicios; cerrar puertos innecesarios

Insider threat	Empleado copia BD antes de retiro	Revocar accesos inmediatamente; preservar evidencia	Auditoría forense; proceso disciplinario / penal; revisar controles DLP
Vulnerabilidad explotada (0-day)	Explotación de CVE crítico en producción	Deshabilitar el servicio afectado; aplicar workaround temporal	Aplicar parche del fabricante; pruebas de regresión; restaurar si hay corrupción

10. NOTIFICACIÓN EXTERNA — A QUIÉN DEBO INFORMAR

La notificación oportuna y precisa a las autoridades competentes es una obligación legal y una buena práctica. La siguiente tabla establece los criterios y canales de notificación externa para Aguas del Cesar S.A. E.S.P.:

Entidad	Cuando notificar	Canal de contacto	Plazo
ColCERT (Grupo Respuesta Cibernética Colombia)	Ciberataques que afecten infraestructura crítica, incidentes de alto impacto nacional.	contacto@colcert.gov.co / +57 601 344 2222	Lo antes posible — sin plazo legal fijo
CCP — Centro Cibernético Policial	Cuando hay evidencia de delito informático (Ley 1273/2009): intrusión, fraude, daño informático.	Página Web / Tel: 5159700	Lo antes posible — para proceso penal
SIC — Superintendencia de Industria y Comercio	Brecha de datos personales (violación de la Ley 1581/2012) que afecte titulares de datos.	Canal oficial SIC — Página Web	≤ 15 días hábiles desde el conocimiento (circular SIC vigente)
Fiscalía General de la Nación	Delitos informáticos que requieran investigación penal formal.	Denunciar ante Fiscalía local / DIJIN	Según urgencia del caso
Usuarios / Ciudadanos afectados	Brecha que afecte sus datos personales con riesgo significativo.	Correo electrónico, notificación en página web, comunicado de prensa.	Tan pronto como sea razonablemente posible
Medios de comunicación	Solo si el incidente es de dominio público o hay riesgo de desinformación — coordinado con Alta Dirección.	A través de la Oficina de Comunicaciones Institucionales.	Según Protocolo de Comunicaciones en Crisis
Proveedor de servicios en nube / hosting	Si el incidente se origina o afecta la infraestructura del proveedor.	Canal de soporte del proveedor (AWS, Azure, GCP, etc.).	Inmediato — para activar SLA de soporte

Consideraciones adicionales para notificación al CCP (Policía Nacional):

- Actualizar los datos de contacto del nombre de dominio .CO en el conforme al art. 5 de la Resolución 1652 de 2008.

- Si el incidente pone en riesgo la estabilidad del dominio, se puede solicitar su suspensión temporal mediante comunicación formal al CCP con asunción expresa de responsabilidad.

11. ROLES Y PERFILES PARA LA ATENCIÓN DE INCIDENTES

Rol	Perfil Recomendado	Responsabilidades Clave
Usuario / Servidor Público	Cualquier funcionario, contratista o tercero con acceso a recursos TIC.	Reportar eventos sospechosos al primer punto de contacto; no alterar evidencia; seguir instrucciones del CSIRT.
Primer Punto de Contacto (Mesa de Servicios)	Técnico con formación básica en seguridad de la información y clasificación de incidentes.	Recibir y registrar el reporte; clasificar si es incidente de seguridad o requerimiento técnico; escalar al CSIRT; hacer seguimiento hasta cierre.
Administrador de Sistemas	Profesional TI con conocimientos en SO, BD y redes; capacitación en técnicas forenses básicas.	Analizar logs; apoyar contención (desconectar equipo, revocar acceso); documentar cambios realizados; notificar al CSIRT.
Administrador de Seguridad (Firewall/IDS/SIEM)	Experto en seguridad de redes; conocimiento en Ethical Hacking y análisis de vulnerabilidades.	Gestionar elementos de seguridad perimetral; correlacionar eventos en SIEM; detectar y bloquear amenazas; documentar IoC.
Analista de Seguridad / CSIRT	Profesional certificado (CEH, CISSP, OSCP o equivalente); conocimiento en gestión de incidentes (NIST / ISO 27035).	Liderar la respuesta técnica; coordinar contención y erradicación; gestionar evidencia; elaborar informes técnicos; notificar a ColCERT/SIC.
Analista Forense	Experto en informática forense; conocimiento en cadena de custodia, admisibilidad de evidencia y judicialización.	Tomar, preservar y analizar evidencia digital; determinar causas raíz; emitir dictamen forense; apoyar proceso penal/disciplinario.
Jefe Oficina TIC / CISO	Directivo TIC con experiencia en SGSI y gestión de riesgos.	Activar la Mesa de Incidentes; coordinar con alta dirección; autorizar notificaciones externas (ColCERT, SIC, medios); supervisar el ciclo de vida del incidente; escalar a PMU si es crítico.
Alta Dirección / PMU	Director General, Subdirectores, asesores de comunicaciones, jurídica y RRHH.	Gestionar incidentes críticos o crisis; aprobar comunicados externos; tomar decisiones de impacto institucional; activar BCP/DRP.
Área Jurídica	Abogado con conocimiento en derecho TIC, protección de datos y delitos informáticos.	Asesorar sobre obligaciones legales de notificación; apoyar proceso disciplinario o penal; gestionar relaciones con la Fiscalía y el CCP.

Área de Comunicaciones	Comunicador institucional.	Gestionar comunicados a medios y ciudadanos; monitorear redes sociales; coordinar con el Protocolo de Comunicaciones en Momentos de Crisis.

12. MATRIZ RACI

Actividad	Jefe TIC / CISO	CSIRT / Analista Seg.	Administrador Sistema	Analista Forense	Alta Dirección
Recibir y registrar el evento / incidente	A	R	I		I
Clasificar y priorizar el incidente	A	R	C		I
Notificar a partes interesadas internas	R	A	I		I
Activar CSIRT / Mesa de Incidentes	R	A	I		I
Ejecutar contención	A	R	R	C	
Recolectar y preservar evidencia digital	A	C	C	R	
Ejecutar análisis forense (si aplica)	A	C	C	R	
Erradicación y recuperación	A	R	R	C	
Notificar a ColCERT / SIC / CCP	R	A			I
Escalar a PMU / Mesa de Crisis	R	A			A
Comunicar a medios / ciudadanos	C	I			R
Cierre y registro en base de conocimiento	A	R	I	I	I
Realizar balance post-incidente	A	R	C	C	I
Actualizar políticas y controles	A	R	C		I

Código	Significado
R — Responsible	Ejecuta la actividad.
A — Accountable	Responde por la calidad y resultado (máximo uno por actividad).
C — Consulted	Aporta información o criterio previo a la ejecución.

I — Informed	Recibe información sobre la ejecución o resultado.

14. PREPARACIÓN — RECURSOS Y ACTIVIDADES PREVIAS

La fase de preparación es la más importante del ciclo de vida. Una entidad bien preparada reduce drásticamente el tiempo de detección, contención y recuperación.

Recurso / Actividad	Descripción y Recomendación
COMUNICACIÓN — Lista de contactos del CSIRT	Directorio actualizado con nombres, cargos, teléfonos celulares y correos de todos los miembros del equipo de respuesta, incluyendo contactos de escalamiento.
COMUNICACIÓN — Escalamiento	Cadena de escalamiento documentada: Administrador → CSIRT → Jefe TIC → Alta Dirección / PMU. Incluir contactos de ColCERT, CCP, SIC, Fiscalía.
HARDWARE — Kit forense	Portátil forense (con herramientas instaladas offline), USB booteable con distribución forense (DEFT, Tails, Kali), bloqueadores de escritura, medios de almacenamiento vírgenes.
SOFTWARE — Análisis de incidentes	SIEM (centralización de logs), IDS/IPS, analizadores de protocolos (Wireshark), software de adquisición forense (FTK, Autopsy), escáner de vulnerabilidades (Nessus, OpenVAS).
SOFTWARE — Gestión de incidentes	Herramienta de ticketing/ITSM ([herramienta de la entidad]) para registro, seguimiento y cierre. Base de conocimiento de incidentes anteriores.
DOCUMENTACIÓN — Línea base de servidores	Inventario actualizado de servidores: nombre, IP, SO, aplicaciones, parches aplicados, usuarios configurados, responsable. Fundamental para identificar anomalías.
DOCUMENTACIÓN — Diagramas de red	Diagrama actualizado de la arquitectura de red para ubicar rápidamente los recursos afectados y los vectores de propagación posibles.
DOCUMENTACIÓN — Puertos y protocolos	Listado de puertos habilitados y de puertos comúnmente usados en ataques, para correlación rápida de alertas.
GESTIÓN — Parches de seguridad	Programa de gestión de vulnerabilidades para SO, BD, aplicaciones y firmware. Proceso de prueba e instalación de parches de seguridad en tiempo oportuno.
GESTIÓN — Aseguramiento de plataforma	Principio de mínimo privilegio, revisión de configuraciones por defecto, habilitación de auditoría en servidores, política de contraseñas robustas, MFA habilitado.
GESTIÓN — Seguridad en redes	Reglas de firewall revisadas periódicamente, firmas de IDS/IPS actualizadas, sincronización de relojes (NTP) para correlación de eventos, logs centralizados en SIEM.
GESTIÓN — Prevención de código malicioso	Antivirus/antimalware activo y actualizado en todos los equipos (servidores y estaciones de trabajo), solución EDR si es posible.

GESTIÓN — Sensibilización	Programa anual de capacitación y sensibilización en seguridad de la información para todos los servidores públicos, contratistas y terceros.
GESTIÓN — Ejercicios de simulación	Pruebas periódicas (tabletop exercises) del protocolo de incidentes para validar tiempos de respuesta, roles y procedimientos. Mínimo 1 vez al año.

14. RECOLECCIÓN Y PRESERVACIÓN DE EVIDENCIA DIGITAL

Cuando el incidente pueda derivar en acciones disciplinarias o penales, la evidencia digital debe tratarse con criterios forenses. El incumplimiento de estos principios puede hacer la evidencia inadmisible ante la autoridad competente.

14.1 Principios Básicos

- Orden de volatilidad: capturar primero la información más volátil (memoria RAM, conexiones de red activas, procesos en ejecución) antes que la información persistente (logs en disco, imágenes de disco).
- No modificar el sistema original — usar bloqueadores de escritura para discos; trabajar sobre copias forenses.
- Documentar cada acción: qué se hizo, quién lo hizo, cuándo y con qué herramienta.
- Cadena de custodia: mantener registro continuo de quién ha tenido acceso a cada pieza de evidencia.
- Dos aspectos clave de la evidencia: (a) Admisibilidad — si puede usarse en un proceso legal; (b) Peso
  — la calidad y completitud de la evidencia.

14.2 Tipos de Evidencia a Recolectar

- Logs de servidores, aplicaciones y dispositivos de seguridad (firewall, IDS, SIEM).
- Volcados de memoria RAM (memory dump) del sistema afectado.
- Imagen forense del disco duro (bit-a-bit) del sistema comprometido.
- Capturas de tráfico de red (pcap) en el momento del incidente.
- Correos electrónicos, chats y comunicaciones relevantes.
- Capturas de pantalla de sistemas y aplicaciones afectadas.
- Registros de acceso físico a instalaciones (si aplica).

15. BALANCE POST-INCIDENTE Y LECCIONES APRENDIDAS

Una de las fases más valiosas del ciclo de vida es el análisis post-incidente. Debe realizarse en un plazo máximo de 5 días hábiles tras el cierre, con participación del equipo involucrado.

15.1 Contenido del Balance Post-Incidente

1. Cronología exacta: qué ocurrió, en qué momento, cómo se detectó y cómo se gestionó.
2. Evaluación de procedimientos: ¿los procedimientos documentados fueron suficientes y efectivos?
3. Acciones que podrían haberse evitado o que dificultaron la recuperación.
4. Acciones correctivas para prevenir incidentes similares en el futuro.
5. Herramientas o recursos adicionales necesarios para mejorar la capacidad de detección y respuesta.
6. Actualización de mapas de riesgo, controles y procedimientos si aplica.
7. Retroalimentación a dependencias involucradas.
8. Análisis de coberturas de seguros y reclamaciones si hay lugar.
9. Actualización del presente protocolo si se identifican mejoras.

El Secretario de la Mesa de Incidentes documenta el balance en el Formato (Reporte de Incidentes — sección de balance post-incidente) y lo registra en la base de conocimiento del CSIRT.

16. INDICADORES DE GESTIÓN

Indicador	Fórmula / Medición	Meta Sugerida
% Incidentes registrados en herramienta de gestión	(Incidentes registrados / Incidentes reportados) × 100	100%
% Incidentes resueltos dentro del tiempo de respuesta	(Incidentes resueltos a tiempo / Total incidentes) × 100	≥ 95%
Tiempo promedio de detección (MTTD)	Suma de tiempos (detección – ocurrencia) / Número de incidentes	Reducir período a período
Tiempo promedio de contención (MTTC)	Suma de tiempos de contención / Número de incidentes	≤ RTO definido en BIA
Tiempo promedio de recuperación (MTTR)	Suma de tiempos de recuperación / Número de incidentes	≤ RTO definido en BIA
Número de incidentes por categoría (mensual)	Conteo por categoría de clasificación (Sección 5)	Tendencia decreciente en categorías recurrentes
% Incidentes con balance post-incidente documentado	(Incidentes con lecciones aprendidas / Total incidentes) × 100	100% para prioridad Alto/Superior; ≥ 80% general
% Incidentes que escalaron a crisis / PMU	(Incidentes escalados a PMU / Total incidentes) × 100	Minimizar; 0 para incidentes recurrentes previamente gestionados
Número de notificaciones externas realizadas a tiempo (SIC/ColCERT)	Conteo de notificaciones dentro del plazo legal / Total obligatorias	100%
% Ejercicios de simulación ejecutados	(Simulacros realizados / Simulacros programados) × 100	100% (mínimo 1 por año)

17. REGISTROS Y EVIDENCIAS

Responsable de diligenciar	Frecuencia	Herramienta / Ubicación
Usuario / Primer Punto de Contacto	Por cada evento reportado	Herramienta de gestión de incidentes / correo
CSIRT / Primer Punto de Contacto	Por cada incidente	ServiceDesk / Mesa de Ayuda
CSIRT / Administrador de Sistemas	Continuo durante el incidente	Documento Word / herramienta de gestión
Analista Forense / CSIRT	Por cada pieza de evidencia recolectada	Formato físico/digital de cadena de custodia
CSIRT / Analista Seguridad	Al cierre de cada incidente	Repositorio documental del SIG
Jefe TIC / Área Jurídica	Cuando aplique	Canal oficial de cada entidad
CSIRT / Jefe TIC	≤ 5 días hábiles post-cierre	Base de conocimiento / SIG
CSIRT / Jefe TIC	Mensual	Cuadro de mando / informe de gestión TIC
Jefe TIC / CSIRT	Mínimo anual	Repositorio documental del SIG

18. BIBLIOGRAFÍA Y REFERENCIAS

- MinTIC. (vigente). Modelo de Seguridad y Privacidad de la Información (MSPI) — Guía No. 21. https://www.mintic.gov.co/
- MinTIC. (vigente). Marco de Referencia de Arquitectura Empresarial (GEL). https://www.mintic.gov.co/arquitecturati/
- NIST. (2012). SP 800-61 Rev. 2 — Computer Security Incident Handling Guide. https://csrc.nist.gov/
- ICONTEC. (2016). NTC-ISO/IEC 27035 — Gestión de Incidentes de Seguridad de la Información.
- ICONTEC. (2022). NTC-ISO/IEC 27001:2022 — Sistemas de Gestión de Seguridad de la Información.
- ICONTEC. (2022). NTC-ISO/IEC 27002:2022 — Controles de Seguridad de la Información.
- ICONTEC. (2019). NTC-ISO 22301:2019 — Gestión de Continuidad del Negocio.
- Ley 1273 de 2009 — Delitos Informáticos. Congreso de la República de Colombia.
- Ley 1581 de 2012 — Protección de Datos Personales. Congreso de la República de Colombia.
- CONPES 3854 de 2016 — Política Nacional de Seguridad Digital. DNP.
- Decreto 1008 de 2018 — Política de Gobierno Digital. Presidencia de la República.
- DIAN. (2025). Protocolo de Manejo de Incidentes e Identificación de Crisis — OD-PEC-0003 v3. [Documento de referencia procedimental].

21. CONTROL DE CAMBIOS

Versión	Fecha	Responsable	Descripción del Cambio
1.0	13/04/2026	Profesional de Gestión de Tics	Creación del documento.

22. RUTA DE APROBACIÓN

Elaboró	Revisó	Aprobó
JANOS CONSULTORES SAS	Profesional de Gestión de Tics	Jefe de oficina asesora de planeación