RESOLUCIÓN ARCOTEL-2018- 0652

LA AGENCIA DE REGULACIÓN Y CONTROL DE LAS TELECOMUNICACIONES

CONSIDERANDO:

Que, la Constitución de la República del Ecuador, en su artículo 66 reconoce y garantiza, como parte de los derechos de libertad: "*19.- El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley. 20. El derecho a la intimidad personal y familiar. 21. El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación.*".

Que, la Constitución de la República del Ecuador, dispone en su artículo 226 que "*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.*".

Que, las telecomunicaciones y el espectro radioeléctrico, por mandato del artículo 313 de la Constitución de la República, pertenecen a los sectores estratégicos del Estado, el que se ha reservado el derecho de administrar, regular, controlar y gestionar dichos sectores, lo cual guarda concordancia con lo establecido en el artículo 7 de la Ley Orgánica de Telecomunicaciones – LOT.

Que, la Constitución de la República, preceptúa en su artículo 314, inciso segundo, que el Estado garantizará que los servicios públicos y su provisión respondan a los principios de obligatoriedad, generalidad, uniformidad, eficiencia, responsabilidad, universalidad, accesibilidad, regularidad, continuidad y calidad.

Que, la Ley Orgánica de Telecomunicaciones - LOT, publicada en el Registro Oficial No. 439 de 18 de febrero de 2015, en su artículo 7 establece las competencias del Gobierno Central, de la siguiente manera: "*El Estado, a través del Gobierno Central tiene competencias exclusivas sobre el espectro radioeléctrico y el régimen general de telecomunicaciones. Dispone del derecho de administrar, regular y controlar los sectores estratégicos de telecomunicaciones y espectro radioeléctrico, lo cual incluye la potestad para emitir políticas públicas, planes y normas técnicas nacionales, de cumplimiento en todos los niveles de gobierno del Estado. (...)*".

Que, la LOT señala, en el artículo 22, dentro de los derechos que tienen los abonados, clientes y usuarios: "*1. A disponer y recibir los servicios de telecomunicaciones contratados de forma continua, regular, eficiente, con calidad y eficacia. (...) 3. Al secreto e inviolabilidad del contenido de sus comunicaciones, con las excepciones previstas en la Ley. (...)*".

Que, la Ley ibídem, en su artículo 23 señala cuales son las obligaciones de los abonados, clientes y usuarios y al respecto establece, entro otros: "*1. Cumplir con los términos del contrato de prestación de servicios celebrado con el prestador, independientemente de su modalidad. 2. Adoptar las medidas sugeridas por el prestador de servicios a fin de salvaguardar la integridad de la red y las comunicaciones, sin perjuicio de las responsabilidades de los prestadores. (...)*".

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • Código Postal: 170518 / Quito - Ecuador • Teléfono: 593-2 294 780
www.arcotel.gob.ec

Que, en el artículo 24 del mismo cuerpo legal, relacionado con las obligaciones de los prestadores de servicios de telecomunicaciones, incluye entre otras las siguientes: *"(...) 13. Garantizar el secreto e inviolabilidad de las comunicaciones cursadas a través de sus redes y servicios de telecomunicaciones, sin perjuicio de las excepciones establecidas en las leyes. 14. Adoptar las medidas necesarias para la protección de los datos personales de sus usuarios y abonados, de conformidad con esta Ley, su Reglamento General y las normas técnicas y regulaciones respectivas. 15. Adoptar las medidas para garantizar la seguridad de las redes.(...) 17. No limitar, bloquear, interferir, discriminar, entorpecer, priorizar ni restringir el derecho de sus usuarios o abonados a utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación, desarrollo o servicio legal a través de Internet o en general de sus redes u otras tecnologías de la información y las comunicaciones, ni podrán limitar el derecho de un usuario o abonado a incorporar o utilizar cualquier clase de instrumentos, dispositivos o aparatos en la red, siempre que sean legales, salvo las excepciones establecidas en la normativa vigente. Se exceptúan aquellos casos en los que el cliente, abonado o usuario solicite de manera previa su decisión expresa de limitación o bloqueo de contenidos, o por disposición de autoridad competente. Los prestadores pueden implementar las acciones técnicas que consideren necesarias para la adecuada administración de la red en el exclusivo ámbito de las actividades que le fueron habilitadas para efectos de garantizar el servicio. (...)".*

Que, en el artículo 25 de la LOT, relacionado con los derechos de los prestadores de servicios de telecomunicaciones, señala: *"...2. Suspender el servicio provisto por falta de pago de los abonados o clientes o uso ilegal del servicio calificado por autoridad competente, previa notificación al abonado o cliente...".*

Que, el Título VIII de la LOT, versa sobre el secreto de las comunicaciones y la protección de datos personales, y establece disposiciones para tal fin, contempladas en los artículos del 76 al 85.

Que, como parte del secreto de las comunicaciones está lo contemplado en el artículo 76 ibídem, el cual, respecto de las medidas técnicas de seguridad e invulnerabilidad, dispone: "*Las y los prestadores de servicios ya sea que usen red propia o la de un tercero, deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de sus servicios y la invulnerabilidad de la red y garantizar el secreto de las comunicaciones y de la información transmitida por sus redes. Dichas medidas garantizarán un nivel de seguridad adecuado al riesgo existente. En caso de que exista un riesgo particular de violación de la seguridad de la red, el prestador de servicios de telecomunicaciones deberá informar a sus abonados, clientes o usuarios sobre dicho riesgo y, si las medidas para atenuar o eliminar ese riesgo no están bajo su control, sobre las posibles soluciones".*

Que, en el Capítulo II del Título VIII de la LOT, se establece la Protección de los Datos Personales, constando, entre otros, los siguientes artículos:

"Art. 78.- Derecho a la intimidad. Para la plena vigencia del derecho a la intimidad, establecido en el Artículo 66, numeral 20 de la Constitución de la República, las y los prestadores de servicios de telecomunicaciones deberán garantizar, en el ejercicio de su actividad, la protección de los datos de carácter personal. Para tal efecto, las y los prestadores de servicios de telecomunicaciones deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de su red con el fin de garantizar la protección de los datos de carácter personal de conformidad con la ley. Dichas medidas incluirán, como mínimo: 1. La garantía de que sólo el personal autorizado tenga acceso a los datos personales para fines autorizados por la ley. 2. La protección de los datos personales almacenados o transmitidos de la destrucción accidental o ilícita, la pérdida o alteración accidentales o el almacenamiento, tratamiento, acceso o revelación no autorizados o ilícitos. 3. La garantía de la aplicación efectiva de una política de seguridad con respecto al tratamiento de datos personales. 4. La garantía de

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • Código Postal: 170518 / Quito - Ecuador • Teléfono: 593-2 294-780
www.arcotel.gob.ec

que la información suministrada por los clientes, abonados o usuarios no será utilizada para fines comerciales ni de publicidad, ni para cualquier otro fin, salvo que se cuente con el consentimiento previo y autorización expresa de cada cliente, abonado o usuario. El consentimiento deberá constar registrado de forma clara, de tal manera que se prohíbe la utilización de cualquier estrategia que induzca al error para la emisión de dicho consentimiento.

Art. 79.- Deber de información. En caso de que exista un riesgo particular de violación de la seguridad de la red pública o del servicio de telecomunicaciones, el prestador de servicios de telecomunicaciones informará a sus abonados, clientes y usuarios sobre dicho riesgo y sobre las medidas a adoptar. En caso de violación de los datos de un abonado o usuario particular, el prestador notificará de tal violación al abonado o usuario particular en forma inmediata, describiendo al menos la naturaleza de la violación de los datos personales, los puntos de contacto donde puede obtenerse más información, las medidas recomendadas para atenuar los posibles efectos adversos de dicha violación y las medidas ya adoptadas frente a la violación de los datos personales. La notificación de una violación de los datos personales a un abonado, cliente o usuario particular afectado no será necesaria si el prestador demuestra a la Agencia de Regulación y Control de las Telecomunicaciones que ha aplicado las medidas de protección tecnológica convenientes y que estas medidas se han aplicado a los datos afectados por la violación de seguridad. Unas medidas de protección de estas características convierten los datos en incomprensibles para toda persona que no esté autorizada a acceder a ellos. A los efectos establecidos en este artículo, se entenderá como violación de los datos personales la violación de la seguridad que provoque la destrucción, accidental o ilícita, la pérdida, la alteración, la revelación o el acceso no autorizados, de datos personales transmitidos, almacenados o tratados en la prestación de un servicio de telecomunicaciones.

Art. 80.- Procedimientos de revelación. Las y los prestadores de servicios implementarán procedimientos internos para atender las solicitudes de acceso a los datos personales de sus abonados, clientes o usuarios por parte de las autoridades legalmente autorizadas. Los procedimientos internos que se implementen, para fines de supervisión y control, estarán a disposición de la Agencia de Regulación y Control de las Telecomunicaciones."

"Art. 83.- Control técnico. Cuando para la realización de las tareas de control técnico, ya sea para verificar el adecuado uso del espectro radioeléctrico, la correcta prestación de los servicios de telecomunicaciones, el apropiado uso y operación de redes de telecomunicaciones o para comprobar las medidas implementadas para garantizar el secreto de las comunicaciones y seguridad de datos personales, sea necesaria la utilización de equipos, infraestructuras e instalaciones que puedan vulnerar la seguridad e integridad de las redes, la Agencia de Regulación y Control de las Telecomunicaciones deberá diseñar y establecer procedimientos que reduzcan al mínimo el riesgo de afectar los contenidos de las comunicaciones. Cuando, como consecuencia de los controles técnicos efectuados, quede constancia de los contenidos, los soportes en los que éstos aparezcan no podrán ser ni almacenados ni divulgados y serán inmediatamente destruidos y desechados.".

Art. 84.- Entrega de información. Las y los prestadores de servicios, entregarán a las autoridades competentes la información que les sea requerida dentro del debido proceso, con el fin de investigación de delitos. La Agencia de Regulación y Control de las Telecomunicaciones establecerá los mecanismos y procedimientos que sean necesarios.

Art. 85.- Obligaciones adicionales. La Agencia de Regulación y Control de las Telecomunicación establecerá y reglamentará los mecanismos para supervisar el cumplimiento de las obligaciones tanto de secreto de las comunicaciones como de seguridad de datos personales y, en su caso, dictará las instrucciones

correspondientes, que serán vinculantes para las y los prestadores de servicios, con el fin de que adopten determinadas medidas relativas a la integridad y seguridad de las redes y servicios. Entre ellas, podrá imponer: 1. La obligación de facilitar la información necesaria para evaluar la seguridad y la integridad de sus servicios y redes, incluidos los documentos sobre las políticas de seguridad. 2. La obligación de someterse a costo del prestador, a una auditoría de seguridad realizada por un organismo público, autoridad competente o, de ser el caso, por una empresa privada o persona natural independiente.".

Que, la LOT, en su artículo 142, crea la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), como 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; y, en el artículo 144, señala dentro de las competencias de la ARCOTEL "*1. Emitir las regulaciones, normas técnicas, planes técnicos y demás actos que sean necesarios en el ejercicio de sus competencias, para que la provisión de los servicios de telecomunicaciones cumplan con lo dispuesto en la Constitución de la República y los objetivos y principios dispuestos en esta Ley y de conformidad con las políticas que dicte el Ministerio rector de las Telecomunicaciones y de la Sociedad de la Información.*".

Que, la LOT, en su artículo 148 determina en el numeral 4, como parte de las atribuciones del Director Ejecutivo de la ARCOTEL: *"(...) 4. Aprobar la normativa para la prestación de cada uno de los servicios de telecomunicaciones, en los que se incluirán los aspectos técnicos, económicos, de acceso y legales, así como los requisitos, contenido, términos, condiciones y plazos de los títulos habilitantes y cualquier otro aspecto necesario para el cumplimiento de los objetivos de esta Ley.".*

Que, en la Disposición General Primera de la LOT, se señala que para la emisión o modificación de planes o actos de contenido normativo, la ARCOTEL deberá realizar consultas públicas para recibir opiniones, recomendaciones y comentarios de las y los afectados o interesados, en forma física o por medios electrónicos; las opiniones, sugerencias o recomendaciones que se formulen en el procedimiento de consulta pública no tendrán carácter vinculante. Dicha disposición establece además que, en todos los casos para la expedición de actos normativos, se contará con estudios o informes que justifiquen su legitimidad y oportunidad; y que la ARCOTEL normará el procedimiento de consulta pública.

Que, en el Registro Oficial Suplemento 676 del 25 de enero de 2016, se publicó el Reglamento General a la Ley Orgánica de las Telecomunicaciones, mismo que en su artículo 9 numeral 3 del Capítulo IV, del título II, establece dentro de las funciones del Director Ejecutivo, entre otras:

"3. Expedir la normativa técnica para la prestación de los servicios y para el establecimiento, instalación y explotación de redes, que comprende el régimen general de telecomunicaciones y el espectro radioeléctrico."

Que, en el artículo 58 del Reglamento General a la LOT, se establece las consideraciones generales de los derechos de los prestadores de servicios, de la siguiente manera: *"Para el ejercicio de los derechos de los prestadores de servicios establecidos en la LOT, se considerará lo siguiente: 1. Para la suspensión del servicio por uso ilegal calificado por autoridad competente, por regla general, se notificará al usuario; salvo que, la ARCOTEL establezca otros mecanismos que permitan la eficaz intervención de las autoridades. (...) 4. Para la suspensión del servicio provisto por falta de pago de los abonados o clientes, se le deberá notificar conforme la normativa que emita para el efecto la ARCOTEL".*

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-7800
www.arcotel.gob.ec

Que, el Reglamento General a la Ley Orgánica de las Telecomunicaciones, en su artículo 117, sobre el secreto de la comunicación, establece que: *"El Estado garantiza la inviolabilidad y secreto de la información y las comunicaciones transmitidas a través de redes de telecomunicaciones; por lo que, ninguna persona o entidad pública o privada tendrá acceso a la misma ni a su utilización, salvo que haya orden emitida por juez competente."*.

Que, el artículo 118 ibídem se refiere a la confidencialidad y al respecto menciona: *"Los prestadores de servicios de telecomunicaciones mantendrán el secreto de la información cursada y no podrán interceptarla, interferirla, divulgarla, publicarla o utilizar su contenido. Por tanto, deberán tomar las medidas técnicas u operativas necesarias para proteger el secreto y confidencialidad de la información transmitida a través de las redes de telecomunicaciones y la seguridad al acceso de la red. (...)"*.

Que, El artículo 121 del mismo cuerpo legal determina que: *"(...) La ARCOTEL establecerá los mecanismos y emitirá las regulaciones correspondientes a fin de precautelar el secreto de las comunicaciones y de la información que se trasmite a través de redes de telecomunicaciones, así como la seguridad de los datos personales y de las redes"*.

Que, el Reglamento para los Abonados/Clientes y Usuarios de los Servicios de Telecomunicaciones y de Valor Agregado, emitido mediante Resolución TEL-477-16-CONATEL-2012, de 11 de julio de 2012, en su artículo 27, numeral 27.3, establece como parte de los derechos de los prestadores, "*suspender el servicio por las causales contempladas en el ordenamiento jurídico vigente y las constantes en los contratos de prestación de servicios celebrados con sus abonados/clientes*".

Que, mediante Resolución Nro. 003-03-ARCOTEL-2015, de 28 de mayo de 2015, el Directorio de la ARCOTEL emitió el Reglamento de Consultas Públicas.

Que, mediante memorando Nro. ARCOTEL-CCDR-2017-0019-M de 03 de julio de 2017, la Dirección Técnica de Control de Seguridad de Redes de Telecomunicaciones, pone en conocimiento de la Dirección Nacional de Procesos, Calidad, Servicios y Cambio y Cultura Organizacional, que se encuentra en proceso la elaboración y aprobación de la "NORMA TÉCNICA PARA COORDINAR LA GESTIÓN DE INCIDENTES Y VULNERABILIDADES QUE AFECTEN A LA SEGURIDAD DE LAS REDES Y SERVICIOS DE TELECOMUNICACIONES", por lo que se requiere la codificación de seis formatos. La Dirección Nacional de Procesos, Calidad, Servicios y Cambio y Cultura Organizacional, con memorando Nro. ARCOTEL-CPDP-2017-0039-M de 04 de julio de 2017, emite la codificación respectiva.

Que, con memorando Nro. ARCOTEL-CREG-2017-0443-M de 13 de noviembre de 2017 la Coordinación Técnica de Regulación de la ARCOTEL pone a consideración del Director Ejecutivo de la ARCOTEL, el Proyecto de Resolución e Informe Técnico-Regulatorio Nro. CRDS-IT-2017-0049 de 6 de noviembre de 2017, para la realización de consultas públicas del proyecto de "NORMA TÉCNICA PARA COORDINAR LA GESTIÓN DE INCIDENTES Y VULNERABILIDADES QUE AFECTEN A LA SEGURIDAD DE LAS REDES Y SERVICIOS DE TELECOMUNICACIONES", donde consta el análisis de competencia, así como la justificación de legitimidad y oportunidad.

Que, mediante sumilla inserta en el memorando Nro. ARCOTEL-CREG-2017-0443-M, la Dirección Ejecutiva de la ARCOTEL autoriza la ejecución del proceso de consultas públicas con sujeción a lo señalado en la Disposición General Primera de la Ley Orgánica de Telecomunicaciones y de lo dispuesto en el artículo 5 del Reglamento de Consultas Públicas.

Que, el 21 de noviembre de 2017 se publicó en el sitio web de la ARCOTEL, la convocatoria a consulta pública y audiencia presencial, respecto del Proyecto de "NORMA TÉCNICA PARA COORDINAR LA GESTIÓN DE INCIDENTES Y VULNERABILIDADES QUE

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • Código Postal: 170518 / Quito Ecuador • Teléfono: 593 2 294 760
www.arcotel.gob.ec

AFECTEN A LA SEGURIDAD DE LAS REDES Y SERVICIOS DE TELECOMUNICACIONES", y el día 12 de diciembre de 2017, a partir de las 09H00 se efectuó la audiencia pública convocada, la cual se realizó en las oficinas de la ARCOTEL de Quito, Guayaquil y Cuenca, en las dos últimas ciudades mediante videoconferencia. Las audiencias públicas tienen por objeto, conforme lo señala la Ley Orgánica de Telecomunicaciones, recibir opiniones, recomendaciones y comentarios, sin el carácter de vinculantes para la ARCOTEL, respecto del proyecto de normativa en consideración.

Que, con memorando Nro. ARCOTEL-CREG-2017-0496-M de 22 de Diciembre de 2017, la Coordinación Técnica de Regulación puso a consideración de la Dirección Ejecutiva de la ARCOTEL, el proyecto de resolución e informe de cumplimiento de audiencias públicas Nro. CRDS-IT-2017-055 de 22 de diciembre de 2017.

Que, con memorando Nro. ARCOTEL-CREG-2018-0010-M de 3 de enero de 2018 la Coordinación Técnica de Regulación solicita a la Coordinación General Jurídica la emisión del criterio de legalidad sobre la propuesta regulatoria denominada "NORMA TÉCNICA PARA COORDINAR LA GESTIÓN DE INCIDENTES Y VULNERABILIDADES QUE AFECTEN A LA SEGURIDAD DE LAS REDES Y SERVICIOS DE TELECOMUNICACIONES".

Que, mediante memorando Nro. ARCOTEL-CJUR-2018-0042-M de 16 de enero de 2018, la Coordinación General Jurídica da contestación al memorando Nro. ARCOTEL-CREG-2018-0010-M, e indica que remite el criterio jurídico No. ARCOTEL-CJDA-2018-0006 del 16 de enero de 2018 aprobado por la Coordinación Jurídica. En el mencionado criterio jurídico se concluye lo siguiente: "*En orden de los antecedentes, competencia y análisis realizado, esta Dirección de Asesoría Jurídica, concluye que el proyecto de acto normativo denominado "NORMA TÉCNICA PARA COORDINAR LA GESTIÓN DE INCIDENTES Y VULNERABILIDADES QUE AFECTEN A LA SEGURIDAD DE LAS REDES Y SERVICIOS DE TELECOMUNICACIONES", ha cumplido el procedimiento establecido en el Reglamento de Consultas Públicas, conforme la Disposición General Primera de la Ley Orgánica de Telecomunicaciones; siendo el Director Ejecutivo de la ARCOTEL, la autoridad administrativa competente para la emisión de la propuesta normativa materia del análisis, en cumplimiento de lo establecido en el artículo 148 de la norma legal ibídem.*".

Que, con memorando Nro. ARCOTEL-CREG-2018-0353-M de 26 de julio de 2018, la Coordinación Técnica de Regulación puso a consideración de la Dirección Ejecutiva de la ARCOTEL, el proyecto de resolución e informe de cumplimiento de audiencias públicas Nro. IT-CRDS-GR-2018-0025 de 25 de julio de 2018.

En ejercicio de sus atribuciones,

RESUELVE:

EXPEDIR LA "NORMA TÉCNICA PARA COORDINAR LA GESTIÓN DE INCIDENTES Y VULNERABILIDADES QUE AFECTEN A LA SEGURIDAD DE LAS REDES Y SERVICIOS DE TELECOMUNICACIONES"

TÍTULO I

ASPECTOS GENERALES

Artículo 1.- Objeto.- Esta Norma Técnica tiene como objeto establecer criterios y mecanismos de coordinación para que los prestadores de servicios de telecomunicaciones, ejecuten las medidas correspondientes para la gestión de vulnerabilidades e incidentes informáticos, para preservar la seguridad de sus servicios y reducir los riesgos de vulnerabilidad de la red, con un

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • Código Postal: 170518 / Quito - Ecuador • Teléfono: 593-2 294-780
www.arcotel.gob.ec

nivel de seguridad acorde al riesgo existente, con el fin de salvaguardar el secreto de las comunicaciones y de la información transmitida por sus redes.

Artículo 2.- Ámbito.- La aplicación de esta Norma abarca a todas las personas naturales o jurídicas de derecho público o privado que sean prestadores de servicios de telecomunicaciones ya sea que utilicen red propia o de terceros.

Son aplicables en lo que corresponda, las disposiciones de esta Norma, a las personas naturales o jurídicas, sean estos abonados o clientes de los servicios de telecomunicaciones, que al hacer uso de los servicios y las redes públicas de telecomunicaciones, pueden verse afectados por eventos de incidentes o vulnerabilidades, o a través de sus redes y equipos se generen incidentes o vulnerabilidades hacia las redes públicas de telecomunicaciones.

Artículo 3.- Definiciones.- Los términos empleados en esta Norma Técnica y no definidos, tendrán el significado establecido en la Ley Orgánica de Telecomunicaciones, en el Reglamento General a la Ley Orgánica de Telecomunicaciones, los adoptados por la Unión Internacional de Telecomunicaciones (UIT), por los convenios y tratados internacionales ratificados por la República del Ecuador; y, en las regulaciones respectivas emitidas por la ARCOTEL.

Para efectos de la presente Norma, se aplicarán las siguientes definiciones:

1. **Acuerdo de Confidencialidad y No divulgación.-** Convenio suscrito entre dos o más partes mediante el cual las mismas se comprometen a no divulgar la información intercambiada en la gestión de incidentes y vulnerabilidades.

2. **Anonimizar la Información.-** Omitir o eliminar datos que permitan la identificación del propietario de la información o su relación con una vulnerabilidad o incidente de seguridad.

3. **ARCOTEL.-** Agencia de Regulación y Control de las Telecomunicaciones.

4. **Centro de Respuesta a Incidentes Informáticos (CRII) de la ARCOTEL**.- Grupo de trabajo o unidad de la ARCOTEL que, conforme el Estatuto Orgánico de Gestión Organizacional por Procesos Institucional, tiene a su cargo el cumplimiento de las obligaciones, actividades y responsabilidades derivadas de la aplicación de la presente Norma en lo relacionado a la ARCOTEL. En general las referencias que se realicen a la ARCOTEL en la presente Norma, se entenderá que corresponden a las actividades y gestión que realizará el CRII, salvo donde se exprese lo contrario.

5. **Comunidad Objetivo.-** La Comunidad Objetivo es aquel grupo de personas naturales o jurídicas de derecho público o privado, sistemas u organismos partícipes de la coordinación y gestión de vulnerabilidades que afecten la seguridad de las redes y servicios de telecomunicaciones. Para fines de aplicación de la presente Norma Técnica, la Comunidad Objetivo de la ARCOTEL estará constituida por prestadores de servicios de telecomunicaciones y los abonados o clientes de dichos servicios.

6. **Encargados de Seguridad.-** Son servidores públicos de la ARCOTEL y personas designadas por las empresas prestadoras de servicios de telecomunicaciones, como responsables de coordinar la gestión de incidentes y vulnerabilidades, así como de planificar, desarrollar, controlar y gestionar la aplicación de políticas, procedimientos y acciones, con la finalidad de mejorar la seguridad de los servicios y redes de telecomunicaciones, la seguridad de la información transmitida y la invulnerabilidad de la red, conforme lo establecido en la presente Norma.

7. **Evento.-** Un evento de seguridad de la información es la ocurrencia identificada de un estado de un sistema, servicio o red, que muestra una posible brecha de política de

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • Código Postal: 170518 / Quito Ecuador • Teléfono: 593-2 294 780
www.arcotel.gob.ec

seguridad de la información, falla de protecciones, o una situación previa desconocida que puede ser relevante para la seguridad.

8. **Fuentes de Información.-** Son personas naturales o jurídicas, públicas o privadas, sean estas nacionales o extranjeras u organismos internacionales que almacenan y administran información respecto a vulnerabilidades o incidentes de seguridad de la información y que reportan periódicamente a la ARCOTEL los eventos relacionados con los Números de Sistemas Autónomos (ASN) del país.

9. **Gestión de Incidentes.-** Son procesos para la detección, notificación, evaluación, respuesta, tratamiento y aprendizaje de incidentes, en aplicación de la presente Norma Técnica.

10. **Gestión de Vulnerabilidades.-** Proceso proactivo de seguridad que consiste en identificar vulnerabilidades y reducirlas antes de que sean causa de un incidente de seguridad.

11. **Hash.-** Es una función criptográfica, que por medio de la aplicación de un algoritmo matemático transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud.

12. **Incidente.-** Es la ocurrencia de uno o varios eventos, que comprometen las operaciones y amenazan la seguridad de la información de la comunidad objetivo. Se define además, como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la Política de Seguridad de la Información, del prestador de servicios de telecomunicaciones.

13. **Network Address Traslation - NAT (Traducción de Direcciones de Red).-** La traducción de direcciones de red es un método mediante el cual se cambian direcciones IP de un dominio a otro, en un intento de proporcionar un enrutamiento transparente a los hosts. Tradicionalmente, los dispositivos NAT se utilizan para cambiar un dominio aislado de direcciones IP privadas no registradas, a un dominio externo con direcciones registradas únicas a nivel mundial.

14. **Notificaciones.-** Son las comunicaciones de vulnerabilidades o incidentes de seguridad de las redes o servicios de telecomunicaciones, que remite la ARCOTEL a los prestadores de servicios de telecomunicaciones, que requieren acciones técnicas para su gestión (solución o mitigación). Las notificaciones se originan en la ARCOTEL o en los prestadores de servicios de telecomunicaciones, conforme el ámbito de la presente Norma.

15. **Números de Sistemas Autónomos (ASN – Autonomous System Numbers).-** Son números únicos a nivel mundial que se asignan a los sistemas autónomos, y que es una parte importante de la arquitectura de enrutamiento de Internet. Los números de sistema autónomo se toman de un campo de números de 16 bits, que en la actualidad se ha extendido a 32 bits.

16. **PGP / GPG (Pretty Good Privacy / GNU Privacy Guard - GnuPG).-** Privacidad Bastante Buena, son aplicaciones cuya finalidad es proteger la información distribuida a través del internet mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos gracias a firmas digitales para tal fin. En el RFC4880 se define el estándar OpenPGP, el mismo que ha sido implementado con el nombre de GNUPG.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • Código Postal: 170518 / Quito - Ecuador • Teléfono: 593-2 294-7800
www.arcotel.gob.ec

17. **Política de Seguridad.-** Conjunto de reglas establecidas por la autoridad de seguridad de la empresa, que rigen la utilización y prestación de servicios y facilidades de seguridad de la red.

18. **Redes de Confianza**.- Es una agrupación de organismos, dentro de los cuales forma parte el Centro de Respuesta a Incidentes Informáticos de la ARCOTEL, que colaboran entre sí en la gestión de vulnerabilidades e incidentes de seguridad informática a través del intercambio de información exclusivamente entre sus miembros.

19. **Reporte.-** Son los informes que remiten los prestadores de servicios de telecomunicaciones a la ARCOTEL como respuesta a la gestión de incidentes y vulnerabilidades, de acuerdo a los formatos establecidos para tal fin.

20. **Tiempo de Respuesta.-** Tiempo en el cual los prestadores de servicios de telecomunicaciones o la ARCOTEL deben remitir la respuesta de las acciones tomadas frente a las notificaciones de incidentes o vulnerabilidades.

21. **TLP (Traffic Light Protocol).-** Protocolo de semáforo o protocolo de señales de tráfico; es un esquema de categorización de la información manejado a nivel de redes de confianza entre centros de respuesta a incidentes y vulnerabilidades de seguridad de las redes y servicios de telecomunicaciones.

22. **Vulnerabilidad.-** Es una debilidad en un sistema que permite a un atacante con conocimiento del hecho, atentar contra la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.

TÍTULO II

CONSIDERACIONES TÉCNICAS

Artículo 4.- Coordinación de Gestión.- La ARCOTEL deberá coordinar la gestión de vulnerabilidades e incidentes con los encargados de seguridad de las redes públicas de telecomunicaciones de los prestadores de servicios de telecomunicaciones del país.

Artículo 5.- Actividades de ARCOTEL.- La ARCOTEL, será la encargada de ejecutar las actividades establecidas en el marco de esta Norma, respecto a su Comunidad Objetivo: actividades de tipo reactivas para la coordinación de la gestión de vulnerabilidades e incidentes, actividades preventivas o proactivas como son la generación de alertas, advertencias y comunicados; incluyendo, entre otras, la función de brindar información para responder a los incidentes, analizar las causas técnicas, proponer soluciones y recomendar a los prestadores de servicios de telecomunicaciones, la implementación de las estrategias de gestión a vulnerabilidades o incidentes.

La ARCOTEL controlará que los prestadores de servicios de telecomunicaciones adopten las medidas de gestión adecuadas para preservar la seguridad de las redes públicas de telecomunicaciones de todo el país, y cooperar con equipos de respuesta nacionales o extranjeros para la gestión de vulnerabilidades e incidentes de seguridad.

Artículo 6.- Procedimientos de Gestión.- Para preservar la seguridad de sus servicios, reducir el impacto de la ocurrencia de una vulnerabilidad de la red y garantizar el secreto de las comunicaciones y de la información transmitida por sus redes, es obligación de los prestadores de servicios de telecomunicaciones establecer procedimientos relacionados con vulnerabilidades e incidentes, en los que se considere al menos el registro, priorización, análisis, escalamiento y gestión.

La ARCOTEL notificará a los prestadores de servicios de telecomunicaciones que deben presentar los procedimientos técnicos implementados para la gestión de vulnerabilidades e incidentes, así como el plazo en el que dicha información debe ser entregada.

Dirección: Av. Diego de Almagro N31 95 entre Whymper y Alpallana • Código Postal: 170518 / Quito Ecuador • Teléfono: 593-2 294 780
www.arcotel.gob.ec

TÍTULO III

NOTIFICACIONES

CAPÍTULO I
GENERACIÓN DE NOTIFICACIONES

Artículo. 7.- Generación de Notificaciones.- Las notificaciones de vulnerabilidades e incidentes de seguridad de las redes o servicios de telecomunicaciones pueden generarse por:

1. **Notificaciones de la ARCOTEL a los prestadores de servicios de telecomunicaciones**, sobre vulnerabilidades e incidentes presentes en la red del prestador o vinculados a sus abonados o clientes.

2. **Notificaciones de los prestadores de servicios de telecomunicaciones a la ARCOTEL**, sobre incidentes provenientes de otras redes tanto nacionales como internacionales y que afecten la seguridad de su red y sus servicios. Este reporte se realiza al correo electrónico incidente@ecucert.gob.ec. Posteriormente la ARCOTEL notificará al (los) prestador (es) de servicios de telecomunicaciones involucrados para que procedan con la atención correspondiente.

Las acciones realizadas, relativas a la gestión de vulnerabilidades o incidentes deben ser comunicadas a la ARCOTEL, conforme a los tiempos establecidos en el Título VII, Capítulo I, de esta Norma.

CAPÍTULO II

CATEGORIZACIÓN DE LA INFORMACIÓN Y PRIORIZACIÓN DE NOTIFICACIONES PARA LA GESTIÓN DE INCIDENTES Y VULNERABILIDADES

Artículo 8.- Categorización y Priorización.- Las notificaciones y reportes que se intercambien entre la ARCOTEL y los prestadores de servicios de telecomunicaciones así como la información contenida en las mismas,, relacionadas con la gestión de incidentes y vulnerabilidades, deberán ser categorizadas acorde los siguientes criterios:

1. **Prioridad:**

   A cada notificación de vulnerabilidad o incidente se le otorgará una prioridad considerando, al menos como parámetros, el impacto y urgencia para su gestión. Dichos parámetros se definen a continuación:

   a. El impacto se define para evaluar en qué grado la vulnerabilidad o incidente afectarían a la seguridad de los servicios, invulnerabilidad de la red, el secreto de las comunicaciones y la información transmitida por la red.

   b. La urgencia se define como la rapidez con la que la vulnerabilidad o el incidente de seguridad de la información debe ser atendido o solucionado.

   Las vulnerabilidades e incidentes se clasificarán de acuerdo a cuatro niveles de prioridad, los que serán establecidos por la ARCOTEL siguiendo el procedimiento detallado en el artículo 9 de la presente Norma, y que corresponden a: Crítica, Alta, Media o Baja. Según la prioridad asignada, se designarán los recursos necesarios y adecuados para su gestión en los términos y plazos establecidos.

   Para el caso de notificaciones de nuevos tipos de vulnerabilidades e incidentes informáticos que aún no hayan sido previamente categorizados por la ARCOTEL, se asumirá el criterio de prioridad "Media" hasta que se le asigne el criterio de prioridad.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • Código Postal: 170518 / Quito - Ecuador • Teléfono: 593-2 294-780
www.arcotel.gob.ec

2. **Categorización:**

Para la determinación de la categorización de la información contenida en las notificaciones o reportes se deberá tomar en cuenta lo dispuesto en la Constitución de la República del Ecuador, en el artículo 66, numeral 19, relacionada con el derecho a la protección de datos de carácter personal; lo establecido en la Ley Orgánica de Telecomunicaciones Título VIII referente al Secreto de las Telecomunicaciones y Protección de Datos Personales; a lo dispuesto en el Reglamento General a la Ley Orgánica de Telecomunicaciones Titulo XV Secreto de la Comunicación y Protección de Datos.

Se utilizará el protocolo TLP, según el cual quien remite la información debe categorizarla de acuerdo a uno de los siguientes criterios: Pública General, Pública Comunitaria, Sensible y Confidencial, con base al detalle que se describe a continuación:

a. **Información Pública General (TLP: Blanco.- Difusión sin restricción)**

La información categorizada con TLP Blanco, es aquella información que la ARCOTEL o el prestador de servicios de telecomunicaciones podrán difundir entre los miembros de su comunidad o el público en general. Este tipo de información debe cumplir con las siguientes consideraciones:

i. Su divulgación no representa riesgo para el abonado o cliente al cual se relaciona la información.
ii. Para su tratamiento no es necesario establecer restricciones especiales, más allá de las recomendaciones sobre el buen uso y conservación de la información.
iii. Su difusión o utilización no transgrede derechos de autor.

b. **Información Pública Comunitaria (TLP: Verde.- Difusión dentro de la comunidad)**

La ARCOTEL o el prestador de servicios de telecomunicaciones podrán compartir la información con miembros específicos de la Comunidad Objetivo, anonimizando la información para no causar perjuicio al propietario de la misma. Este tipo de información nunca debe ser publicada en internet o cualquier medio al cual el público en general pueda acceder.

i. Se debe observar la no transgresión de los derechos de autor.
ii. Se puede compartir con miembros que no pertenezcan al mismo sector, siempre y cuando sirva para prevenir que sean afectados por la misma vulnerabilidad o incidente.

c. **Información Sensible (TLP: Ámbar.- Difusión limitada)**

Este tipo de información puede ser difundida por la ARCOTEL o por los prestadores de servicios de telecomunicaciones, a los miembros de su equipo de seguridad, o con prestadores de servicios de telecomunicaciones que tengan relación directa en la solución del incidente o vulnerabilidad a la que se relaciona la información; y, con los clientes o, abonados que necesitan conocerla, para gestionar a una vulnerabilidad o incidente de seguridad de la información.

El dueño de la información deberá autorizar el uso de la misma cuando se requiera su utilización para un propósito distinto al original, y que no se encuentre enmarcado en cualquiera de los aspectos establecidos en esta Norma; es decir, que no sea para la gestión de un incidente o vulnerabilidad,

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • Código Postal: 170518 / Quito Ecuador • Teléfono: 593-2 294-780
www.arcotel.gob.ec

por lo que bajo ninguna circunstancia se trasmitirá a terceros de forma verbal, escrita, o electrónica, sin autorización expresa del dueño de la información.

i. Se debe asegurar la existencia de controles que garanticen la integridad y seguridad de información sensible, cuando sea transmitida por cualquier medio, cumpliendo como mínimo con lo indicado en el Anexo 1 "Protección de la Información".
ii. Se evitará imprimir documentos que contengan información sensible, más allá de lo estrictamente necesario, por lo cual se recomienda el intercambio de información a través de correo electrónico firmado y cifrado cumpliendo como mínimo con las condiciones establecidas en el Anexo 1.

d. **Información Confidencial (TLP: Rojo.- Solo para destinatarios específicos)**

La información catalogada como confidencial sólo podrá ser difundida por la ARCOTEL o por los prestadores de servicios de telecomunicaciones, a miembros específicos de éstas, y será únicamente accedida por los destinatarios de la misma, prohibiéndose la compartición de este tipo de información, incluso a un nivel superior, ya que su difusión fuera del grupo deseado, podría tener un impacto en la privacidad, reputación o en la operación del negocio; si es mal utilizada.

i. Si la información necesita ser extendida fuera del grupo deseado, se requiere autorización explícita por escrito del dueño de la información.
ii. En general se debe evitar imprimir este tipo de información.
iii. La transmisión de esta información se la debe realizar únicamente a través de medios seguros que garanticen la prohibición de acceso por parte de personas no autorizadas.
iv. Este tipo de información debe cumplir, como mínimo, con las medidas de seguridad establecidas en el Anexo 1.

Artículo 9.- Asignación de Prioridad de las Notificaciones.- La ARCOTEL elaborará los documentos con la asignación inicial de prioridad de vulnerabilidades e incidentes registrados, tomando en consideración los datos estadísticos existentes, así como otros parámetros y referencias nacionales e internacionales, para lo cual seguirá las siguientes acciones:

1. El documento deberá ser puesto en conocimiento de los prestadores de servicios de telecomunicaciones, mediante comunicaciones por correo electrónico, por escrito o cualquier otro medio válido.

2. En el documento se establecerá un término de quince (15) días, haciendo constar la fecha límite, para que los prestadores de servicios de telecomunicaciones emitan las observaciones debidamente sustentadas respecto de la asignación de prioridades.

3. Cumplido el término anterior, la ARCOTEL analizará las observaciones recibidas, en un término de quince (15) días y procederá, de ser necesario, a modificar las prioridades asignadas.

4. Luego del análisis realizado, ARCOTEL dará a conocer el listado de las prioridades asignadas a los incidentes y vulnerabilidades.

Artículo 10.- Cambio de los Niveles de Prioridad Asignados.- El cambio de la prioridad previamente asignada a un determinado incidente o vulnerabilidad se lo podrá realizar luego de transcurridos 3 (tres) meses de la asignación inicial de la prioridad. El procedimiento se instruirá por iniciativa propia de la ARCOTEL o a solicitud de uno o varios prestadores de servicios de telecomunicaciones, en cuyo caso, deberán sustentar debidamente la solicitud. Una vez que se

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alcalana • Código Postal: 170518 / Quito - Ecuador • Teléfono: 593-2 294-7800
www.arcotel.gob.ec

ha aceptado proceder con el cambio de prioridad, se debe seguir los pasos descritos en el artículo anterior.

La ARCOTEL deberá comunicar por cualquier medio válido, en un término no mayor a 8 (ocho) días, al (los) prestador (es) de servicios de telecomunicaciones, la aprobación, negación o el pedido de información adicional, en caso de que se requiera, con respecto de la solicitud presentada.

En caso de haber sido requerida información por parte de la ARCOTEL, el prestador de servicios de telecomunicaciones deberá presentar la información adicional solicitada en un término máximo de 3 (tres) días. Una vez recibida dicha información, la ARCOTEL tendrá 5 (cinco) días para emitir una respuesta al (los) prestador (es) de servicios de telecomunicaciones.

Artículo 11.- Asignación de Niveles de Prioridad a nuevos Incidentes o Vulnerabilidades Identificados.- La ARCOTEL, según se vayan identificando nuevos incidentes o vulnerabilidades, les asignará prioridades siguiendo los pasos descritos en el artículo 9 de la presente Norma.

La ARCOTEL mantendrá publicada en la página web institucional la información actualizada de niveles de prioridad asignados a los incidentes y vulnerabilidades conocidos.

TÍTULO IV

PROTECCIÓN DE LA INFORMACIÓN

Artículo 12.- Confidencialidad y No Divulgación de información como parte de las actividades de gestión de incidentes o vulnerabilidades.- El (los) encargado (s) de seguridad del prestador de servicios de telecomunicaciones, previo al comienzo de sus actividades en la gestión de incidentes o vulnerabilidades, deberán firmar Acuerdo (s) de Confidencialidad o establecerse cláusulas de confidencialidad y no divulgación durante el proceso de contratación de personal, con el representante legal de la empresa prestadora de servicios de telecomunicaciones o persona natural titular de una habilitación para prestar servicios de telecomunicaciones, o sus delegados, en el que se establezcan las obligaciones respecto a la no divulgación y tratamiento de información.

Los Acuerdos de confidencialidad podrán basarse en lo contemplado en el **Anexo 2** "Modelo de Acuerdo de Confidencialidad y No Divulgación de Información" de la presente Norma, que se presenta como referencia.

Artículo 13.- Consideraciones para el intercambio de Información relacionada con incidentes o vulnerabilidades.- Para el intercambio de información de incidentes o vulnerabilidades, se deberá considerar lo siguiente:

1. La información intercambiada entre el prestador de servicios de telecomunicaciones y la ARCOTEL, relacionada con la gestión de incidentes y vulnerabilidades, deberá establecer el nivel de confidencialidad alineado al protocolo de categorización TLP.

2. Toda información que ha sido remitida sin otorgarle un criterio de confidencialidad, se tratará como sensible (TLP: ÁMBAR).

3. El nivel de prioridad y confidencialidad que se otorgue a la información intercambiada se mantendrá durante su tratamiento; podrá ser reconsiderada siempre a un nivel mayor al inicialmente establecido pero no a uno inferior.

4. Para el intercambio de información vía correo electrónico se deberá incluir el criterio de categorización TLP, en el asunto del correo electrónico, de la siguiente manera:

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • Código Postal: 170518 / Quito Ecuador • Teléfono: 593-2 294-780
www.arcotel.gob.ec

ASUNTO: Asunto **[TLP: COLOR]**

5. Para el caso de intercambio de información de manera impresa se deberá incluir el color TLP adecuado para indicar qué alcance tiene la difusión de dicha información, normalmente incluyendo el texto "TLP: COLOR" en la cabecera o pie del documento. En caso de que la información sea TLP AMBAR o ROJO, se deberá entregar en sobre cerrado e indicando que la información es sensible o confidencial, respectivamente. Para el caso del TLP ROJO se deberá especificar en el sobre que debe ser abierto únicamente por el destinatario.

Artículo 14.- Consideraciones para el intercambio de información a través de correo electrónico.- Los mensajes de correo electrónico generados por la ARCOTEL hacia los prestadores de servicios de telecomunicaciones, y de los prestadores hacia la ARCOTEL, deberán incluir una Cláusula de Confidencialidad; los prestadores que así lo deseen pueden utilizar el contenido propuesto en el Anexo 3 "Cláusula de confidencialidad para correo electrónico" de la presente Norma Técnica, el cual es referencial.

La ARCOTEL y los prestadores de servicios de telecomunicaciones, implementarán controles de seguridad, para el intercambio cifrado de los mensajes de correo electrónico y otros documentos necesarios en la gestión de vulnerabilidades e incidentes, tanto para la transmisión de información como para su almacenamiento, de acuerdo al Anexo 4 "Firmado y cifrado en el intercambio de correo electrónico y documentos" de la presente Norma Técnica.

Artículo 15.- Requerimientos de Autoridad Competente.- Ante un requerimiento de la autoridad competente, el prestador de servicios de telecomunicaciones proporcionará la información solicitada, la cual en caso de ser Sensible o Confidencial, deberá salvaguardar sus propiedades de seguridad, indicando la categorización de la misma.

TÍTULO V

RESPALDO Y CONSERVACIÓN DE LA INFORMACIÓN RELACIONADA CON LA GESTIÓN DE INCIDENTES Y VULNERABILIDADES

Artículo 16.- Respaldo.- La información referente a la gestión de incidentes y vulnerabilidades, ya sea notificada por la ARCOTEL, o que corresponda a los casos detectados por los prestadores de servicios de telecomunicaciones, será respaldada de manera que se garantice la confidencialidad, integridad y disponibilidad de la misma; es obligación del prestador el mantener la evidencia documentada.

Artículo 17.- Conservación.- La información referente a la gestión de vulnerabilidades e incidentes, ya sea notificada por la ARCOTEL, o los casos detectados por los prestadores de servicios de telecomunicaciones, será conservada por éstos últimos de acuerdo al siguiente detalle:

1. Información Pública General o Pública Comunitaria: durante 6 (seis) meses;

2. Información Sensible: durante un (1) año;

3. Información Confidencial: durante tres (3) años.

Artículo 18.- Identificación de Abonados o Clientes relacionados con Incidentes y Vulnerabilidades.- Con la finalidad de que se puedan gestionar las vulnerabilidades o incidentes, el prestador de servicios de telecomunicaciones deberá almacenar, por un lapso de 1 (un) año, la información relativa a la asignación de direcciones IP de sus clientes o abonados, con el propósito de identificar a clientes o abonados que poseían una dirección IP pública o la dirección IP privada en caso de estar disponible, la información incluirá la fecha y hora en que la IP fue asignada, independientemente de la tecnología o protocolo utilizado para la asignación de direcciones.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec

De ser requerida esta información en casos específicos, por pedido de autoridad competente, la misma será provista por parte de los prestadores siguiendo los procedimientos establecidos en la LOT y los reglamentos.

TÍTULO VI

DIFUSIÓN DE INFORMACIÓN

Artículo 19.- Obligación de Información.- En caso de presentarse el riesgo de violación de seguridad a la red pública o de un servicio de telecomunicaciones, los prestadores de servicios de telecomunicaciones informarán dentro de los términos establecidos en el artículo 22 de la presente Norma Técnica, a sus abonados o clientes sobre dicha vulnerabilidad o incidente y las medidas que adoptará para atenuar o mitigar el riesgo. Esta información podrá ser enviada de manera general o a determinados abonados o clientes, de acuerdo al ámbito de afectación.

En caso de violación de seguridad de los datos de un abonado o cliente particular, para aplicación del artículo 79 de la LOT, el prestador notificará de tal violación a dicho abonado o cliente en forma inmediata, describiendo al menos la naturaleza de la violación de los datos personales, los puntos de contacto donde puede obtenerse más información, las medidas recomendadas para atenuar los posibles efectos adversos de dicha violación y las medidas ya adoptadas frente a la violación de los datos personales.

Para el control del cumplimiento del presente artículo, las notificaciones realizadas por el prestador de servicios de telecomunicaciones a sus abonados o clientes debe ser comunicada de manera simultánea al Centro de Respuestas de Incidentes Informáticos de la ARCOTEL, al correo electrónico notificaciones@ecucert.gob.ec; el prestador de servicios de telecomunicaciones deberá mantener un registro de las comunicaciones realizadas.

La ARCOTEL podrá realizar publicaciones de incidentes o vulnerabilidades con fines informativos y de prevención, siempre y cuando la misma no exponga ni relacione a su Comunidad Objetivo; por tanto, el texto utilizado se limitará a describir de manera general y concreta la amenaza y el escenario técnico de análisis y mitigación por parte de los prestadores de servicios de telecomunicaciones.

TÍTULO VII
GESTIÓN Y REPORTE DE VULNERABILIDADES E INCIDENTES

CAPÍTULO I

GESTIÓN DE NOTIFICACIONES EMITIDAS POR LA ARCOTEL A LOS PRESTADORES DE SERVICIOS DE TELECOMUNICACIONES.

Artículo 20.- Sistema de Gestión de Comprobantes.- La ARCOTEL para cada vulnerabilidad o incidente receptado, generará una notificación dirigida al prestador de servicios de telecomunicaciones que debe gestionar la vulnerabilidad o incidente. El objetivo es determinar el inicio de las acciones de gestión, y dar a conocer el número asignado al caso (número de ticket o comprobante), para facilitar su seguimiento.

La ARCOTEL, para el caso 2 del artículo 7 de la presente Norma Técnica, deberá realizar el análisis previo de las notificaciones y una vez que se determine como procedentes, deberán ser comunicadas a los prestadores de servicios de telecomunicaciones involucrados, en un tiempo no mayor a tres días contados desde que se recibió la notificación inicial en la ARCOTEL.

Todas las notificaciones de vulnerabilidades o incidentes, de fuentes de información nacional o internacional, enviados para la gestión desde la ARCOTEL hacia el prestador de servicios de telecomunicaciones contendrán al menos la siguiente información:

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • Código Postal: 170518 / Quito Ecuador • Teléfono: 593-2 294-780
www.arcotel.gob.ec

Campo	Posibles valores del campo
Número de ticket-comprobante	Número de notificación
Evento	Incidente o vulnerabilidad
Prioridad	Crítica, alta, media o baja
Confidencialidad (TLP)	Rojo, ámbar, verde o blanco
Tipo de usuario	Abonados o clientes, Infraestructura propia.

Artículo 21.- Gestión de notificaciones.- En relación con la gestión de notificaciones, se deberá cumplir lo siguiente:

1. La ARCOTEL, es responsable de: receptar, validar, analizar, clasificar y priorizar las notificaciones de vulnerabilidades o incidentes recibidos de las fuentes de información previo a la coordinación con los prestadores de servicios de telecomunicaciones para su gestión.

2. Los prestadores de servicios de telecomunicaciones deberán entregar a la ARCOTEL la información del bloque o bloques de direcciones IP que son asignados a:

    a. Abonados y Clientes

    b. Infraestructura propia.

    De presentarse actualizaciones o modificaciones en los bloques de direcciones IP, deberá informarse a la ARCOTEL en un término de quince (15) días para su actualización, siguiendo las consideraciones descritas previamente.

3. El/los encargado/s de seguridad designado/s por el prestador de servicios de telecomunicaciones, serán responsables de receptar, analizar, gestionar y dar seguimiento al trámite de las vulnerabilidades e incidentes de seguridad de la información que le sean notificadas por la ARCOTEL o que hayan sido detectadas por sí mismos.

Artículo 22.- Tiempos de recepción, gestión y respuesta de notificaciones.- Los prestadores de servicios de telecomunicaciones deberán cumplir con los siguientes términos para notificar las acciones implementadas o a implementarse para la gestión de los incidentes y vulnerabilidades reportadas por la ARCOTEL.

a) **Para Vulnerabilidades.-** Frente a cada notificación enviada por la ARCOTEL al prestador de servicios de telecomunicaciones, y considerando la prioridad otorgada a la vulnerabilidad, se deben cumplir los siguientes tiempos máximos:

Vulnerabilidad	Tiempos máximos
Prioridad	Recepción, Gestión y Respuesta a la ARCOTEL
Crítica	4 días hábiles
Alta	8 días hábiles
Media	Informativa
Baja	Informativa

En caso de que ARCOTEL requiera información respecto de la gestión de determinadas vulnerabilidades con prioridad media o baja, solicitará el reporte

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • Código Postal: 170518 / Quito Ecuador • Teléfono: 593-2 294-7800
www.arcotel.gob.ec

respectivo al prestador, el mismo que deberá ser presentado en el término de diez (10) días.

b) **Para Incidentes.-** Frente a cada notificación enviada por la ARCOTEL al prestador de servicios de telecomunicaciones, y considerando la prioridad otorgada al incidente, se deberán cumplir los siguientes tiempos:

Incidente	Tiempos máximos
Prioridad	Recepción, Gestión y Respuesta a la ARCOTEL
Crítica	1 día calendario
Alta	2 días hábiles
Media	4 días hábiles
Baja	Informativa

En caso de que ARCOTEL requiera información respecto de la gestión de determinados incidentes con prioridad baja, solicitará el reporte respectivo al prestador, el mismo que deberá ser presentado en el término de diez (10) días.

Artículo 23.- Estados de Gestión.- La gestión de vulnerabilidades o incidentes por parte del prestador de servicios de telecomunicaciones podrá tener los siguientes estados:

1. **Atendido.-** Se establece cuando la vulnerabilidad o incidente fue gestionado en su totalidad, o cuando el prestador de servicios de telecomunicaciones presenta los justificativos con los cuales se pone en conocimiento de la ARCOTEL la gestión realizada respecto de la vulnerabilidad o incidente.

2. **Pendiente.-** Se establece cuando la gestión de la vulnerabilidad o incidente se ha realizado de manera parcial. El prestador de servicios de telecomunicaciones debe indicar una fecha en la que completará la gestión total de la vulnerabilidad o incidente.

3. **En análisis.-** Se establece cuando la gestión total de la vulnerabilidad o incidente requiere de la toma de acciones que están fuera del alcance inmediato del prestador de servicios de telecomunicaciones. Se deberá justificar para análisis de la ARCOTEL.

Las vulnerabilidades o incidentes catalogados como pendientes o en análisis, podrán alcanzar el estado de atendidos, previa presentación de los justificativos por parte del prestador de servicios de telecomunicaciones ante la ARCOTEL, quien luego del análisis respectivo procederá a comunicar al prestador de servicios de telecomunicaciones las observaciones debidamente sustentadas en caso de existir, en un término no mayor a cinco (5) días. Los justificativos se presentarán de parte del prestador de servicios de telecomunicaciones, dentro del tiempo máximo de gestión y respuesta establecido en el artículo 22 de la presente Norma Técnica. El tiempo que tome la ARCOTEL en revisar los justificativos presentados por el prestador de servicios de telecomunicaciones no serán imputados a los términos establecidos en el artículo 22.

La ARCOTEL podrá solicitar información adicional al prestador de servicios durante el análisis de la justificación presentada, quién deberá entregar la información en el término o plazo que la ARCOTEL establezca para el efecto.

CAPÍTULO II

GESTIÓN DE NOTIFICACIONES DE PERSONAS NATURALES O JURÍDICAS

Artículo 24.- Gestión de vulnerabilidades e incidentes que involucren a la Comunidad Objetivo de la ARCOTEL.- Las notificaciones originadas en información generada por personas naturales o jurídicas, organismos nacionales o internacionales, en relación con el

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • Código Postal: 170518 / Quito Ecuador • Teléfono: 593-2 294-780
www.arcotel.gob.ec

ámbito de la presente Norma, se realizará a través del formulario de la página web (www.ecucert.gob.ec), correo electrónico (incidente@ecucert.gob.ec), comunicación escrita, o vía telefónica. Los servidores públicos de la ARCOTEL receptarán, validarán, analizarán, y priorizarán las notificaciones recibidas, previo el envío a los prestadores de servicios de telecomunicaciones que correspondan, para su gestión en un término de cinco (5) días.

CAPÍTULO III

REPORTE DE GESTIÓN POR PARTE DE PRESTADORES DE SERVICIOS DE TELECOMUNICACIONES A LA ARCOTEL

Artículo 25.- Reporte del estado de gestión a la ARCOTEL.- Respecto de las notificaciones enviadas por la ARCOTEL a los prestadores de servicios de telecomunicaciones, se deberá remitir los correspondientes reportes de acuerdo al siguiente detalle:

a) **Para Vulnerabilidades.-** En el envío de la información de respuesta (reporte) sobre la gestión de las vulnerabilidades se tendrán en cuenta los tiempos establecidos en el artículo 22, letra a) de la presente Norma, la respuesta se enviará en contestación al correo electrónico con el cual el prestador de servicios de telecomunicaciones recibió el número de comprobante (ticket) asignado; todo esto utilizando el Formato que la ARCOTEL establezca.

b) **Para Incidentes.-** Referente al reporte sobre la gestión de incidentes, se tendrán en cuenta los tiempos establecidos en el artículo 22, letra b) de la presente Norma, la respuesta se enviará en contestación al correo electrónico con el cual el prestador de servicios de telecomunicaciones recibió el número de comprobante (ticket) asignado; todo esto utilizando el Formato que la ARCOTEL establezca.

Para el caso de las vulnerabilidades e incidentes con carácter informativo se cerrarán automáticamente a los sesenta (60) días bajo el estado "Cerrado – Sin respuesta".

El comprobante continuará abierto en el sistema de gestión de la ARCOTEL para incidentes y vulnerabilidades, hasta que el prestador reporte debidamente las acciones tomadas para la solución de todas las direcciones IP en el ámbito de su competencia. El reporte se realizará en el Formato que la ARCOTEL establezca.

Artículo 26.- Reporte de vulnerabilidades o incidentes detectados y solucionados por el prestador de servicios de telecomunicaciones.- Los reportes de vulnerabilidades o incidentes detectados y solucionados por el prestador de servicios de telecomunicaciones y que tengan una prioridad crítica, alta o que requieran el apoyo técnico de la ARCOTEL, deberán ser enviados al correo electrónico incidente@ecucert.gob.ec, para su registro.

Artículo 27.- Forma de reporte de vulnerabilidades o incidentes detectados y gestionados por el prestador de servicios de telecomunicaciones.- Para el reporte de vulnerabilidades e incidentes por parte de los prestadores de servicios de telecomunicaciones y que tengan una prioridad crítica, alta o que requieran el apoyo técnico de la ARCOTEL, se deberá cumplir lo siguiente:

1. **Reporte de vulnerabilidades.-** Las vulnerabilidades detectadas y gestionadas por los prestadores de servicios de telecomunicaciones, en su red o en sus clientes o abonados, y que no correspondan a los notificados por ARCOTEL, serán reportados mensualmente a dicha Agencia de manera consolidada por cada tipo de vulnerabilidad y tipo de usuario, dentro de los diez (10) primeros días del mes siguiente, utilizando el Formato que la ARCOTEL establezca

2. **Reporte de incidentes.-** Los incidentes detectados y gestionados por los prestadores de servicios de telecomunicaciones, en su red o en sus clientes o abonados, que no correspondan a los notificados por ARCOTEL, serán reportados en el término de siete

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • Código Postal: 170518 / Quito - Ecuador • Teléfono: 593-2 294-7800
www.arcotel.gob.ec

(7) días luego de su gestión, a la ARCOTEL, utilizando el Formato que la ARCOTEL establezca

Artículo 28.- Notificación de incidentes que pertenezcan a un prestador de servicios de telecomunicaciones diferente o cuya fuente de origen no se encuentre dentro del territorio nacional.- Para el caso de incidentes que afectan a un prestador de servicios de telecomunicaciones y que se originan en las redes de otro prestador de servicios de telecomunicaciones o cuyo origen no se encuentre dentro del territorio nacional, se debe remitir la notificación en el formato establecido por la ARCOTEL. Si el origen corresponde a redes del país, se consideran los tiempos para la respuesta y gestión que han sido definidos en el artículo 22, letra b) de la presente Norma Técnica; si el origen está fuera del país, la ARCOTEL procederá con la coordinación internacional, para lo cual no aplican los tiempos definidos en el artículo 22 de esta Norma.

Artículo 29.- Escalamiento de incidentes detectados y que requieren apoyo de ARCOTEL.- Para el caso de incidentes de seguridad en las redes y servicios detectados por el prestador de servicios de telecomunicaciones en su red, o en la de sus clientes o abonados, y que no puedan ser solucionados, podrán solicitar apoyo técnico a la ARCOTEL remitiendo el formato establecido por la ARCOTEL.

Se dispondrá de los mismos tiempos para la respuesta y gestión que han sido definidos en el artículo 22, letra b) de la presente Norma Técnica.

Artículo 30.- Gestión de Incidentes y vulnerabilidades que involucre las redes de los abonados o clientes.-

1. Si la gestión al problema presentado en la red del abonado o cliente, consiste en el bloqueo o limitación de ciertos contenidos o aplicaciones; en atención de lo establecido en la LOT en su artículo 24, número 17, el prestador de servicios de telecomunicaciones podrá proceder con dicho bloqueo o limitación siempre y cuando el abonado o cliente manifieste expresamente su consentimiento, o por disposición de autoridad competente. El prestador de servicios deberá mantener el registro de la autorización o consentimiento del abonado o cliente.

   Si el abonado o cliente no autoriza o no expresa su consentimiento en el término de quince (15) días contados a partir del siguiente día de haber sido comunicado; cumplido el término, el prestador de servicios notificará del particular a la ARCOTEL en un término máximo de dos días, adjuntando el respaldo de las comunicaciones realizadas al abonado o cliente.

   Con base en el análisis del caso y la documentación remitida por el prestador de servicios, la ARCOTEL podrá tomar las acciones pertinentes conforme el ordenamiento jurídico vigente en relación al abonado o cliente.

2. Para los casos en los que la gestión de incidentes o vulnerabilidades de las redes públicas de telecomunicaciones requiera correctivos por parte del cliente o abonado, el prestador del servicio informará al abonado o cliente acerca del particular, indicándole las medidas técnicas que debe tomar para solucionar el problema. Es obligación del abonado o cliente adoptar las medidas sugeridas por el prestador de servicios, a fin de salvaguardar la integridad de la red y las comunicaciones, sin perjuicio de las responsabilidades de los prestadores.

Los términos asignados al abonado o cliente no serán contabilizados dentro de aquellos establecidos en el artículo 22 de la presente Norma Técnica para gestión de incidentes o vulnerabilidades que deben cumplir los prestadores de servicios de telecomunicaciones.

Artículo 31.- Elaboración y actualización de formularios.- Corresponde a la ARCOTEL la elaboración y actualización de los formatos para aplicación de la presente Norma Técnica, así

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • Código Postal: 170518 / Quito - Ecuador • Teléfono: 593-2 294-7800
www.arcotel.gob.ec

como sus respectivos instructivos. En caso de producirse modificaciones en los mismos, la ARCOTEL comunicará por escrito a los prestadores de servicios de telecomunicaciones involucrados.

TÍTULO VIII

DERECHOS Y OBLIGACIONES DE LOS PRESTADORES DE SERVICIOS DE TELECOMUNICACIONES Y DE LOS ABONADOS O CLIENTES.

Artículo 32.- Obligaciones de los prestadores de servicios de telecomunicaciones.- Adicional a las obligaciones de los poseedores de títulos habilitantes para la prestación de servicios de telecomunicaciones contempladas en el artículo 24 de la Ley Orgánica de Telecomunicaciones, en el artículo 59 de su Reglamento General, y las establecidas en los títulos habilitantes u otras normas o reglamentos emitidos por la ARCOTEL, los prestadores de servicios de telecomunicaciones, tendrán las siguientes obligaciones:

1. Cumplir con los tiempos de gestión y reporte, establecidos en la presente Norma Técnica.

2. Entregar la información en los formularios que para el efecto publique la ARCOTEL.

3. En caso de que se haya determinado el riesgo de violación de la red pública o del servicio de telecomunicaciones, el prestador de servicios de telecomunicaciones informará a sus abonados o clientes, de acuerdo a lo establecido en la presente Norma.

4. Remitir información solicitada por el Centro de Respuesta a Incidentes Informáticos de la ARCOTEL, relacionada con la gestión de vulnerabilidades e incidentes informáticos.

Artículo 33.- Derechos de los prestadores de servicios de telecomunicaciones.- Adicional a los derechos de los poseedores de títulos habilitantes para la prestación de servicios de telecomunicaciones contempladas en el artículo 25 de la Ley Orgánica de Telecomunicaciones, en el artículo 58 de su Reglamento General, y las establecidas en los títulos habilitantes u otras normas o reglamentos emitidos por la ARCOTEL, los prestadores de servicios de telecomunicaciones, tendrán los siguientes derechos:

1. Disponer de los formatos para la presentación de reportes establecidos en la presente Norma Técnica.

2. Disponer del documento con los niveles de prioridad asignados por la ARCOTEL.

3. Reportar ante la ARCOTEL acerca de incidentes y vulnerabilidades originados en otros prestadores de servicios de telecomunicaciones, para que se coordinen las acciones de atención correspondientes.

4. Sugerir a los clientes, abonados o suscriptores adoptar medidas a fin de salvaguardar la integridad de la red y las comunicaciones.

Artículo 34.- Obligaciones de los abonados o clientes.- Adicional a las obligaciones que deben cumplir los abonados, clientes o usuarios, contempladas en el artículo 23 de la Ley Orgánica de Telecomunicaciones, en el artículo 57 de su Reglamento General, y las establecidas en los títulos habilitantes u otras normas o reglamentos emitidos por la ARCOTEL, los abonados o clientes de los servicios de telecomunicaciones tendrán las siguientes obligaciones:

1. Adoptar las medidas sugeridas por el prestador de servicios a fin de salvaguardar la integridad de la red y las comunicaciones.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec

2. No realizar alteraciones a los equipos que puedan causar interferencias o daños a las redes y servicios de telecomunicaciones en general.

Artículo 35.- Derechos de los abonados o clientes.- Adicional a los derechos de los abonados, clientes o usuarios, contempladas en el artículo 22 de la Ley Orgánica de Telecomunicaciones, en el artículo 56 de su Reglamento General, y las establecidas en los títulos habilitantes u otras normas o reglamentos emitidos por la ARCOTEL, los abonados o clientes de los servicios de telecomunicaciones tendrán los siguientes derechos:

1. A utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación, desarrollo o servicio legal a través de Internet o en general de sus redes u otras tecnologías de la información y las comunicaciones. Se exceptúan aquellos casos en los que el cliente o abonado solicite de manera previa su decisión expresa de limitación o bloqueo de contenidos, o por disposición de autoridad competente.

2. A incorporar o utilizar cualquier clase de instrumentos, dispositivos o aparatos en la red, siempre que sean legales, salvo las excepciones establecidas en la normativa vigente.

3. A disponer y recibir los servicios de telecomunicaciones contratados de forma continua, regular, eficiente, con calidad y eficacia.

4. Al secreto e inviolabilidad del contenido de sus comunicaciones, con las excepciones previstas en la Ley.

5. A la privacidad y protección de sus datos personales, por parte del prestador con el que contrate servicios, con sujeción al ordenamiento jurídico vigente.

6. A que su prestador le informe oportunamente sobre la interrupción, suspensión o averías de los servicios contratados y sus causas, en relación con la aplicación de la presente Norma Técnica.

7. A recibir información del prestador de servicios de telecomunicaciones, acorde a lo establecido en la presente Norma, sobre el riesgo de la violación de la red pública o de un servicio de telecomunicaciones y las medidas que adoptará para atenuar o eliminar el riesgo, así como; de ser el caso, las medidas que debe adoptar el abonado o cliente.

TÍTULO IX

SEGURIDAD DE REDES Y SERVICIOS

Artículo 36.- Auditoría.- La ARCOTEL, podrá disponer a los prestadores de servicios de telecomunicaciones, la realización, a costo del prestador de una auditoría de seguridad, con el fin de identificar vulnerabilidades y mitigar los riesgos que podrían afectar a la seguridad de la red y los servicios que se brindan. Las auditorías deben ser realizadas por un organismo público, autoridad competente o, de ser el caso, por una empresa privada o persona natural independiente, aplicando estándares vigentes y reconocidos a nivel internacional; estas auditorías deben incluir al menos pruebas de vulnerabilidad y penetración a su propia red.

Los prestadores deberán ejecutar planes de acción sobre las vulnerabilidades detectadas para preservar la seguridad de sus servicios la invulnerabilidad de la red y garantizar el secreto de las comunicaciones y de la información transmitida por sus redes.

Hasta el 30 de noviembre de cada año, la ARCOTEL notificará por escrito, a las empresas prestadoras de servicios de telecomunicaciones que durante el año siguiente al de la notificación deberán cumplir con la obligación establecida en el presente artículo, para lo cual se considerará lo siguiente:

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • Código Postal: 170518 / Quito Ecuador • Teléfono: 593-2 294-780
www.arcotel.gob.ec

1. La recurrencia de incidentes relacionados con la red del prestador, su nivel de afectación en relación con el tamaño de la red o la cantidad de abonados o clientes afectados por los incidentes.

2. La recurrencia en la detección de vulnerabilidades y las acciones tomadas por el prestador de servicios de telecomunicaciones, en relación con el tamaño de la red y la cantidad de abonados o clientes vinculados.

3. En general, tamaño de la red o aspectos relacionados con los equipos de la misma y su operación, que puedan implicar la generación de riesgos o vulnerabilidades relevantes.

El prestador de servicios de telecomunicaciones deberá comunicar a la ARCOTEL con al menos 15 días de anticipación la fecha en la que tiene planificado ejecutar la auditoría, incluyendo el alcance de análisis de riesgos relacionados con las vulnerabilidades existentes en los servicios y redes de telecomunicaciones y la duración de la misma.

Como resultado de la auditoría, el prestador de servicios de telecomunicaciones deberá presentar ante la ARCOTEL en un término no superior a treinta (30) días luego de finalizada la misma, un informe ejecutivo de la auditoría. En el caso de que la ARCOTEL requiera información adicional, se solicitará al prestador del servicio.

En el caso de que la ARCOTEL requiera información técnica de los resultados obtenidos se solicitará por escrito los puntos sobre los cuales se requieren información, para garantizar la confidencialidad de la información se deberá indicar su clasificación y aplicar los mecanismos de protección descritos en la presente Norma.

Artículo 37.- Infraestructura Crítica respecto de la Gestión de Incidentes y Vulnerabilidades.- Como resultado de la auditoría y con el fin de preservar la seguridad de los servicios y la invulnerabilidad de la red, los prestadores de servicios de telecomunicaciones identificarán los equipos críticos de su infraestructura sobre la cual brindan el servicio, así como también deberán almacenar en una ubicación específica, los registros referentes a seguridad e invulnerabilidad de la red que generen éstos. Los registros deberán almacenarlos al menos por un año.

Se considera infraestructura crítica aquella que:

1. Como resultado de la auditoría se ha determinado que presentan vulnerabilidades.

2. Históricamente se ha identificado que son susceptibles a incidentes relacionados con seguridad de las redes y servicios, sobre la base de registros de la propia empresa o de otras empresas.

3. Equipos, cuya afectación originada por un incidente o que como resultado de la materialización de una vulnerabilidad, implique la violación de la seguridad de la red, servicios y de los datos personales de los abonados o clientes, entendiéndose como tal la destrucción, accidental o ilícita, la pérdida, la revelación o el acceso no autorizados, de datos personales transmitidos, almacenados o tratados en la prestación de un servicio de telecomunicaciones.

El reporte infraestructura crítica, deberá contener como mínimo:

1. El nombre del equipo, marca y modelo.

2. Vulnerabilidades detectadas.

3. Historial de incidentes propios (ocurridas en el mencionado equipo).

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • Código Postal: 170518 / Quito Ecuador • Teléfono: 593-2 294-780
www.arcotel.gob.ec

4. Tipo de información afectada en caso de ocurrencia de un incidente.

Artículo 38.- Acciones para la identificación de ataques o eventos de seguridad de redes.- La ARCOTEL, a fin de que los prestadores de servicios de telecomunicaciones adopten las medidas técnicas y de gestión adecuadas para preservar la seguridad de sus servicios y la invulnerabilidad de la red y garantizar el secreto de las comunicaciones y de la información transmitida por sus redes, elaborará y ejecutará conjuntamente con los prestadores acciones conjuntas orientadas a la adquisición de información que permita identificar posibles ataques o correlacionar eventos de seguridad en las redes, para lo cual los prestadores facilitarán apoyo logístico, técnico y administrativo, en cumplimiento de lo dispuesto en el artículo 85 de la LOT.

Los prestadores de servicios de telecomunicaciones brindarán a la ARCOTEL, cuando dicha Agencia lo solicite, las facilidades técnicas para que ésta ejerza las tareas de control relacionadas con la comprobación de las medidas implementadas para garantizar el secreto de las comunicaciones y seguridad de datos personales, en cumplimiento de lo establecido en el artículo 83, párrafo 1 de la LOT.

TÍTULO X

CONTACTOS Y NOTIFICACIONES

Artículo 39.- Encargados de Seguridad.- Para la coordinación de las acciones contempladas en la presente Norma Técnica, es obligación de los prestadores de servicios de telecomunicaciones, que previamente han sido notificados por la ARCOTEL, procedan a designar al menos un empleado, quien actuará como encargado de seguridad. La designación deberá constar por escrito y ser remitida a la ARCOTEL.

Se deberá remitir de forma escrita a la ARCOTEL los nombres completos, cargo, teléfonos de contacto, y correos electrónicos, designación del (los) encargado (s) de seguridad designado (s). En caso de presentarse modificaciones en las designaciones realizadas o en su información de contacto, estas deberán ser comunicadas a la ARCOTEL por escrito o medio electrónico, para su actualización, en un tiempo máximo tres (3) días laborables.

DISPOSICIONES GENERALES

PRIMERA.- La ARCOTEL difundirá la guía de uso del protocolo TLP, misma que deberá ser publicada en su página WEB institucional en un término no mayor a treinta (30) días contados a partir de la publicación de la presente Norma en el Registro Oficial. Adicionalmente, la ARCOTEL implementará una página web propia para la gestión de incidentes y en general para la aplicación de la presente Norma Técnica.

SEGUNDA.- La información de contacto, direcciones de correo electrónico, u otra información de carácter público que sea necesaria para la aplicación de la presente Norma Técnica, se publicará por parte de la ARCOTEL en la página web institucional www.ecucert.gob.ec.

DISPOSICIONES TRANSITORIAS

PRIMERA.- En un término máximo de treinta (30) días, desde la publicación de la presente Norma Técnica en el Registro Oficial, la ARCOTEL notificará por escrito a los prestadores de servicios de telecomunicaciones, que inicialmente y en un plazo máximo de nueve (9) meses contados a partir de la notificación, deberán proporcionar a la ARCOTEL, información de acuerdo a lo establecido en el número 1 del artículo 85 de la Ley Orgánica de Telecomunicaciones, y artículo 6 de la presente Norma Técnica.

SEGUNDA.- En un término de treinta (30) días, a partir de la publicación de la presente Norma Técnica en el Registro Oficial, la ARCOTEL notificará por escrito a los prestadores de servicios de telecomunicaciones que en un inicio deben remitir la información del (los)

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • Código Postal: 170518 / Quito - Ecuador • Teléfono: 593-2 294-780
www.arcotel.gob.ec

encargado (s) de seguridad designados de acuerdo a lo indicado en el artículo 39 de la presente Norma. Además deberán remitir la llave pública PGP/GPG a la ARCOTEL, de acuerdo a lo establecido en el Anexo 4 de la presente Norma.

TERCERA.- En un término de cuarenta y cinco (45) días, a partir de la publicación de la presente Norma Técnica en el Registro Oficial, la ARCOTEL realizará la publicación y notificación del listado inicial de prioridades asignadas a los incidentes y vulnerabilidades gestionados por el Centro de Respuesta a Incidentes Informáticos de la ARCOTEL, de acuerdo al procedimiento indicado en el artículo 9 de la presente Norma.

CUARTA.- La ARCOTEL publicará en su página WEB, en un término máximo de treinta (30) días contados a partir de la entrada en vigencia de la presente Norma Técnica, los formatos de aplicación de la presente Norma, así como sus respectivos instructivos de llenado, tomando en cuenta el criterio o aportes de los prestadores de servicios de telecomunicaciones.

QUINTA.- La ARCOTEL en un término de treinta (30) días luego de la entrada en vigencia de la presente Norma Técnica, notificará a los prestadores de servicios de telecomunicaciones que en un plazo máximo de tres (3) meses, contados a partir de la notificación respectiva, deberán remitir la información de los bloques de direcciones IP de acuerdo a lo establecido en el artículo 21, número 2) de la presente Norma Técnica.

SEXTA.- Los tiempos de gestión de incidentes y vulnerabilidades establecidos en el artículo 22 de la presente Norma Técnica serán de aplicación obligatoria, una vez que se hayan cumplido los términos y plazos de las Disposiciones Transitorias previas, establecidas en esta Resolución.

La presente Norma, entrará en vigencia a partir de su publicación en el Registro Oficial.
Dado en Quito, Distrito Metropolitano, a

Ing. Germán Alberto Célleri López
DIRECTOR EJECUTIVO
AGENCIA DE REGULACIÓN Y CONTROL DE LAS TELECOMUNICACIONES (S)

ELABORADO POR:	REVISADO POR	APROBADO POR
Dirección Técnica de Regulación de Servicios y Redes de Telecomunicaciones Ing. Alex Troya A. Dr. Gustavo Quijano	Dirección Técnica de Regulación de Servicios y Redes de Telecomunicaciones Ing. Pablo López P. Ing. Paulina Zhunio C. **DIRECTORA TÉCNICA DE LA CRDS (E)**	Coordinadora Técnica de Regulación, encargada. Ing. Ana Valdiviezo B.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • Código Postal: 170518 / Quito - Ecuador • Teléfono: 593-2 294-780
www.arcotel.gob.ec

ANEXO 1

PROTECCIÓN DE LA INFORMACIÓN.

1. MECANISMOS DE PROTECCIÓN DE LA INFORMACIÓN.

El encargado de seguridad del prestador de servicios de telecomunicaciones, considerará al menos los siguientes mecanismos para proteger la información:

1.1. Información Pública General y Pública Comunitaria.

Sobre este tipo de información, de acuerdo a su nivel de criticidad menor, en lo posible se mantendrá un control de integridad utilizando un control de cambios, asociable a la versión de cada documento o mediante la generación de un hash.

1.2. Información Sensible y Confidencial.

a. La información Sensible y Confidencial debe ser almacenada en sistemas o repositorios centralizados y para su acceso al menos se debe implementar un mecanismo de autenticación de usuario/clave (password), y tendrán acceso los encargados de seguridad y las personas a las que expresamente el prestador de servicios de telecomunicaciones haya establecido conforme a sus políticas internas.

b. Para el caso de la información Sensible y Confidencial que sea impresa, esta deberá ser almacenada en un solo archivo físico y su acceso asegurado mediante mecanismos biométricos a los cuales solo podrán acceder el encargado de seguridad y demás personas que el prestador de servicios de telecomunicaciones haya establecido conforme a sus políticas internas. En caso de no contar con mecanismos biométricos se deberá almacenar la información bajo llave cuyo custodio será el encargado de seguridad.

c. La información sensible y confidencial deberá ser cifrada para garantizar la confidencialidad e integridad de la información.

d. La información sensible y confidencial no se almacenará en dispositivos personales, tales como discos duros externos, pendrives, o similares, procurando que esta permanezca únicamente en equipos destinados exclusivamente para el efecto por el prestador de servicios de telecomunicaciones.

e. La información sensible y confidencial no deberá ser almacenada en ningún sitio remoto en Internet comúnmente denominados como "la nube"; únicamente se deberá almacenar en sistemas que estén bajo pleno control del encargado de seguridad del prestador de servicios de telecomunicaciones.

f. La información enviada en cualquier formato, ya sea electrónico, papel, audio, video u otros, que esté bajo responsabilidad del prestador de servicios de telecomunicaciones, no será utilizada, por sus encargados de seguridad o el personal que tenga acceso a la misma, de manera personal o en actividades ajenas a la gestión de incidentes informáticos y no será accesible a terceras personas, sin autorización previa del encargado de seguridad de la empresa.

2. INTEGRIDAD Y CONFIDENCIALIDAD DE INFORMACIÓN TRANSMITIDA DE MANERA FÍSICA O POR CORREO ELECTRÓNICO.

La ARCOTEL y los prestadores de servicios de telecomunicaciones intercambiarán información, tanto física como electrónica, de manera segura mediante técnicas de protección de la información que consideren al menos lo siguiente:

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • Código Postal: 170518 / Quito - Ecuador • Teléfono: 593-2 294-7800
www.arcotel.gob.ec

2.1. Información transmitida de manera física.

La información que requiera ser enviada en medios de almacenamiento físicos debe mantener los siguientes aspectos:

a) Los documentos deben ser entregado en sobre cerrado o sellado con el membrete indicando la categorización del documento.

b) En el envío de medios magnéticos sean CD's, DVD's, Memorias USB, Discos duros, u otros medios de almacenamiento de información, la información contenida será cifrada y la contraseña de descifrado junto con su SHA-2 será enviado en un correo seguro cifrado conforme Anexo No 4.

2.2. Información a remitirse por medio de correo electrónico.

a) Correo electrónico único (Empresarial), con un tamaño máximo de 10MB.

b) Creación de claves PGP/GPG del encargado de seguridad para la transacción segura de extremo a extremo.

c) Manejo de funciones Hash (SHA-2) criptográficas sobre archivos o documentos adjuntos al correo electrónico de incidentes de seguridad de la información.

d) En el caso de envío que requiera una capacidad superior a 10MB se deberá remitir un enlace seguro con acceso mediante usuario y contraseña enviado bajo correo electrónico seguro (PGP/GPG).

Importante:

Si la evidencia (información) tiene código malicioso o pueden comprometer equipos o servicios, deberá indicarse claramente, para su tratamiento.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec

ANEXO 2

MODELO DE ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE INFORMACIÓN.

ACUERDO SUSCRITO ENTRE EL ENCARGADO DE SEGURIDAD DEL PRESTADOR DE SERVICIOS Y LA MÁXIMA AUTORIDAD DE LA EMPRESA.

Intervienen en la celebración del presente Acuerdo de Confidencialidad, por una parte el Sr. XXXXX, en calidad de Encargado de Seguridad de la Información, de la empresa XXXXXX, designado a través del Acta o Documento #####, suscrita el ########, mayor de edad y domiciliado(a) en la ciudad de XXXX, identificado(a) como aparece al pie de su respectiva firma; en adelante conocido como "EL ENCARGADO DE SEGURIDAD DE LA INFORMACIÓN"; y por la otra, el Sr. XXXXX, en calidad de Representante Legal de la Empresa XXXXXXXXXXXXXXXXXXXXXXX, mayor de edad y domiciliado(a) en la ciudad de XXXXXXX, identificado(a) como aparece al pie de su firma.

PRIMERA.- ANTECEDENTES.

- La empresa XXXXXX dispone del correspondiente Título Habilitante otorgado con fecha XXXXXXX por la ARCOTEL para la provisión de los servicios de telecomunicaciones de XXXXXXX. El señor XXXXXX, con documento de identidad Nro. XXXXXX, fue nombrado representante legal de la empresa XXXXXX, según consta en la documentación de respaldo que se adjunta.

- El señor XXXXX, con documento de identidad No. XXXXXX, fue designado Encargado de Seguridad de la empresa XXXXXX, mediante Acta o Documento ##### de fecha XXXXXX, cuya copia se adjunta.

- Conforme el artículo 76 de la Ley Orgánica de Telecomunicaciones "*Medidas técnicas de seguridad e invulnerabilidad. Las y los prestadores de servicios ya sea que usen red propia o la de un tercero, deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de sus servicios y la invulnerabilidad de la red y garantizar el secreto de las comunicaciones y de la información transmitida por sus redes. Dichas medidas garantizarán un nivel de seguridad adecuado al riesgo existente.*".

- Artículo 84 de la Ley Orgánica de Telecomunicaciones "*Obligaciones adicionales. La Agencia de Regulación y Control de las Telecomunicación establecerá y reglamentará los mecanismos para supervisar el cumplimiento de las obligaciones tanto de secreto de las comunicaciones como de seguridad de datos personales y, en su caso, dictará las instrucciones correspondientes, que serán vinculantes para las y los prestadores de servicios, con el fin de que adopten determinadas medidas relativas a la integridad y seguridad de las redes y servicios...*".

SEGUNDA.- OBJETO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE INFORMACIÓN.

- El objeto del presente acuerdo se refiere al compromiso y obligación que asume el Encargado de Seguridad y la empresa XXXXXXXXXX, respecto a la confidencialidad y no divulgación de información que en ejercicio de las funciones obtienen o reportan para la gestión de vulnerabilidades o incidentes.

- El Encargado de Seguridad utilizará la información recibida con fines de generación de estadísticas, administración, manejo y gestión de vulnerabilidades o incidentes de seguridad de la información.

- El Encargado de Seguridad, únicamente utilizaran la información para el fin mencionado en la condición anterior, comprometiéndose a mantener la más estricta

confidencialidad, advirtiendo que dicha obligación se extiende a cualquier persona que por su relación con EL PRESTADOR, deba tener acceso a la información entregada, obtenida o elaborada.

- El Encargado de Seguridad no podrá reproducir, modificar, hacer pública o divulgar ya sea en forma oral, visual, escrita, grabada en medios magnéticos o en cualquier otra forma tangible, la información objeto del presente acuerdo, en cumplimiento con lo dispuesto en la Norma Técnica para la gestión de incidentes y vulnerabilidades.

- El Encargado de Seguridad asume la obligación de guardar secreto sobre cuanta información pudieran disponer con relación a la gestión de vulnerabilidades e incidentes y no comunicarlos a terceros, aún después de cinco (5) años de la finalizada la relación entre las partes.

TERCERA.- EXCEPCIONES.

Sin prejuicio de lo establecido en el presente Acuerdo, las partes aceptan que la obligación de confidencialidad no se aplicara en el siguiente caso:

- Cuando la información fuera de dominio público en el momento de su suministro al PRESTADOR, o una vez suministrada la información, esta acceda al dominio público sin transgredir ninguna de las condiciones del presente Acuerdo.

- Cuando un mandato judicial exija su divulgación. En este caso EL PRESTADOR proporcionará la información solicitada salvaguardando sus propiedades de seguridad e indicando la categorización de información.

CUARTA.- VIGENCIA Y PLAZO.

- El Acuerdo entrará en vigor en el momento de la firma del mismo por ambas partes y tiene validez hasta cinco (5) años después del cese de las funciones del encargado de seguridad.

QUINTA.- CONFLICTO.

En caso de cualquier conflicto o discrepancia que pueda surgir en relación con la interpretación y/o cumplimiento del presente Acuerdo, las partes se someten expresamente a los Jueces competentes de la ciudad de XXXXXX, con renuncia a su fuero propio, aplicándose la legislación vigente en la República del Ecuador.

SÉPTIMA.- INCUMPLIMIENTO.

El incumplimiento de las obligaciones establecidas en el presente Acuerdo de no Divulgación, dará lugar al inicio de las acciones administrativas, civiles y penales contempladas en la normativa jurídica vigente en el estado ecuatoriano.

Y en señal de expresa conformidad y aceptación de los términos recogidos en el presente acuerdo, lo firman las partes por duplicado.

Dado y firmado en Quito, a XX de XXX de 201X

Sr Encargado de Seguridad de la Prestadora de Servicios	Sr. Prestador/a de Servicios

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito - Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec

ANEXO 3

CLÁUSULA DE CONFIDENCIALIDAD PARA CORREO ELECTRÓNICO.

En los correos electrónicos, se deberá incluir el siguiente contenido acorde a la categorización de la información remitida en los mismos.

1. TLP Blanco y TLP Verde.

"La información contenida en este correo y sus anexos es pública. Si ha recibido este correo por error le solicitamos notificar a la persona que lo envió.

Este mensaje ha sido sometido a programas antivirus. No obstante, ARCOTEL/EMPRESA no asume ninguna responsabilidad por eventuales daños generados por el recibo y uso de este material, siendo responsabilidad del destinatario verificar con sus propios medios la existencia de virus u otros defectos."

2. TLP Amarillo.

"La información contenida en este correo y sus anexos es sensible y para uso exclusivo de la(s) persona(s) a quien(es) se dirige. Si el lector de esta transmisión electrónica no es el destinatario, se le notifica que cualquier distribución o copia de la misma está estrictamente prohibida. Si ha recibido este correo por error le solicitamos notificar inmediatamente a la persona que lo envió y borrarlo definitivamente de su sistema.

Este mensaje ha sido sometido a programas antivirus. No obstante, ARCOTEL/EMPRESA no asume ninguna responsabilidad por eventuales daños generados por el recibo y uso de este material, siendo responsabilidad del destinatario verificar con sus propios medios la existencia de virus u otros defectos."

3. TLP Rojo.

"La información contenida en este correo y sus anexos es confidencial y para uso exclusivo de la(s) persona(s) a quien(es) se dirige. Si el lector de esta transmisión electrónica no es el destinatario, se le notifica que cualquier distribución o copia de la misma está estrictamente prohibida. Si ha recibido este correo por error le solicitamos notificar inmediatamente a la persona que lo envió y borrarlo definitivamente de su sistema.

Este mensaje ha sido sometido a programas antivirus. No obstante, ARCOTEL/EMPRESA no asume ninguna responsabilidad por eventuales daños generados por el recibo y uso de este material, siendo responsabilidad del destinatario verificar con sus propios medios la existencia de virus u otros defectos."

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • Código Postal: 170518 / Quito - Ecuador • Teléfono: 593-2 294 780
www.arcotel.gob.ec

ANEXO 4

FIRMADO Y CIFRADO EN EL INTERCAMBIO DE CORREO ELECTRÓNICO Y DOCUMENTOS

Para el envío de correos electrónicos es necesario el establecimiento de medidas de seguridad que impidan su intercepción por terceros no autorizados. Es decir que los correos electrónicos y demás información que sea intercambiada con los encargados de seguridad de los prestadores de servicios de telecomunicaciones deben ser firmados y cifrados.

PGP/GPG (Pretty Good Privacy/GNU PGP) es un método estándar de software libre para la firma y cifrado de correo electrónico y archivos electrónicos. Se utiliza para cifrar mensajes y archivos y para verificar (a través de la firma) que la persona que originó el mensaje es quien dice ser. Cada servidor de la ARCOTEL, encargado de la coordinación de gestión de incidentes y vulnerabilidades, cuenta con un par de llaves PGP/GPG pública y privada por lo que los correos enviados, por defecto son firmados digitalmente, y cifrados en caso de contar con la llave pública del destinatario.

Los encargados de seguridad de los prestadores de servicios de telecomunicaciones tendrán un plazo de un mes luego de haber sido notificados por la ARCOTEL para la generación del par de llaves personales PGP/GPG pública y privada para el intercambio cifrado de correos y documentos con personal de la ARCOTEL. Dentro del mismo plazo deberán remitir la llave pública a ARCOTEL.

A partir del plazo establecido será obligatorio el cifrado de correos electrónicos, anexos y cualquier otro tipo de documento que esté relacionado con la Gestión de Vulnerabilidades e Incidentes de seguridad de las redes y servicios de telecomunicaciones y se envíe a través de este medio.

Para la creación del par de llaves PGP/GPG se pueden utilizar herramientas de software libre, que no involucran costos para el encargado de seguridad o el prestador de servicios de telecomunicaciones, siempre y cuando guarden compatibilidad.

Creación y almacenamiento de llaves PGP/GPG.

Los pares de llaves pública y privada, así como el certificado para el proceso de revocación son creados individualmente por cada encargado de seguridad de los prestadores de servicios de telecomunicaciones que deban gestionar vulnerabilidades e incidentes de manera coordinada con personal de la ARCOTEL. Una vez éstas han sido creadas, el encargado de seguridad del prestador de servicios de telecomunicaciones reportará la llave pública a la ARCOTEL para que sus miembros procedan a la firma y cifrado e iniciar con el intercambio seguro de información.

Las llaves creadas quedarán a custodia del encargado de seguridad del prestador de servicios de telecomunicaciones y éste deberá asegurarse que sean almacenadas en un repositorio que cuente con control de accesos para evitar lecturas no autorizadas.

Revocación de las llaves PGP/GPG.

El proceso de revocación de una llave PGP/GPG se dará en los siguientes casos:

- El encargado de seguridad del prestador de servicios de telecomunicaciones ya no realiza funciones de Gestión de Vulnerabilidades e Incidentes en coordinación con personal de la ARCOTEL.
- El encargado de seguridad del prestador de servicios de telecomunicaciones ha olvidado la contraseña de su llave privada.
- Existe la certeza o posibilidad fundada de que la llave privada ha sido comprometida.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito Ecuador • **Teléfono:** 593-2 294-780
www.arcotel.gob.ec

Para los dos últimos casos, el encargado de seguridad deberá crear un nuevo par de llaves pública y privada, y comunicar en un término no mayor a dos días a la ARCOTEL, adjuntando su nueva llave pública.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana • **Código Postal:** 170518 / Quito Ecuador • **Teléfono:** 593-2 294 780
www.arcotel.gob.ec