OBSERVACIONES AL PROYECTO DE NORMA TÉCNICA PARA COORDINAR LA GESTIÓN DE INCIDENTES Y VULNERABILIDADES QUE AFECTEN A LA SEGURIDAD DE LAS REDES Y SERVICIOS DE TELECOMUNICACIONES

OBSERVACIONES GENERALES

- Se sugiere que la norma sea para gestión de incidentes, puesto que es imposible garantizar la invulnerabilidad al 100% de una red, incluso a nivel internacional existe la obligación de solucionar incidentes, mientras que para las vulnerabilidades se hacen recomendaciones.
- El artículo 2 señala que dentro del ámbito de aplicación se incluye a los abonados clientes y usuarios, por lo que son responsables de la seguridad y uso de la red, la norma debe establecer claramente las responsabilidades y obligaciones de los abonados clientes y usuarios, actualmente la norma establece solo la responsabilidad al prestador del servicio de telecomunicaciones.
- Los prestadores de servicios de telecomunicaciones no puede exigir al abonado, cliente y usuario la gestión de su red, es necesario que la norma incluya cómo la ARCOTEL actuará frente a vulnerabilidades que son responsabilidad de los abonados clientes y usuarios.
- Se debe especificar en todo el documento que se trata de vulnerabilidades e incidentes de seguridad de red.
- La ARCOTEL se comprometió en el taller de remitir los formatos a fin de emitir observaciones sobre los mismos.
- Como empresa prestadora de servicios, se nos puede atribuir una responsabilidad por temas netamente inherentes al cliente como es el caso del uso del servicio de internet (ejemplo: suplantación de identidad, correo malicioso, estafa electrónica, etc), que no necesariamente puede catalogarse como una vulnerabilidad en la red con la cual se presta el servicio.
  Cabe indicar que el servicio garantiza accesibilidad desde o hacia a cualquier servidor o página web, bajo este concepto no debería existir el reporte de abonados por vulnerabilidad de la seguridad de su información, ya que si fuera el caso deberían ser vulnerabilidades de la red que afecten masivamente a nuestros clientes.

OBSERVACIONES ESPECÍFICAS

PROYECTO REGLAMENTO	PROPUESTA CNT EP	OBSERVACIONES
Artículo 1.- Objeto.- Esta Norma Técnica tiene como objeto, establecer criterios, medidas técnicas y de gestión, procedimientos; y, mecanismos de coordinación para que los prestadores de servicios del régimen general de telecomunicaciones, adopten las medidas técnicas y de gestión adecuadas para preservar la seguridad de sus servicios y la invulnerabilidad de la red y	**Artículo 1.- Objeto.-** Esta Norma Técnica tiene como objeto, establecer criterios, medidas técnicas y de gestión, procedimientos; y, mecanismos de coordinación para que los prestadores de servicios del régimen general de telecomunicaciones, adopten las medidas técnicas y de gestión ~~adecuadas~~ para preservar la seguridad de sus servicios y ~~la invulnerabilidad~~ de la red ~~y~~ a fin	Se sugiere aclarar cuáles serían las medidas y gestión adecuadas puesto que es un tema subjetivo y muy amplio. Es imposible garantizar la invulnerabilidad al 100% de una red.

garantizar, con un nivel de seguridad adecuado al riesgo existente, el secreto de las comunicaciones y de la información transmitida por sus redes.	de garantizar, ~~con un nivel de seguridad adecuado al riesgo existente,~~ el secreto de las comunicaciones y de la información transmitida por sus redes.	
Artículo 4.- Coordinación de Gestión.- La ARCOTEL será la encargada de coordinar la gestión de vulnerabilidades e incidentes de seguridad de los servicios y redes públicas de telecomunicaciones de los prestadores de servicios del régimen general de telecomunicaciones del país; como parte de dichas actividades la ARCOTEL podrá establecer políticas generales de seguridad, las cuales serán de cumplimiento obligatorio de los prestadores del régimen general de telecomunicaciones.	**Artículo 4.- Coordinación de Gestión.-** La ARCOTEL será la encargada de coordinar la gestión de vulnerabilidades e incidentes de seguridad de los servicios y redes públicas de telecomunicaciones de los prestadores de servicios del régimen general de telecomunicaciones del país; como parte de dichas actividades la ARCOTEL podrá establecer lineamientos ~~políticas~~ generales de seguridad. ~~las cuales serán de cumplimiento obligatorio de los prestadores del régimen general de telecomunicaciones~~ para lo cual los prestadores de servicios de telecomunicaciones informará las acciones adoptadas para la ejecución de los lineamientos establecidos por ARCOTEL.	No es competencia de ARCOTEL emitir políticas. De igual manera los lineamientos de seguridad no deben ser de carácter obligatorio puesto que cada prestador de servicios de telecomunicaciones es responsable de la seguridad de su propia red, y de determinar cómo resguardar y proteger su red de acuerdo al servicio que presta.
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. Tendrá además la función de brindar información para responder a los incidentes, analizar las causas técnicas, investigar soluciones y recomendar a los prestadores de servicios del régimen general de telecomunicaciones, o a la comunidad objetivo en general, la implementación de las estrategias de gestión a vulnerabilidades o incidentes.		Se sugiere que ARCOTEL aclare los servicios a través de una declaración bajo estándares internacionales de la implementación de un CERT.

La ARCOTEL controlará que los prestadores de servicios del régimen general de telecomunicaciones adopten las medidas técnicas y 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 resolución de vulnerabilidades e incidentes de seguridad.		
Artículo 6.- Procedimientos de Gestión.- 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, es obligación de los prestadores de servicios del régimen general de telecomunicaciones establecer procedimientos de gestión de vulnerabilidades e incidentes, en los que se considere al menos el registro, priorización, análisis, escalamiento y solución. La ARCOTEL notificará a los proveedores de servicios del régimen general de telecomunicaciones que deben presentar la información especificada en el presente artículo, así como el plazo en el que la deben entregar.	**Artículo 6.- Procedimientos de Gestión.-** 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, es obligación de los prestadores de servicios del régimen general de telecomunicaciones establecer procedimientos de gestión de vulnerabilidades e incidentes, en los que se considere al menos el registro, priorización, análisis, escalamiento y solución. La ARCOTEL notificará a los proveedores de servicios del régimen general de telecomunicaciones que deben presentar la información especificada en el presente artículo, así como el plazo en el que la deben entregar.	Es imposible garantizar la invulnerabilidad al 100% de una red.
Artículo 7.- Unidades Especializadas.- Con el fin de implementar acciones técnicas para la administración del secreto de las comunicaciones y seguridad de la red, los prestadores de servicios del régimen general de telecomunicaciones, podrán conformar unidades especializadas, con el número adecuado de personal, que se encarguen de tomar medidas relativas a la integridad y seguridad de la red y servicios, así como de gestionar	**Artículo 7.- Unidades Especializadas.-** Con el fin de implementar acciones técnicas para la administración del secreto de las comunicaciones y seguridad de la red, los prestadores de servicios del régimen general de telecomunicaciones, podrán conformar unidades especializadas, con el número adecuado de personal, que se encarguen de tomar medidas relativas a la integridad y seguridad de la red y servicios, así como de gestionar	Las prestadoras de servicios de telecomunicaciones no pueden gestionar en tiempos exactos las vulnerabilidades puesto que depende de la gravedad de las mismas y dependen del análisis de impacto que implican las mismas para la red y los servicios de la operadora.

vulnerabilidades e incidentes detectados en su red; con la finalidad de cumplir de manera obligatoria con los plazos de atención de incidentes y vulnerabilidades establecidos en esta norma.	vulnerabilidades e incidentes detectados en su red; con la finalidad de cumplir de manera obligatoria con los plazos de atención de incidentes ~~y vulnerabilidades~~ establecidos en esta norma.	
Artículo. 8.- Generación de Notificaciones.- (…) 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.	**Artículo. 8.- Generación de Notificaciones.-** (…) 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.	No se define el tiempo que dispone la ARCOTEL para la notificación al prestador. 7. En el artículo 8 "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 10 de la presente Norma.
Artículo 10.- Procedimiento de Asignación de Prioridad de las Notificaciones.- Tomando como referencia las estadísticas disponibles acerca de la solución o atención de incidentes y vulnerabilidades, la ARCOTEL, asignará prioridad a todos los incidentes y vulnerabilidades conocidos e identificados. Para lo cual seguirá el siguiente procedimiento. 1. La ARCOTEL elaborará, tomando en consideración los datos estadísticos existentes, un documento con la asignación inicial de prioridad a los incidentes y vulnerabilidades conocidos. 2. El documento deberá ser puesto en conocimiento de los prestadores del régimen general de telecomunicaciones, mediante publicación en su página web o vía comunicaciones por correo electrónico, por escrito o	**Artículo 10.- Procedimiento de Asignación de Prioridad de las Notificaciones.-** Tomando como referencia las estadísticas disponibles acerca de la solución o atención de incidentes y vulnerabilidades, la ARCOTEL, asignará prioridad a todos los incidentes y vulnerabilidades conocidos e identificados. Para lo cual seguirá el siguiente procedimiento. 1. La ARCOTEL elaborará, tomando en consideración los datos estadísticos existentes, un documento con la asignación inicial de prioridad a los incidentes y vulnerabilidades conocidos. 4. La ARCOTEL analizará y justificará las observaciones recibidas, y procederá, de ser necesario, a modificar las prioridades asignadas.	Para la aplicación del numeral uno se sugiere que el criterio de asignación de probabilidad no debe estar únicamente sujeto a estadísticas existentes por lo que para ello se plantea la adopción de estándares o mecanismos que permitan estimar el impacto derivado de vulnerabilidades identificadas y cuantificar la severidad que pueden representar dichas vulnerabilidades. Además, se deberá promover el uso de bases de datos de vulnerabilidades públicamente conocidas y de general aceptación tales como: National Vulnerability Database (NVDB), Common

cualquier otro medio válido. 3. En el documento publicado se establecerá un plazo de quince (15) días calendario, haciendo constar la fecha límite, para que los prestadores del régimen general de telecomunicaciones emitan las observaciones debidamente sustentadas respecto de la asignación de prioridades. 4. La ARCOTEL analizará las observaciones recibidas, y procederá, de ser necesario, a modificar las prioridades asignadas. 5. Luego del análisis realizado, ARCOTEL publicará el listado definitivo de las prioridades asignadas a los incidentes y vulnerabilidades.		Vulnerabilities and Exposures (CVE) u Open Source Vulnerability Database "OSVDB", con el fin de establecer un marco de trabajo bajo métricas base, dado que los riesgos planteados por una vulnerabilidad pueden cambiar con el transcurso del tiempo. Para la aplicación del numeral 4 se sugiere establecer criterios y parámetros que se consideraran para modificar la prioridad inicial asignada de igual manera el tiempo de respuesta por parte de ARCOTEL no debe ser imputable a los tiempos de gestión y respuesta de los requerimientos
Artículo 11.- 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 seis 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 del régimen general de telecomunicaciones, en cuyo caso, deberán sustentar debidamente la solicitud. Una vez que se 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 al (los) prestador (es) de servicios del régimen general de telecomunicaciones en el caso que no haya sido aceptada su solicitud de cambio de prioridad de un determinado incidente o		Se recomienda que el periodo de modificación no sea de 6 meses, pues es un periodo extenso y se contrapone con la gestión de vulnerabilidades puesto que la misma es dinámica.

vulnerabilidad.		
Artículo 14.- Consideraciones para el intercambio de Información.- Para el intercambio de información, se deberá considerar lo siguiente: 1. La información intercambiada entre el prestador de servicios del régimen general de telecomunicaciones y la ARCOTEL, relacionada con la gestión de incidentes y vulnerabilidades, deberá establecer el nivel de confidencialidad alineado al protocolo de clasificación 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 clasificación TLP, en el asunto del correo electrónico, de la siguiente manera: 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.-** Para el intercambio de información, se deberá considerar lo siguiente: 1. La información intercambiada entre el prestador de servicios del régimen general de telecomunicaciones y la ARCOTEL, relacionada con la gestión de incidentes y vulnerabilidades, deberá establecer el nivel de confidencialidad alineado al protocolo de clasificación 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 clasificación TLP, en el asunto del correo electrónico, de la siguiente manera: 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.	**Acuerdos de transferencia de la información** Los prestadores de servicios de telecomunicaciones y el Ente de Regulación y Control de Telecomunicaciones, previo a la entrega de información sensible para el giro específico del negocio, deberán suscribir acuerdos para transferir dicha información en el que se defina los controles mínimos que deberán implementar las partes, caso contrario, los prestadores de servicios estaríamos expuestos a que nuestra información sea divulgada, y de esta manera afectar los intereses empresariales y estrategias del negocio.

	Los prestadores de servicios de telecomunicaciones y el Ente de Regulación y Control de Telecomunicaciones, suscribirán acuerdos de transferencia de información.	
Artículo 17.- Respaldo.- Toda información referente a la gestión de vulnerabilidades e incidentes, ya sea notificada por la ARCOTEL, o que corresponda a los casos detectados por los prestadores de servicios del régimen general de telecomunicaciones, o los detectados por los abonados, clientes y usuarios; será respaldada de manera trimestral y se incluirá dentro del proceso de copias de respaldo y plan de recuperación de información que mantenga internamente el prestador de servicios del régimen general de telecomunicaciones, de acuerdo a las siguientes directrices o lineamientos, así como otras que establezca la ARCOTEL para tal fin. Las copias de respaldo deben conservarse en un sitio físico con acceso restringido bajo un sistema redundante evitando fallas y pérdida de información; para su transporte se utilizarán mecanismos de inviolabilidad y en caso de que sea una tercera empresa contratada para efectuar el transporte, el representante legal de esta, deberá firmar el respectivo compromiso de confidencialidad con el prestador de servicios del régimen general de telecomunicaciones que contrató sus servicios. Además, el prestador de servicios del régimen general de telecomunicaciones realizará comprobaciones de utilidad de las copias de seguridad dos veces al año y se evitará el uso de copias de seguridad en la nube con sistemas comerciales;	**Artículo 17.- Respaldo.-** Toda información referente a la gestión de vulnerabilidades e incidentes, ya sea notificada por la ARCOTEL, o que corresponda a los casos detectados por los prestadores de servicios del régimen general de telecomunicaciones, o los detectados por los abonados, clientes y usuarios; será respaldada en infraestructura local de cada prestador del servicio de telecomunicaciones dicha información tendrá el carácter confidencial. ~~de manera trimestral y se incluirá dentro del proceso de copias de respaldo y plan de recuperación de información que mantenga internamente el prestador de servicios del régimen general de telecomunicaciones, de acuerdo a las siguientes directrices o lineamientos, así como otras que establezca la ARCOTEL para tal fin.~~ ~~Las copias de respaldo deben conservarse en un sitio físico con acceso restringido bajo un sistema redundante evitando fallas y pérdida de información; para su transporte se utilizarán mecanismos de inviolabilidad y en caso de que sea una tercera empresa contratada para efectuar el transporte, el representante legal de esta, deberá firmar el respectivo compromiso de confidencialidad con el prestador de servicios del régimen general de telecomunicaciones que contrató sus servicios. Además, el prestador de servicios del régimen general de telecomunicaciones realizará comprobaciones de utilidad de~~	Los prestadores de servicios de telecomunicaciones tienen la obligación de respaldar la información de acuerdo a la infraestructura que tiene cada operador, no se debe imponer el método y mecanismo de respaldo.

es obligación del prestador el mantener adicionalmente la evidencia documentada, con los respaldos correspondientes de dichas comprobaciones.	~~las copias de seguridad dos veces al año y se evitará el uso de copias de seguridad en la nube con sistemas comerciales; es obligación del prestador el mantener adicionalmente la evidencia documentada, con los respaldos correspondientes de dichas comprobaciones.~~	
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 del régimen general de telecomunicaciones para su gestión. 2. Para el proceso de clasificación por tipo de usuario, en los casos que involucre direcciones IP, los prestadores de servicios del régimen general de telecomunicaciones deberán entregar a la ARCOTEL, en el plazo que ésta establezca, información del bloque o bloques de direcciones IP que son asignados a: a. Infraestructura propia b. Clientes corporativos c. Clientes sector público d. Clientes residenciales De presentarse modificaciones o actualizaciones en los bloques de IP, estas deberán ser comunicadas en un plazo no mayor a 48 horas siguiendo las consideraciones descritas previamente, para su inmediata actualización. 3. El encargado de seguridad designado por el prestador de servicios del régimen general de telecomunicaciones, es responsable de receptar, analizar, gestionar y dar seguimiento a la solución de las	**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 del régimen general de telecomunicaciones para su gestión. 2. ~~Para el proceso de clasificación por tipo de usuario, en los casos que involucre direcciones IP,~~ los prestadores de servicios del régimen general de telecomunicaciones deberán entregar a la ARCOTEL, en el plazo que ésta establezca, información del bloque o bloques de direcciones IP que son asignados para~~:~~ ~~a.~~ Infraestructura propia y clientes ~~b. Clientes corporativos~~ ~~c. Clientes sector público~~ ~~d. Clientes residenciales~~ De presentarse ~~modificaciones o~~ actualizaciones en los bloques de IP, el prestador de servicios de telecomunicaciones comunicará ~~estas deberán ser comunicadas~~ en el término de ~~un plazo no mayor a~~ 5 días laborables ~~48 horas siguiendo las consideraciones descritas previamente, para~~ su ~~inmediata~~ actualización. 3. El encargado de seguridad designado por el prestador de servicios del régimen general de telecomunicaciones, es	La Corporación Nacional de Telecomunicaciones no tiene una clasificación de IP como la solicita la ARCOTEL, es por eso que se sugiere que se mantenga el procedimiento que se realiza actualmente, que es la entrega de IP de infraestructura propia y clientes. En el numeral 3 se elimina la solución de vulnerabilidades puesto que existen casos que el plan de remediación se aplica en dependencia del riesgo detectado

vulnerabilidades e incidentes de seguridad de la información que le sean notificadas por la ARCOTEL o que hayan sido detectadas por sí mismos.	responsable de receptar, analizar, gestionar y dar seguimiento ~~a la solución~~ 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 Gestión de notificaciones.- Los prestadores de servicios del régimen general de telecomunicaciones deberán cumplir con los siguientes plazos para gestionar o dar solución a los incidentes o vulnerabilidades reportados por la ARCOTEL, así como dar respuesta a ésta respecto de las acciones tomadas. a) Para Vulnerabilidades.- Frente a cada notificación enviada por la ARCOTEL al prestador de servicios del régimen general de telecomunicaciones, y considerando la prioridad otorgada a la vulnerabilidad, se deben cumplir los siguientes tiempos máximos:	**Artículo 22.- Tiempos de Gestión de notificaciones.-** Los prestadores de servicios del régimen general de telecomunicaciones deberán cumplir con los siguientes plazos para gestionar o dar solución a los incidentes ~~o vulnerabilidades~~ reportados por la ARCOTEL, así como dar respuesta a ésta respecto de las acciones tomadas. ~~a) Para Vulnerabilidades.- Frente a cada notificación enviada por la ARCOTEL al prestador de servicios del régimen general de telecomunicaciones, y considerando la prioridad otorgada a la vulnerabilidad, se deben cumplir los siguientes tiempos máximos:~~ b) Para Incidentes.- Frente a cada notificación enviada por la ARCOTEL al prestador de servicios del régimen general de telecomunicaciones y considerando la prioridad otorgada al incidente, se deberán cumplir los siguientes tiempos: (…)	Con relación al literal a), no se debería considerar los tiempos establecidos por cuanto no todas las vulnerabilidades (en su mayoría) son posibles de solucionar. En tal sentido, se sugiere eliminar dicho literal. Con relación al literal b), los tiempos máximos de respuesta deben estar sujetos a una tipología y dimensionamiento de la infraestructura gestionada por los prestadores de servicios de régimen general de telecomunicaciones, así como por estándares internacionales de general aceptación, considerando que cumplimiento de los tiempos está en dependencia de varios factores (tamaño de la infraestructura, recursos de personal, procesos internos de gestión de incidentes, procesos de Gestión de Cambios, etc.). Cabe anotar además que no todos los operadores se encuentran en capacidad de implementar un CERT o una unidad especializada que cubra tiempos de operación 24/7, por lo que se solicita incluir una Disposición Transitoria Cuarta en la cual ARCOTEL evalúe dichos plazos luego de un periodo de prueba no

		mayor a seis meses de entrada en vigencia de la norma..
Artículo 23.- Estados de Gestión.- La gestión de vulnerabilidades o incidentes por parte del prestador de servicios del régimen general 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 régimen general de telecomunicaciones presenta los justificativos con los cuales la ARCOTEL apruebe 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 del régimen general 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 del régimen general de telecomunicaciones. Se deberá justificar y esperar aprobación por parte 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 del régimen general de telecomunicaciones ante la ARCOTEL, quien luego del análisis respectivo procederá a su aceptación o rechazo y lo		Es necesario aclarar que el tiempo que la ARCOTEL tome para el análisis y aprobación no sean imputables a los establecidos al operador en el artículo 22. Sería importante conocer cuáles son los criterios mínimos bajo los cuales la ARCOTEL aceptará la justificación.

comunicará al prestador de servicios del régimen general de telecomunicaciones. Los justificativos se presentarán de parte del prestador de servicios del régimen general de telecomunicaciones, dentro del tiempo máximo de gestión y respuesta establecido en el artículo 22 de la presente Norma Técnica; la ARCOTEL comunicará al prestador la aceptación o rechazo de justificativos, en un plazo no mayor a cuarenta (40) horas continuas, luego de recibida la justificación. El prestador de servicios del régimen general de telecomunicaciones deberá informar sobre los procedimientos internos de gestión para cada tipo de vulnerabilidad o incidente que la ARCOTEL reporta.		
Artículo 25.- Reporte del estado de gestión a la ARCOTEL.- Respecto de las notificaciones enviadas por la ARCOTEL a los prestadores de servicios del régimen general 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 del régimen general de telecomunicaciones recibió el número de comprobante (ticket) asignado; todo esto utilizando el Formato FO-CCDR-01, publicado por la ARCOTEL. El comprobante continuará abierto en el sistema de gestión de la ARCOTEL para incidentes y		-Para garantizar una adecuada gestión y control de los requerimientos enviados por ECUCERT se recomienda la implementación de una herramienta de gestión de incidentes que garantice la trazabilidad de todas las interacciones que se realicen en la gestión. -Es necesario aclarar que el tiempo que la ARCOTEL tome para el análisis, validación y aceptación de la solución no sean imputables a los establecidos al operador en el artículo 22.

vulnerabilidades, hasta que todas las direcciones IP que el prestador de servicios del régimen general de telecomunicaciones debe gestionar y reportar su estado a través del Formato FOCCDR-01, se encuentren en estado atendido. 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 del régimen general de telecomunicaciones recibió el número de comprobante (ticket) asignado; todo esto utilizando el Formato FO-CCDR-02. El comprobante/ticket continuará abierto en el sistema de gestión de incidentes informáticos de la ARCOTEL hasta que la solución sea aceptada por dicha Agencia. La ARCOTEL podrá solicitar cualquier información adicional, con respecto a las acciones tomadas en la solución de las vulnerabilidades o incidentes por parte del prestador de servicios del régimen general de telecomunicaciones, la cual deberá ser remitida por el prestador del servicio en los plazos indicados por la ARCOTEL, conforme el ordenamiento jurídico vigente.		
Artículo 26.- Reporte de vulnerabilidades o incidentes detectados y solucionados por el prestador de servicios del régimen general de telecomunicaciones.- Los reportes de vulnerabilidades o incidentes detectados y solucionados por el prestador de servicios del régimen general de telecomunicaciones deberán ser enviadas al correo electrónico	**Artículo 26.- Reporte de vulnerabilidades o incidentes detectados ~~y solucionados~~ por el prestador de servicios del régimen general de telecomunicaciones.-** Los reportes de vulnerabilidades o incidentes detectados ~~y solucionados~~ por el prestador de servicios del régimen general de telecomunicaciones deberán ser enviadas al correo electrónico	Para garantizar una adecuada gestión y control de los requerimientos enviados por ECUCERT se recomienda la implementación de una herramienta de gestión de incidentes que garantice la trazabilidad de todas las interacciones que se realicen en la gestión.

incidente@ecucert.gob.ec, para su registro.	incidente@ecucert.gob.ec, para su registro.	
Artículo 27.- Forma de reporte de vulnerabilidades o incidentes detectados y solucionados por el prestador de servicios del régimen general de telecomunicaciones.- Para el reporte de vulnerabilidades e incidentes por parte de los prestadores de servicios del régimen general de telecomunicaciones, se deberá cumplir lo siguiente: 1. Reporte de vulnerabilidades.- Las vulnerabilidades detectadas y solucionadas por los prestadores de servicios del régimen general de telecomunicaciones, en su red o en sus clientes, abonados o usuarios, 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 cinco (5) primeros días hábiles del mes siguiente, utilizando el Formato FO-CCDR-03, publicado por la ARCOTEL. 2. Reporte de incidentes.- Los incidentes detectados y solucionados por los prestadores de servicios del régimen general de telecomunicaciones, en su red o en sus clientes, abonados o usuarios, que no correspondan a los notificados por ARCOTEL, serán reportados en el plazo de tres (3) días hábiles luego de su solución, a la ARCOTEL, utilizando el Formato FO-CCDR-04. Para efectos de control, el prestador de servicios del régimen general de telecomunicaciones deberá mantener los respaldos correspondientes de la gestión de las vulnerabilidades o incidentes, de acuerdo a los tiempos establecidos en el artículo 18 de	**Artículo 27.- Forma de reporte de vulnerabilidades o incidentes detectados ~~y solucionados~~ por el prestador de servicios del régimen general de telecomunicaciones.-** Para el reporte de vulnerabilidades e incidentes por parte de los prestadores de servicios del régimen general de telecomunicaciones, se deberá cumplir lo siguiente: 1. Reporte de vulnerabilidades.- Las vulnerabilidades detectadas ~~y solucionadas~~ por los prestadores de servicios del régimen general de telecomunicaciones, en su red o en sus clientes, abonados o usuarios, 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 cinco (5) primeros días hábiles del mes siguiente, utilizando el Formato FO-CCDR-03, publicado por la ARCOTEL. 2. Reporte de incidentes.- Los incidentes detectados y solucionados por los prestadores de servicios del régimen general de telecomunicaciones, en su red o en sus clientes, abonados o usuarios, que no correspondan a los notificados por ARCOTEL, serán reportados en el plazo de tres (3) días hábiles luego de su solución, a la ARCOTEL, utilizando el Formato FO-CCDR-04. Para efectos de control, el prestador de servicios del régimen general de telecomunicaciones deberá mantener los respaldos correspondientes de la gestión de las vulnerabilidades o incidentes, de acuerdo a los tiempos establecidos en el artículo 18 de	Se elimina la solución de vulnerabilidades puesto que existen casos que el plan de remediación se aplica en dependencia del riesgo detectado

la presente Norma, y remitirla en caso de que la ARCOTEL lo solicite. Los tiempos de atención de los incidentes y vulnerabilidades deben estar de acuerdo a lo dispuesto en el artículo 22 de la presente Norma.	la presente Norma, y remitirla en caso de que la ARCOTEL lo solicite. Los tiempos de atención de los incidentes ~~y vulnerabilidades~~ deben estar de acuerdo a lo dispuesto en el artículo 22 de la presente Norma.	
Artículo 28.- Notificación de incidentes que pertenezcan a un proveedor 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 del régimen general de telecomunicaciones y que se originan en las redes de otro prestador de servicios del régimen general de telecomunicaciones o cuyo origen no se encuentre dentro del territorio nacional, se debe remitir el Formato FO-CCDR-05, 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, el prestador de servicios del régimen general de telecomunicaciones procederá con la coordinación internacional para lo cual no aplican los tiempos definidos en el artículo 22 de esta Norma.		La ARCOTEL deberá establecer los lineamientos de control y seguimiento que se dará a los incidentes y vulnerabilidades bajo coordinación internacional por cuanto el 70 % de eventos de seguridad registrados se encuentran bajo dicho escenario. Además, se deberá establecer las directrices sobre la intervención y participación de la ARCOTEL para subsanar las debilidades detectadas.
Artículo 30.- Elaboración y actualización de formularios.- Corresponde a la ARCOTEL la elaboración y actualización de los formularios FO-CCDR-01, FO-CCDR-02, FO-CCDR-03, FO-CCDR-04, FO-CCDR-05 y FO-CCDR-06, así como sus respectivos instructivos. En caso de producirse modificaciones en los mismos, la ARCOTEL comunicará por escrito a los prestadores de servicios del	**Artículo 30.- Elaboración y actualización de formularios.-** Corresponde a la ARCOTEL en el plazo de 30 días contados a partir de la publicación de la norma en el Registro Oficial, la elaboración y actualización de los formularios FO-CCDR-01, FO-CCDR-02, FO-CCDR-03, FO-CCDR-04, FO-CCDR-05 y FO-CCDR-06, así como sus respectivos instructivos, para lo cual deberá realizarse una	Es necesario establecer el plazo para la entrega de los formularios

régimen general de telecomunicaciones involucrados.	socialización. En caso de producirse modificaciones en los mismos, la ARCOTEL comunicará por escrito a los prestadores de servicios del régimen general de telecomunicaciones involucrados.	
Artículo 31.- Obligaciones de los Prestadores.- Adicional a las obligaciones de los poseedores de títulos habilitantes para la prestación de servicios del régimen general de telecomunicaciones contempladas en el artículo 24 de la Ley Orgánica de Telecomunicaciones y 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 del régimen general de telecomunicaciones, tendrán las siguientes obligaciones(...) 3. Para los casos en los que la solución de incidentes o vulnerabilidades requiera correctivos en los equipos o redes del cliente, abonado o usuario, y este último no realice los cambios correspondientes, el proveedor de servicios debe tomar las acciones necesarias para la solución o mitigación de vulnerabilidades e incidentes, procedimientos que serán puestos a consideración de la ARCOTEL en concordancia con lo descrito en el artículo 22, numerales 1 y 2; y, artículo 25, numeral 2, de la Ley Orgánica de Telecomunicaciones.	**Artículo 31.- Obligaciones de los Prestadores.-** Adicional a las obligaciones de los poseedores de títulos habilitantes para la prestación de servicios del régimen general de telecomunicaciones contempladas en el artículo 24 de la Ley Orgánica de Telecomunicaciones y 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 del régimen general de telecomunicaciones, tendrán las siguientes obligaciones(...) 3. Para los casos en los que la solución de incidentes o vulnerabilidades requiera correctivos en los equipos o redes del cliente, abonado o usuario, y este último no realice los cambios correspondientes, el proveedor de servicios debe tomar las acciones necesarias para la solución o mitigación de vulnerabilidades e incidentes, procedimientos que serán puestos a consideración de la ARCOTEL en concordancia con lo descrito en el artículo 22, numerales 1 y 2; y, artículo 25, numeral 2, de la Ley Orgánica de Telecomunicaciones.	Los prestadores de servicios de telecomunicaciones no tienen la potestad de obligar al cliente, abonado o usuario de realizar acciones específicas sobre el uso de su red.
Artículo 32.- Derechos de los Prestadores.- Adicional a los derechos de los poseedores de títulos habilitantes para la prestación de servicios del régimen general de telecomunicaciones contempladas en el artículo 25 de la Ley Orgánica de	**Artículo 32.- Derechos de los Prestadores.-** Adicional a los derechos de los poseedores de títulos habilitantes para la prestación de servicios del régimen general de telecomunicaciones contempladas en el artículo 25 de la Ley Orgánica de	Los prestadores de servicios de telecomunicaciones no podemos obligar a los abonados, clientes y usuarios de la aplicación de medidas de seguridad.

Telecomunicaciones y 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 del régimen general de telecomunicaciones, tendrán los siguientes derechos: 1. Disponer de los formatos para la presentación de reportes establecidos en la presente norma. 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 del régimen general 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.	Telecomunicaciones y 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 del régimen general de telecomunicaciones, tendrán los siguientes derechos: 1. Disponer de los formatos para la presentación de reportes establecidos en la presente norma. 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 del régimen general 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. 5. No ser sancionados por la ARCOTEL por incumplimientos de los clientes, abonados o suscriptores, de las medidas advertidas por los operadores de telecomunicaciones para salvaguardar la integridad de la red.	
Artículo 33- Auditoría.- Los prestadores de servicios del régimen general de telecomunicaciones que así lo determine la ARCOTEL, deberán realizar auditorías de seguridad, de infraestructura tecnológica, de seguridad de redes, seguridad de las comunicaciones y datos personales una vez al año, 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,	**Artículo 33- Auditoría.-** Los prestadores de servicios del régimen general de telecomunicaciones que así lo determine la ARCOTEL, deberán realizar auditorías de seguridad, de infraestructura tecnológica, de seguridad de redes, seguridad de las comunicaciones y datos personales una vez al año, 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:	Se sugiere incluir la posibilidad de realizar auditorías internas.

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 deben definir y 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. Previo a la ejecución de la auditoría de seguridad debe realizarse el correspondiente análisis de riesgos relacionados con las vulnerabilidades existentes en los servicios y redes de telecomunicaciones. Hasta el 30 de noviembre de cada año la ARCOTEL notificará por escrito, a las empresas del régimen general 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: 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 del régimen general 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	1.- Auditoria Interna. 2.-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 deben definir y 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. Previo a la ejecución de la auditoría de seguridad debe realizarse el correspondiente análisis de riesgos relacionados con las vulnerabilidades existentes en los servicios y redes de telecomunicaciones. Hasta el 30 de noviembre de cada año la ARCOTEL notificará por escrito, a las empresas del régimen general 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: 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 del régimen general de telecomunicaciones, en relación con el tamaño de la red y la cantidad de abonados o clientes vinculados.	

equipos de la misma y su operación, que puedan implicar la generación de riesgos o vulnerabilidades relevantes. El prestador de servicios del régimen general de telecomunicaciones deberá comunicar a la ARCOTEL con al menos 15 días hábiles de anticipación la fecha en la que tiene planificado ejecutar la auditoría, su alcance y la duración de la misma, con la finalidad de que en caso de considerarlo necesario participe con un servidor en la ejecución de las pruebas de la auditoría. Como resultado de la auditoría anual el prestador de servicios del régimen general de telecomunicaciones deberá presentar un informe ante la ARCOTEL en un plazo no superior a 30 días hábiles luego de finalizada la misma, el cual deberá incluir como mínimo lo siguiente: 1. Análisis preliminar de riesgos respecto de las vulnerabilidades en los servicios y redes de telecomunicaciones. 2. Información de la empresa, organismo o personas que ejecutaron la auditoría, lo que debe incluir datos de la experiencia relacionada con la realización de este tipo de auditorías. 3. Alcance y objetivos. 4. Estándares o procedimientos adoptados para llevar a cabo la auditoría. 5. Plan de ejecución, actividades y acciones. 6. Resultados de riesgos y vulnerabilidades detectados. 7. Medidas preventivas implementadas o por implementar. 8. Se deberá adjuntar el informe de la empresa o persona que ejecutó la auditoría. 9. Reporte de Equipos críticos.	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 del régimen general de telecomunicaciones deberá comunicar a la ARCOTEL con al menos 15 días hábiles de anticipación la fecha en la que tiene planificado ejecutar la auditoría, su alcance y la duración de la misma, con la finalidad de que en caso de considerarlo necesario participe con un servidor en la ejecución de las pruebas de la auditoría. Como resultado de la auditoría anual el prestador de servicios del régimen general de telecomunicaciones deberá presentar un informe ante la ARCOTEL en un plazo no superior a 30 días hábiles luego de finalizada la misma, el cual deberá incluir como mínimo lo siguiente: 1. Análisis preliminar de riesgos respecto de las vulnerabilidades en los servicios y redes de telecomunicaciones. 2. Información de la empresa, organismo o personas que ejecutaron la auditoría, lo que debe incluir datos de la experiencia relacionada con la realización de este tipo de auditorías. 3. Alcance y objetivos. 4. Estándares o procedimientos adoptados para llevar a cabo la auditoría. 5. Plan de ejecución, actividades y acciones. 6. Resultados de riesgos y vulnerabilidades detectados. 7. Medidas preventivas implementadas o por implementar. 8. Se deberá adjuntar el informe de la empresa o persona que ejecutó la auditoría. 9. Reporte de Equipos críticos.	

Artículo 34.- Equipos Críticos.- 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 del régimen general 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, en formato texto plano. Los registros deberán almacenarlos al menos por tres (3) años. Se consideran equipos críticos aquellos 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 usuarios, 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 servicios de telecomunicaciones. El reporte de equipos críticos deberá contener como mínimo: 1. El nombre del equipo 2. Ubicación del equipo (Dirección, coordenadas geográficas DATUM WGS84, formato decimal)	**Artículo 34.- Equipos Críticos.-** 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 del régimen general 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, en formato texto plano. Los registros deberán almacenarlos al menos por tres (3) años. Se consideran equipos críticos aquellos 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 usuarios, 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 servicios de telecomunicaciones. El reporte de equipos críticos deberá contener como mínimo: 1. El nombre del equipo 2. Ubicación del equipo (Dirección, coordenadas geográficas DATUM WGS84, formato decimal)	Los criterios establecidos bajo disposición normativa difieren de los criterios sustentados bajo riesgo instaurados por lo prestadores de servicios de régimen general de telecomunicaciones (Arquitectura de Seguridad instaurada). Sobre dicha base, los prestadores de servicios requeriremos un tiempo prudencial para la identificación e instauración del proceso que sustenta el reporte de equipos críticos. Además, dado que reporte deberá ser actualizado en forma periódica se requiere que la ARCOTEL establezca las directrices de control y actualización.

3. Vulnerabilidades detectadas. 4. Historial de incidentes propios (ocurridas en el mencionado equipo) 5. Historial de incidentes (ocurridos en otras empresas para el mismo tipo de equipos) 6. Tipo de información afectada en caso de ocurrencia de un incidente.	3. Vulnerabilidades detectadas. 4. Historial de incidentes propios (ocurridas en el mencionado equipo) 5. Historial de incidentes (ocurridos en otras empresas para el mismo tipo de equipos) 6. Tipo de información afectada en caso de ocurrencia de un incidente. Los prestadores de servicios de telecomunicaciones en el plazo de 6 meses contados a partir de la publicación de la presente norma para la identificación e instauración del proceso que sustenta el reporte de equipos críticos.	
	DISPOSICION GENERAL **DISPOSICIÓN GENERAL PRIMERA.- Control bianual** La Agencia de Regulación y Control de las telecomunicaciones será la encargada de realizar controles bianuales para mitigar incidentes que afecten la seguridad de las redes y servicios de telecomunicaciones	Con el objetivo de atenuar los impactos por posibles incidentes que afecten la seguridad de las redes y servicios de telecomunicaciones, y a efectos de que los controles no sean represivos para los operadores, se solicita que los controles sean bianuales, tomando en cuenta periodos trimestrales.
	DISPOSICIÓN TRANSITORIA TERCERA.- Para la ejecución de las actividades establecidas en el artículo 5 de la presente norma, la ARCOTEL emitirá en el plazo de 90 días la declaración y descripción de los servicios, así como los procedimientos vinculados a la gestión de cada servicio.	
	DISPOSICIÓN TRANSITORIA CUARTA.- Para determinar los tiempos de gestión de las notificaciones que se menciona en el literal b) del artículo 22 de la presente norma, la ARCOTEL deberá evaluar la aplicación de la norma por parte de los prestadores de servicios de telecomunicaciones y en el plazo de 6 meses contados a partir de	Los tiempos máximos de respuesta deben estar sujetos a una tipología y dimensionamiento de la infraestructura gestionada por los prestadores de servicios de régimen general de telecomunicaciones, así como por estándares internacionales de general

	la entrada en vigencia de la norma, en coordinación con los prestadores de servicios de telecomunicaciones establecerá los tiempos de gestión de las notificaciones.	aceptación, considerando que cumplimiento de los tiempos está en dependencia de varios factores (tamaño de la infraestructura, recursos de personal, procesos internos de gestión de incidentes, procesos de Gestión de Cambios, etc.). Cabe anotar además que no todos los operadores se encuentran en capacidad de implementar un CERT o una unidad especializada que cubra tiempos de operación 24/7.
	DISPOSICION TRANSITORIA QUINTA.- La ARCOTEL en el plazo de 180 días implementará una herramienta de gestión de incidentes que garantice la trazabilidad de todas las interacciones que se realicen en la gestión de incidentes y vulnerabilidades.	
DISPOSICIÓN FINAL.- Vigencia de la Norma *"La norma técnica para coordinar la gestión de incidentes y vulnerabilidades que afecten la seguridad de las redes y servicios de telecomunicaciones, entrarán en vigencia luego de transcurridos 365 días, contados a partir de su publicación en el Registro Oficial."*		Justificación: Actualmente la Empresa Pública no cuenta con las herramientas necesarias para realizar una implementación inmediata de los sistemas necesarios que permitirán cumplir lo establecido en la norma técnica, en tal virtud, se solicita un tiempo no menor a un año para contar con el personal suficiente y debidamente capacitado que permita a la Corporación cumplir con dicha norma técnica.