RESOLUCIÓN No. ARCOTEL-2024-0271

LA AGENCIA DE REGULACIÓN Y CONTROL DE LAS TELECOMUNICACIONES ARCOTEL

CONSIDERANDO:

Que, la Constitución de la República del Ecuador, manda:

*"**Art. 226**.- Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley. Tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución.*

***Art. 227**.- La administración pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación.";*

Que, mediante Decreto Ejecutivo No. 8, de 13 de agosto de 2009, publicado en el Registro Oficial No. 10, de 24 de agosto de 2009, el Presidente de la República del Ecuador creó el Ministerio de Telecomunicaciones y de la Sociedad de la Información, como el órgano rector del desarrollo de las Tecnologías de la Información y Comunicación, que incluye las telecomunicaciones y el espectro radioeléctrico;

Que, la Ley Orgánica de Telecomunicaciones, publicada en el Registro Oficial Suplemento No. 439, del 18 de febrero de 2015, dispone:

*"**Art. 142.- Creación y naturaleza. -** Créase la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) como persona jurídica de derecho público, con autonomía administrativa, técnica, económica, financiera y patrimonio propio, adscrita al Ministerio rector de las Telecomunicaciones y de la Sociedad de la Información. La Agencia de Regulación y Control de las Telecomunicaciones es la entidad encargada de la administración, regulación y control de las telecomunicaciones y del espectro radioeléctrico y su gestión, así como de los aspectos técnicos de la gestión de medios de comunicación social que usen frecuencias del espectro radioeléctrico o que instalen y operen redes.*

*(…) **Art. 147.- Director Ejecutivo. -** La Agencia de Regulación y Control de las Telecomunicaciones será dirigida y administrada por la o el director ejecutivo, de libre nombramiento y remoción del Directorio.*

Con excepción de las competencias expresamente reservadas al Directorio, la o el Director Ejecutivo tiene plena competencia para expedir todos los actos necesarios para el logro de los objetivos de esta Ley y el cumplimiento de las funciones de administración, gestión, regulación y control de las telecomunicaciones y del espectro radioeléctrico, así como para regular y controlar los aspectos técnicos de la gestión de medios de comunicación social que usen frecuencias del espectro radioeléctrico o que instalen y operen redes, tales como los de audio y vídeo por suscripción.

Ejercerá sus competencias de acuerdo con lo establecido en esta Ley, su Reglamento General y las normas técnicas, planes generales y reglamentos que

emita el Directorio y, en general, de acuerdo con lo establecido en el ordenamiento jurídico vigente.

Art. 148.- Atribuciones del Director Ejecutivo. *Corresponde a la Directora o Director Ejecutivo de la Agencia de Regulación y Control de las Telecomunicaciones:*

(…)

11. *Aprobar la normativa interna, suscribir los contratos y emitir los actos administrativos necesarios para el funcionamiento de la Agencia de Regulación y Control de las Telecomunicaciones. (…)";*

Que, la Ley Orgánica para la Transformación Digital y Audiovisual, publicada en el Registro Oficial Suplemento No. 245, del 07 de febrero de 2023, dispone:

*"**Artículo 3.- Rectoría.** El ente rector en materia de telecomunicaciones será la entidad rectora en transformación digital y gobierno digital, para lo cual ejercerá atribuciones y responsabilidades, así como emitirá las políticas, directrices, acuerdos, normativa y lineamientos necesarios para su implementación.*

*(…) **Artículo 7.- Atribuciones del ente rector de transformación digital.** El ente rector de la transformación digital tendrá las siguientes atribuciones:*

*(…) **b.** Emitir políticas públicas, lineamientos, metodologías, regulaciones para la transformación digital, gobierno digital y evaluar su cumplimiento por parte de las entidades del sector público.*

*(…) **Artículo 19.- Gestión del Marco de Seguridad Digital.** El Marco de Seguridad Digital del Estado se tienen que observar y cumplir con lo siguiente:*

*(…) **d. Institucional:** Las entidades de la Administración Pública deberán establecer, mantener y documentar un Sistema de Gestión de la Seguridad de la Información. (…)*

***Artículo 20.- Articulación de la Seguridad Digital con la Seguridad de la Información.** El Marco de Seguridad Digital se articula y sustenta en las normas, procesos, roles, responsabilidades y mecanismos regulados e implementados a nivel nacional en materia de Seguridad de la Información. La Seguridad de la Información se enfoca en la información, de manera independiente de su formato y soporte. La seguridad digital se ocupa de las medidas de la seguridad de la información procesada, transmitida, almacenada o contenida en el entorno digital, procurando generar confianza, gestionando los riesgos que afecten la seguridad de las personas y la prosperidad económica y social en dicho entorno."*

Que, mediante Acuerdo Ministerial No. 011-2018, publicado en el Registro Oficial Edición Especial No. 612, de 08 de noviembre de 2018, se expidió el Plan Nacional de Gobierno Electrónico 2018-2021; y en el Capítulo 1. Fundamentos Generales, numeral 5. "Diagnóstico", se estableció que el diagnóstico del gobierno electrónico en Ecuador es analizado desde lo perspectiva de los tres programas del plan: Gobierno Abierto, Gobierno Cercano y Gobierno Eficaz y Eficiente, enfatizando en el número 5.2 "Gobierno cercano", que: *"Dentro de las iniciativas relevantes que ha implementado el gobierno en torno a la ciberseguridad se encuentra: la implementación y gestión del Esquema Gubernamental de Seguridad de la Información (EGSI),...";*

Que, con Acuerdo Ministerial No. 015-2019, publicado en el Registro Oficial No. 69, de 28 de octubre del 2019, se expidió la Política Ecuador Digital cuyo objeto es transformar al país hacia una economía basada en tecnologías digitales, mediante la disminución de la brecha digital, el desarrollo de la Sociedad de la Información y del Conocimiento, el Gobierno Digital, la eficiencia de la administración pública y la adopción digital en los sectores sociales y económicos;

Que, con Decreto Ejecutivo No. 981, publicado en el Registro Oficial Suplemento No. 143, de 14 de febrero del 2020, se dispuso sobre el gobierno electrónico, que: *"La implementación del gobierno electrónico en la Función Ejecutiva, consiste en el uso de las tecnologías de la información y comunicación por parte de las entidades para transformar las relaciones con los ciudadanos, entre entidades de gobierno y empresas privadas a fin de mejorar la calidad de los servicios gubernamentales a los ciudadanos, promover la interacción con las empresas privadas, fortalecer la participación ciudadana a través del acceso a la información y servicios gubernamentales eficientes y eficaces y coadyuvar con la transparencia, participación y colaboración ciudadana"*;

Que, con Acuerdo Ministerial No. MINTEL-MINTEL2022-0031, publicado en el Registro Oficial No. 198, de 28 de noviembre de 2022, se emitió la Política para la Transformación Digital del Ecuador 2022-2025, con el objetivo de *"(…) establecer los lineamientos para fomentar la Transformación Digital del Ecuador, considerando la investigación, desarrollo e innovación sobre infraestructuras y capacidades digitales, así como la digitalización de las empresas y servicios públicos, fomentando el uso de tecnologías emergentes, gestión de datos, seguridad de la información e interoperabilidad hacia todos los sectores sociales del país, considerando el desarrollo de un entorno normativo, regulatorio e institucional"*;

Que, mediante Acuerdo Ministerial No. MINTEL-MINTEL-2024-0003, de 08 de febrero de 2024, publicado en el Registro Oficial - Tercer Suplemento No. 509 de 1 de marzo de 2024, el Ministerio de Telecomunicaciones y de la Sociedad de la Información, expidió el Esquema Gubernamental de Seguridad de la Información - EGSI, mismo que establece que su implementación es obligatoria en las entidades, organismos e instituciones del sector público.

Que, mediante Memorando No. ARCOTEL-ARCOTEL-2024-0109-M, de 22 de marzo de 2024, la Dirección Ejecutiva de la ARCOTEL, designó al Magister Marcelo Ricardo Filián Narváez, como Oficial de Seguridad de la Información de la ARCOTEL.

Que, mediante Resolución No. 03-02SE-ARCOTEL-2024, de 19 de junio de 2024, el Directorio de la ARCOTEL, resolvió designar al señor Mgs. Jorge Roberto Hoyos Zabala, como Director Ejecutivo de la Agencia de Regulación y Control de Telecomunicaciones (ARCOTEL);

Que, el Director Ejecutivo de la ARCOTEL, cumpliendo lo dispuesto en el Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003, de 08 de febrero de 2024, con sumilla inserta el 28 de junio de 2024, en Memorando Nro. ARCOTEL-CPGE-2024-0402-M de 21 de junio de 024, aprobó y suscribió la Política Institucional de Seguridad de la Información de Alto Nivel, así como las Políticas Institucionales específicas de Seguridad de la información, referidas a controles organizacionales, de personas, físicos y tecnológicos, las mismas que son de cumplimiento obligatorio para funcionarios, servidores y terceras personas que tienen relación con la Institución.

Que, para dar cumplimiento a la implementación del Esquema Gubernamental de Seguridad de la Información en la Institución descrito en el Acuerdo Ministerial Nro.

MINTEL-MINTEL-2024-0003, de 08 de febrero de 2024, publicado en el Registro Oficial - Tercer Suplemento No. 509 de 1 de marzo de 2024, así como para dar cumplimiento a lo dispuesto a la Políticas Institucionales de Seguridad de la Información de alto nivel y específicas en la que hacen referencia a Gestión de Crisis, a través del Informe No. IT-CCDR-OSI-2024-007, de 23 de septiembre de 2024, la Presidente del Comité de Seguridad de la Información, aprobó y suscribió el *"Informe de motivación para la conformación del Comité de Crisis en la ARCOTEL"*; así también la Dirección de Asesoría Jurídica emitió el Informe Jurídico No. ARCOTEL-CJDA-2024-0050 de 15 de noviembre de 2024 con asunto: Informe Jurídico sobre la propuesta reglamentaria denominada " REGLAMENTO INTERNO PARA EL FUNCIONAMIENTO DEL COMITÉ DE CRISIS DE LA AGENCIA DE REGULACIÓN Y CONTROL DE LAS TELECOMUNICACIONES".

En ejercicio de las facultades conferidas en el artículo 148 la Ley Orgánica de Telecomunicaciones y demás normas señaladas**:**

RESUELVE:

Expedir el **"REGLAMENTO INTERNO PARA EL FUNCIONAMIENTO DEL COMITÉ DE CRISIS DE LA AGENCIA DE REGULACIÓN Y CONTROL DE LAS TELECOMUNICACIONES"**

SECCIÓN I
DEL COMITÉ DE CRISIS

Artículo 1. El Comité de crisis. - El Comité de Crisis de la Agencia de Regulación y Control de las Telecomunicaciones, es un órgano administrativo encargado de gestionar, tomar decisiones y coordinar las acciones necesarias para hacer frente o resolver emergencias calificadas como crisis, dentro de la institución, referente a situaciones críticas, como, por ejemplo:

- Crisis de seguridad (ataques cibernéticos, ataques informáticos internos, robo de activos de información y asociados, filtración de datos personales)
- Crisis de comunicación y reputación (afectación a la imagen y reputación de la institución en redes sociales y medios de comunicación),
- Crisis de operaciones (interrupciones en la cadena de suministro, fallos técnicos, interrupción de servicios básicos),
- Crisis de tecnología (fallos de sistemas críticos, daño del Centro de Datos, pérdida de datos y de información)
- Crisis de salud pública (epidemias, pandemias)
- Crisis ambiental (desastres naturales)
- Crisis financiera (crisis económica),
- Crisis administrativa (conflictos laborales que afecten a los activos de información y asociados de la Institución por incumplimiento de Políticas Institucionales de Seguridad de la Información y reglamentos internos)
- Crisis de gestión (problemas en la atención oportuna de trámites administrativos en la Institución)

Artículo 2. Objeto. - La presente norma tiene como objeto**,** regular el funcionamiento del Comité de Crisis de la ARCOTEL para:

a) Reducir el impacto de una crisis.
b) Proteger la reputación de la Institución.

c) Minimizar pérdidas financieras y de activos de información y asociados.
d) Garantizar la seguridad de funcionarios, servidores y Prestadores de Servicios de Telecomunicaciones que acceden a los servicios de la ARCOTEL.
e) Mantener la continuidad y oportunidad de las operaciones y servicios que presta la ARCOTEL.
f) Mejorar la respuesta en futuras crisis.

Artículo 3.- Ámbito. - Las disposiciones emitidas por el Comité de Crisis serán de aplicación obligatoria a nivel nacional para todas las Unidades Administrativas, Organismos Desconcentrados, Oficinas Técnicas, funcionarios, servidores y terceros asociados a la Institución.

Artículo 4.- Integración. - El Comité de Crisis estará integrado por los siguientes miembros:

a) Director Ejecutivo;
b) Oficial de Seguridad de la Información;
c) Delegado/a de Protección de Datos Personales
d) Coordinador/a General de Planificación y Gestión Estratégica;
e) Coordinador/a Técnico/a de Control;
f) Coordinador/a Técnico/a de Regulación;
g) Coordinador/a Técnico/a de Títulos Habilitantes;
h) Coordinador/a General Jurídico/a;
i) Coordinador/a General Administrativo/a Financiero/a;

La designación de los miembros del Comité de Crisis y su participación en las respectivas reuniones de trabajo es indelegable.

Artículo 5. Del Presidente del Comité de Crisis. – El Directo/a Ejecutivo/a de la ARCOTEL o su delegado presidirá el Comité de Crisis y será responsable de:

a) Aprobar el orden del día propuesto;
b) Convocar, instalar, presidir, suspender, diferir o clausurar las sesiones del Comité de Crisis;
c) Solicitar al Secretario del Comité de Crisis que proceda a tomar los votos de los miembros al concluir la discusión de los puntos del orden del día que requieran de aprobación;
d) Actuar con voto dirimente cuando el proceso de votación así lo requiera;
e) Cumplir y hacer cumplir acuerdos, decisiones y resoluciones aprobados por el Comité de Crisis y requerir de los responsables, los avances de cumplimiento;
f) Autorizar la participación de funcionarios y servidores invitados a las sesiones cuando hayan sido convocados para tratar temas específicos sujetos a deliberación; y,
g) Suscribir las actas del Comité de Crisis juntamente con el Secretario y los demás miembros.
h) Notificar, para su gestión y cumplimiento, los acuerdos, decisiones y resoluciones adoptados por el Comité de Crisis a las Unidades Administrativas correspondientes.
i) Nombrar un Secretario Ad-hoc entre los miembros del comité, en caso de ausencia temporal del Secretario del Comité de Crisis.

Artículo 6. Del Secretario del Comité de Crisis. – El Director de Tecnologías de la Información y Comunicación de la ARCOTEL actuará como Secretario del Comité de Crisis; y, le corresponderá:

a) Una vez que, el Oficial de Seguridad de la Información, haya determinado que se debe convocar a un Comité de Crisis acorde al nivel de peligrosidad de un incidente, elaborará el orden del día de las sesiones, y pondrá en consideración del Presidente del Comité de Crisis;
b) Elaborar las convocatorias a las sesiones para que sean aprobadas por el Presidente del Comité de Crisis e incluir los documentos de los temas por tratarse;
c) Consolidar la información remitida por las Unidades Administrativas y Organismos Desconcentrados de la ARCOTEL de ser el caso, para ser presentada en las sesiones;
d) Constatar el quorum necesario para la instalación de las sesiones y mantener un registro de los asistentes;
e) Dar lectura al orden del día respectivo, así como al acta aprobada de la sesión anterior en caso de reuniones ordinarias;
f) Mantener un registro de las sesiones, elaborar y suscribir las actas dando fe de su veracidad y contenido;
g) Mantener y custodiar los expedientes del Comité de Crisis que contendrán las actas de las sesiones debidamente codificadas, convocatorias, listas de asistencia, órdenes del día, informes y otros documentos relacionados con la gestión del Comité;
h) Conceder, cuando le sean requeridas, copias certificadas de la documentación que reposa en los expedientes, previa aprobación del presidente del Comité de Crisis, y;
i) Supervisará y verificará el cumplimiento de las disposiciones tomadas por el Comité de Crisis.

Artículo 7.- De las competencias del Comité de Crisis y sus miembros. - El Comité de Crisis tendrá las siguientes atribuciones:

a) El Oficial de Seguridad de la Información, debe **determinar la pertinencia de convocar a un Comité de Crisis** acorde al nivel de peligrosidad de un incidente en la Institución.
b) **Evaluación de la situación:** Analizar la crisis y determinar su impacto.
c) **Toma de decisiones:** Tomar decisiones rápidas e informadas para mitigar el daño.
d) **Coordinación:** Coordinar esfuerzos entre Unidades Administrativas, Organismos Desconcentrados de la ARCOTEL y terceros.
e) **Comunicación:** Gestionar la comunicación interna y externa.
f) **Gestión de recursos:** Asignar recursos para abordar la crisis a través de las Unidades Administrativas competentes de la Institución.
g) **Análisis de riesgos:** Identificar y mitigar riesgos asociados.
h) **Recuperación:** Planificar la recuperación y restauración de los activos de información y asociados de la Institución.

SECCIÓN II
PARÁMETROS PARA LA CALIFICACIÓN DE UNA CRISIS

Artículo 8.- Nivel de peligrosidad real de un incidente que puede provocar una crisis. - Se debe considerar el nivel de peligrosidad de los incidentes (asignación de prioridades, recursos, entre otros) y determinar la peligrosidad potencial que el incidente posee.

La peligrosidad de un incidente debería tener los siguientes niveles:

- L1 – Nivel Bajo
- L2 – Nivel Medio
- L3 – Nivel Alto

- L4 – Nivel Muy Alto
- L5 – Nivel Crítico

a) **L1 – Nivel Bajo:** Taxonomía de incidentes asociados a este nivel de peligrosidad:
- SPAM
- Escaneo de Redes (SCANNING)
- Análisis de Paquetes (SNIFFING)
- Otros incidentes de bajo impacto para la Institución calificados por el Oficial de Seguridad de la Información.

b) **L2 – Nivel Medio:** Taxonomía de incidentes asociados a este nivel de peligrosidad:
- Discurso de odio
- Ingeniería Social
- Explotación de Vulnerabilidades conocidas
- Intentos de acceso no autorizado
- Vulneración de credenciales
- Compromiso de cuentas sin privilegios
- Uso no autorizado de recursos
- Derechos de autor
- Suplantación
- Criptografía Débil
- Denegación de Servicios (DoS)
- Servicios con acceso potencial no deseado
- Revelación de Información
- Sistemas Vulnerables
- Otros incidentes de mediano impacto para la Institución calificados por el Oficial de Seguridad de la Información.

c) **L3 – Nivel Alto:** Taxonomía de incidentes asociados a este nivel de peligrosidad:
- Pornografía infantil
- Contenido sexual o violento inadecuado
- Sistema infectado
- Compromiso de aplicaciones
- Compromiso de cuentas con privilegios
- Ataque desconocido
- Denegación de Servicios Distribuida (DDoS)
- Acceso no autorizado a información
- Pérdida de datos
- Phishing
- Otros incidentes de alto impacto para la Institución calificados por el Oficial de Seguridad de la Información

d) **L4 – Nivel Muy Alto:** Taxonomía de incidentes asociados a este nivel de peligrosidad:
- Distribución de malware (código malicioso)
- Configuración de malware (código malicioso)
- Robo
- Sabotaje
- Interrupciones
- Otros incidentes de muy alto impacto para la Institución calificados por el Oficial de Seguridad de la Información

e) **L5 – Nivel Crítico:** Taxonomía de incidentes asociados a este nivel de peligrosidad:

- Amenazas Persistentes Avanzadas (APT)
- Ataques de Ransomware
- Desastre natural
- Controversias Públicas
- Accidentes Laborales
- Problemas de Salud Pública
- Crisis Administrativas o de Gestión Documental
- Crisis Financieras
- Otros incidentes de impacto crítico para la Institución calificados por el Oficial de Seguridad de la Información

Artículo 9.- Escenarios de Declaración de Crisis. - Los escenarios a considerar para atender el nivel de peligrosidad y taxonomía de un incidente pueden ser establecidos de la siguiente manera:

a) **L1 – Nivel Bajo:** No hay declaración de crisis
b) **L2 – Nivel Medio:** No hay declaración de crisis
c) **L3 – Nivel Alto:** Declaración de crisis opcional
d) **L4 – Nivel Muy Alto:** Si se debe declarar crisis
e) **L5 – Nivel Crítico:** Si se debe declarar crisis

Artículo 10.- Actuación en el caso de Crisis. - Es necesario considerar los equipos que actuarán en el caso de una crisis.

a) Equipo de Nivel Operativo (Nivel Tres)
L1 – Nivel Bajo
L2 – Nivel Medio

Equipos de nivel operativo muy especializado y concretos, que dependiendo del caso puede ser la Dirección de Tecnología y Comunicación, Dirección Administrativa, Organismos Desconcentrados, Oficial de Seguridad de la Información, Delegado de Protección de Datos Personales y la Unidad Administrativa pertinente.

b) Comité de Crisis (Nivel Dos)
L3 – Nivel Alto
L2 – Nivel Muy Alto

Oficial de Seguridad de la Información, Delegada/o de Protección de Datos Personales, Coordinadores Técnicos, Coordinadores Generales, Direcciones y de ser el caso Directores Zonales, que trabajen con varios equipos de Nivel Tres en aspectos operativos, muy especializados y concretos.

Por ejemplo, las Unidades Administrativas a cargo de los activos estratégicos de información y asociados de la Institución como se describe a continuación:

- Infraestructura Tecnológica – Centro de Datos (Dirección de Tecnologías de la Información y Comunicación)
- Hardware – Software – Enlaces de Telecomunicaciones – Networking – Aplicaciones. (Dirección de Tecnologías de la Información y Comunicación)
- SICOEIR (Dirección Técnica de Homologación – Coordinación Técnica de Control)
- SACER (Dirección Técnica de Control del Espectro Radioeléctrico - Coordinación Técnica de Control)

- SAMM (Dirección Técnica de Control de Servicios de Telecomunicaciones – Coordinación Técnica de Control)
- SIETEL (Dirección Técnica de Control de Servicios de Telecomunicaciones - Coordinación Técnica de Control)
- SPECTRA (Dirección Técnica de Títulos Habilitantes del Espectro Radioeléctrico - Coordinación Técnica de Títulos Habilitantes)
- SACOF (Unidad de Registro Público - Coordinación Técnica de Títulos Habilitantes)
- ONBASE (DEDA – Sistema Documental)
- SIFAF (Coordinación General Administrativa Financiera – Sistema de facturación)
- Otras aplicaciones de Software de la ARCOTEL a cargo de las Diferentes Unidades Administrativas de la ARCOTEL.

c) Comité de Crisis Estratégico (Nivel Uno)
L5 – Nivel Crítico

Director Ejecutivo **–** Asesor del Director Ejecutivo, Oficial de Seguridad de la Información, Delegado/a de Protección de Datos Personales, Coordinadores Técnicos, Coordinadores Generales – Director de Tecnologías de la Información y Comunicación - Unidad de Comunicación.

Por ejemplo, en un ciberataque de categoría crítica el Director Ejecutivo, Asesor, Coordinadores Técnicos, Coordinadores Generales, Presidente del Comité de Crisis, Oficial de Seguridad de la Información, Delegado/a de Protección de Datos Personales, serán quienes tomen las decisiones finales dentro del Comité Nivel Uno, según las aportaciones tanto del Comité de Nivel Dos como del Comité Nivel Tres.

Artículo 11.- Gestión de Crisis y Cibercrisis. –

a) Se debe entender por **CRISIS** a cualquier circunstancia, deliberada o fortuita, ocasionada internamente o no, que podría causar un desequilibrio en la Institución ya sea con sus servicios, autoridades, funcionarios, servidores, terceros asociados a la Institución, inclusive Prestadores de Servicios de Telecomunicaciones u otras entidades, afectando o dañando la imagen o reputación pública. Independientemente del origen de la crisis, la Institución debe gestionarla y se necesita dotación de capacidades, estructuras de gestión adecuadas, que permita abordar la crisis con garantías de éxito.

b) En una crisis se necesita actuar desde dos perspectivas:

1) **Operativa y de respuesta:** Motivo que la origina y cuyos efectos inmediatos deben ser contenidos y resueltos por un equipo de respuesta especializado de acuerdo con el incidente que originó la crisis, actividad que debe tener en cuenta métodos de recopilación y análisis de datos y eventos, metodologías de seguimiento y procedimientos.
2) **Organizativa y estratégica:** Ya sea que el impacto afecte a diferentes ámbitos de la Institución como servicio, operativa, imagen, reputación, grupos de interés, presencia en redes sociales, entre otros, se requiere de una respuesta coordinada a alto nivel, determinando los canales de comunicación con otras Unidades Administrativas o entidades propias o ajenas.

c) Una **CIBERCRISIS** es un acontecimiento del ámbito de la ciberseguridad con gran impacto sobre la actividad de la Institución y que demanda tomar decisiones rápidas con información limitada. La probabilidad de ese acontecimiento dependerá del grado de preparación previa de la Institución. La gestión de los ciberincidentes, exige determinar la peligrosidad con los que compara las evidencias que se disponen del ciberincidente, en sus estadios iniciales; el ciberincidente puede comprometer la confidencialidad,

integridad y disponibilidad de los activos de información de la Institución y sus activos asociados.

d) Se debe considerar 5 pilares fundamentales en la Gestión de una Crisis.

1) **LIDERAZGO**
2) **PREPARACIÓN**
   - Planes y Protocolos estructurales
   - Configuración del Comité de Crisis
   - Control permanente de la superficie de exposición
   - Gestión adecuada de grupos de interés
3) **RESPUESTA**
   - Coordinación
   - Iniciativa y Proactividad
4) **COMUNICACIÓN**
   - Discurso unificado y fuente oficial de información
   - Transparencia, empatía y asunción de responsabilidades
5) **CIERRE**
   - Puesta en valor de las acciones adoptadas
   - Implementación de lecciones aprendidas.

SECCIÓN III
DEL FUNCIONAMIENTO DEL COMITÉ DE CRISIS

Artículo 12. Convocatorias. - El Secretario del Comité de Crisis, una vez que el Oficial de Seguridad de la Información haya determinado la pertinencia de convocar a un Comité de Crisis acorde al nivel de peligrosidad de un incidente en la Institución, y previa autorización del Presidente, enviará la convocatoria a las sesiones ordinarias o extraordinarias mediante medios de comunicación oficiales de la Institución, señalando fecha, hora, lugar, y los puntos del orden del día, que no podrán exceder de cinco puntos en caso de reuniones ordinarias.

El Secretario del Comité de Crisis acompañará a las convocatorias, de manera formal y obligatoria, los informes, estudios y demás documentación que contenga integralmente la información de respaldo pertinente a cada punto del orden del día, y que permita a los miembros del Comité contar con suficientes elementos de juicio para adoptar las resoluciones que el caso requiera.

Artículo 13. Sesiones. - El Comité de Crisis se reunirá en sesiones ordinarias o extraordinarias en cualquier tiempo que amerite, ya sean estas de manera presencial o virtual, según corresponda el caso.

Los funcionarios o servidores de la institución que participen en las sesiones en calidad de invitados no tendrán derecho a voto, su participación requerirá de la autorización previa del presidente del Comité y se limitará al punto de tratamiento en el orden del día para el que fueren convocados.

Artículo 14. Quorum de instalación y decisión. - La instalación del Comité de Crisis se conformará con al menos la mitad de sus miembros que tienen voz y voto, uno de los cuales obligatoriamente, será el Presidente o su delegado/a; en ningún caso se instalará una sesión sin la presencia del Presidente del Comité o su delegado/a. El voto será obligatorio y su pronunciamiento afirmativo o negativo. Las resoluciones se adoptarán por mayoría

simple de votos afirmativos y, en caso de empate, el asunto se resolverá por el voto dirimente del Presidente del Comité o su delegado/a.

Artículo 15. Sesiones Ordinarias. - El Comité de Crisis sesionará de forma ordinaria y obligatoria cuando el Oficial de Seguridad de la Información declare un incidente con nivel de peligrosidad Alto (opcional), Muy Alto o Crítico.

Las sesiones ordinarias serán convocadas con al menos un (1) día hábil de anticipación, anexando el orden del día y la información pertinente.

Artículo 16. Sesiones Extraordinarias. - El Comité de Crisis podrá sesionar extraordinariamente por disposición del presidente del Comité y cuando el Oficial de Seguridad de la Información declare un incidente con nivel de peligrosidad Alto (opcional), Muy Alto o Crítico; o por pedido debidamente motivado, de uno de sus miembros y autorizado por el Presidente del Comité de Crisis, cuando las circunstancias lo ameriten.

En estas sesiones se tratarán asuntos puntuales considerados urgentes o impostergables.

Las sesiones extraordinarias serán convocadas a través de algún medio de comunicación de la Institución, con al menos 2 horas de anticipación, anexando el orden del día y la información pertinente.

Artículo 17. Desarrollo de la sesión. - Las sesiones del Comité de Crisis se desarrollarán de la siguiente manera:

a) Constatación del quorum por parte del Secretario del Comité de Crisis;
b) Instalación de la sesión por parte del Presidente del Comité de Crisis;
c) Aprobación del orden del día. Cualquiera de los miembros del Comité podrá proponer la modificación de los puntos que van a ser tratados, su reordenamiento, o la declaración del carácter confidencial o reservado de uno de sus puntos;
d) Conocimiento y tratamiento de los puntos del orden del día aprobado, con la participación y propuestas de los miembros del Comité;
e) Una vez tratado un punto del orden del día, y de considerarlo suficientemente estudiado o examinado, el Presidente del Comité de Crisis lo someterá a consideración de los miembros del Comité para su resolución; y,
f) El Secretario del Comité tomará la votación de la resolución o acuerdo planteado, por cada uno de los puntos tratados.

Los miembros del Comité, y los demás asistentes a la sesión, deberán solicitar al presidente del Comité su autorización para hacer uso de la palabra.

Artículo 18. Registro de las sesiones. - Toda sesión será grabada en medios digitales de audio o video y de éstos se levantará el acta correspondiente.

Las grabaciones, transcripciones, resúmenes y actas de las sesiones permanecerán bajo custodia y responsabilidad del Secretario del Comité.

Artículo 19. Votación. - Para iniciar la votación se requerirá la participación de todos los miembros del Comité de Crisis asistentes a la sesión convocada; una vez dispuesta la votación, ningún miembro podrá abandonar la sesión.

Los miembros del Comité de Crisis podrán votar a favor o en contra; en cualquier caso, su voto deberá realizarlo de manera motivada.

Para el caso de sesión virtual, la votación se realizará durante la misma reunión; en caso de no poder expresar el voto por inconvenientes técnicos verificables, se podrá considerar utilizar cualquier medio tecnológico de telecomunicaciones que permita verificar el voto a favor o en contra de la moción. En caso de pérdida de comunicación virtual que afecte al quorum de la sesión, el Presidente del Comité de Crisis podrá suspender la votación hasta restaurar la comunicación con el o los participantes y continuar con la votación.

Artículo 20. Actas de las sesiones. - El desarrollo y resoluciones o acuerdos de cada sesión se registrarán en el **"**Acta de sesión", documento codificado que al menos contendrá:

1. Número, lugar, fecha y hora de inicio y cierre de la sesión;
2. Tipo de sesión;
3. Nombres completos de los asistentes y cargos;
4. Los puntos tratados y un breve resumen de las intervenciones, recomendaciones u observaciones realizadas en cada punto;
5. La votación adoptada por los miembros; y,
6. Las resoluciones o acuerdo tomados por los miembros del Comité.

La propuesta de "Acta de sesión", será realizada y enviada por el Secretario del Comité a los miembros para su revisión, hasta un (1) día hábil posterior a la sesión.

Para la revisión del acta, los miembros del Comité tendrán hasta un (1) día hábil posteriores a su recepción para presentar sus observaciones, en caso de que, en el plazo determinado, no se recibieran observaciones, correcciones o cambios, se deberá aprobar el acta y continuar con su suscripción.

Las actas suscritas y legalizadas, al igual que las grabaciones de audio, serán archivadas de forma física o digital, según corresponda; mismas que estarán bajo custodia y responsabilidad del Secretario del Comité.

Artículo 21. Resoluciones o Acuerdos. - Las Resoluciones o acuerdos del Comité de Crisis sobre los asuntos tratados en el orden del día de la sesión convocada serán adoptadas por mayoría simple.

DISPOSICIÓN GENERAL

PRIMERA. - En todo lo no previsto en la presente Resolución, el Comité se sujetará a lo establecido en el Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003 de 08 de febrero de 2024, publicado en el Registro Oficial - Tercer Suplemento No. 509 de 1 de marzo de 2024, con el cual se expidió el Esquema Gubernamental de Seguridad de la Información – EGSI v3; y, las demás disposiciones conexas emitidas por la autoridad competente.

DISPOSICIONES TRANSITORIAS

PRIMERA. – El Oficial de Seguridad de la Información junto con el Director de Tecnologías de la Información y Comunicación de la ARCOTEL, en el término de 15 días una vez aprobada esta resolución por la Máxima Autoridad de la ARCOTEL presentarán un "Plan de Gestión de Crisis", documento que establece los procedimientos y estrategias para manejar situaciones de crisis en la Institución.

El “Plan de Gestión de Crisis” debe contener como mínimo lo siguiente: 1) Introducción, 2) Identificación y análisis de riesgos, 3) Estructura del Comité de Crisis, 4) Procedimientos de respuesta, 5) Comunicación, 6) Gestión de la Crisis, 7) Recuperación y posterior a la Crisis, 8) Capacitación y simulacros, 9) Revisión y actualización.

SEGUNDA. – Todas las Unidades Administrativas, Organismos Desconcentrados y Oficina Técnica Galápagos de la ARCOTEL, en el término de 15 días una vez aprobada esta resolución por la Máxima Autoridad de la ARCOTEL, presentarán un “Plan de Continuidad de Negocio” que permita garantizar que su área dentro de la Institución pueda mantener sus operaciones críticas en funcionamiento, o recuperarlas lo más rápido posible, después de sufrir una interrupción significativa.

El “Plan de Continuidad del Negocio” debe contener como mínimo lo siguiente: 1) Inventario de recursos críticos, 2) Análisis de riesgos, 2) Procedimientos de respuesta, 3) Plan de recuperación, 4) Pruebas y ejercicios, 5) Comunicación.

El Oficial de Seguridad de la Información, elaborará, asesorará y coordinará con las Unidades Administrativas, Organismos Desconcentrados y Oficina Técnica Galápagos de la ARCOTEL, la ejecución del Estudio de Gestión de Riesgos de Seguridad de la Información, necesario para la elaboración del “Plan de Continuidad del Negocio”.

TERCERA. – La Unidad de Comunicación de la ARCOTEL, en el término de 15 días una vez aprobada esta resolución por la Máxima Autoridad de la ARCOTEL presentarán un “Manual de Comunicación de Crisis” que permita guiar y coordinar las acciones de comunicación durante una situación crítica, asegurando que la Institución transmita un mensaje claro, coherente y oportuno a todos sus públicos de interés.

El Manual de Comunicación de Crisis debe contener como mínimo lo siguiente: 1) Identificación de crisis, 2) Equipo de crisis, 3) Voceros, 4) Mensajes clave, 5) Canales de comunicación, 6) cronograma de comunicación, 7) monitoreo de medios, 8) evaluación y mejora.

CUARTA. – La Dirección de Tecnologías de la Información y Comunicación de la ARCOTEL, en el plazo de 1 mes, una vez aprobada esta resolución por la Máxima Autoridad de la ARCOTEL presentarán un “Plan de Contingencia de Tecnologías de la Información y Comunicación”, que permita minimizar el impacto de cualquier interrupción o falla en los sistemas de información de la Institución, asegurando la continuidad de los servicios y la protección de los datos.

El “Plan de Contingencia de Tecnologías de la Información y Comunicación, debe contener como mínimo lo siguiente: 1) Análisis de riesgos, 2) Procedimientos de respuesta, 3) Plan de recuperación, 4) Pruebas y ejercicios, 5) Comunicación.

DISPOSICIONES FINALES

PRIMERA: Encárguese de la ejecución de la presente Resolución a los miembros del Comité de Crisis, a las diferentes Unidades Administrativas, Organismos Desconcentrados y Oficina Técnica Galápagos de la ARCOTEL según el caso.

SEGUNDA: Disponer a la Unidad de la Gestión Documental y Archivo, notifique con el contenido de la presente resolución, a las Coordinaciones Técnicas, Generales, Organismos Desconcentrados, Oficinas Técnicas y demás Unidades Administrativas de la Agencia de Regulación y Control de las Telecomunicaciones; y, a la Unidad de Comunicación Social para su difusión a través de los canales oficiales de la Institución.

La presente resolución entrará en vigencia a partir de su suscripción sin perjuicio de su publicación en el Registro Oficial.

Dada, en la ciudad de Quito, D. M. el, 21 de noviembre de 2024

Firmado electrónicamente por:
JORGE ROBERTO HOYOS ZAVALA

Mgs. Jorge Roberto Hoyos Zavala.
DIRECTOR EJECUTIVO
AGENCIA DE REGULACIÓN Y CONTROL DE LAS TELECOMUNICACIONES

Elaborado por:	MSc. Marcelo Ricardo Filián Narváez **Oficial de Seguridad de la Información** **ARCOTEL**	Firmado electrónicamente por: MARCELO RICARDO FILIAN NARVAEZ
Revisado por:	Mgs. Pablo Ramiro Almeida López **Director de Procesos, Calidad, Servicios y Cambio y Cultura Organizacional** **ARCOTEL**	Firmado electrónicamente por: PABLO RAMIRO ALMEIDA LOPEZ
Aprobado por:	Mgs. Luis Ramiro Moncayo Córdova **Coordinador General de Planificación y Gestión Estratégica** **Presidente del Comité de Seguridad de la Información** **ARCOTEL**	Firmado electrónicamente por: LUIS RAMIRO MONCAYO CORDOVA