Telefónica

Quito, 7 de diciembre de 2017

VPR-16320-2017

Ingeniero
Washington Carrillo
Director Ejecutivo
ARCOTEL
En su despacho

De mi consideración:

En relación con el Proyecto "**NORMA TÉCNICA PARA COORDINAR LA GESTIÓN DE INCIDENTES Y VULNERABILIDADES QUE AFECTEN A LA SEGURIDAD DE LAS REDES Y SERVICIOS DE TELECOMUNICACIONES**" (en lo sucesivo, "la Norma Técnica"), exponemos las siguientes observaciones y sugerencias:

La Ley Orgánica de Telecomunicaciones (en adelante, "LOT") en su artículo 24 señala que es obligación de los Prestadores de Servicios de Telecomunicaciones (PST), garantizar el secreto e inviolabilidad de las telecomunicaciones, así como también es explícita en señalar que se deberán adoptar las medidas necesarias para garantizar la seguridad de las redes y para la protección de los datos personales de sus usuarios y abonados.

La LOT le otorga facultades específicas a ARCOTEL para establecer y reglamentar los mecanismos para supervisar el cumplimiento de las obligaciones tanto de secreto de las comunicaciones como de seguridad de datos personales; es por ello que se ha elaborado este Proyecto de Norma Técnica, en la que se establecen los procedimientos para gestionar las vulnerabilidades de red e incidentes informáticos que emita el EcuCERT.

La misma LOT establece que les corresponde a los PST adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad, así como establecer políticas de seguridad, las mismas que podrán ser **verificadas** por ARCOTEL.

Por su parte, OTECEL, S.A. ha adoptado acciones específicas para garantizar la seguridad de la red, estableciendo políticas internas de seguridad de red y protección de datos personales, mientras que, a nivel corporativo, se siguen políticas y gestión de seguridad desde un CSIRT global, acciones que nos permiten afirmar que la red y los datos personales de los usuarios tienen un alto nivel de seguridad conforme lo establece la LOT.

Estamos conscientes que cada día surgen amenazas a la seguridad de las redes, para lo cual, creemos que la acción del EcuCERT, como en todos los casos de este tipo de centros de alcance nacional, puede servir para mejorar la coordinación y el intercambio de información con las demás organizaciones que trabajan en el país, y así poder responder con eficacia a la ciberdelincuencia. Sin embargo, consideramos que a través del Proyecto de Norma Técnica propuesto, no es la manera más idónea de conseguir la colaboración, por las razones que se exponen a continuación.

1. GESTIÓN DE VULNERABILIDADES E INCIDENTES DE RED

Respecto a la regulación para GESTIONAR las vulnerabilidades e incidentes de seguridad, que reporta un CERT nacional, de la revisión realizada, en ningún caso se ha podido encontrar alguna norma que establezca como obligación un tiempo máximo de respuesta ante incidentes de seguridad y vulnerabilidades; y, peor aún que establezca todo un sistema de atención a través de tickets de las vulnerabilidades e incidentes de red, reportados por un CERT de alcance nacional.

Se observa que en España y Colombia se han emitido los siguientes documentos referenciales: "*Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información*"; y, "*Guía de Seguridad de las TIC CCN-STIC 817*", respectivamente. Las dos guías se refieren a tiempos **"recomendados"** para tratar únicamente incidentes de seguridad, en ningún caso para gestionar vulnerabilidades y menos como obligación de los operadores.

En relación a los incidentes de seguridad, revisando la Guía española, una vez notificado el incidente al organismo afectado por parte del CCN-CERT realizará un seguimiento del mismo, dependiendo de la peligrosidad del incidente. En el cuadro que se muestra a continuación, se observa que para los "incidentes" no hay obligación de realizar ningún reporte para los casos bajo y medio; mientras que para los casos Alto a Crítico, los tiempos de respuesta varían de cuarenta y cinco (45) días para un nivel alto, hasta ciento veinte (120) días para un nivel crítico.

Nivel de Peligrosidad	Obligación de notificación del ciberincidente al CCN-CERT(*)	Cierre del ciberincidente (días naturales)	Precisiones
BAJO	No	15	- Se cierran automáticamente por los Sistemas de Alerta Temprana a los 60 días con el estado "Cerrado – Sin respuesta". - El Sistema de Alerta Temprana no renotifica el aviso al organismo afectado.
MEDIO	No	30	
ALTO	Sí	45	
MUY ALTO	Sí	90	- No se cierran por el Sistema de Alerta Temprana. - Se cierran por el organismo afectado. - No debe asignarse nunca el estado "Cerrado – Sin respuesta) - El Sistema de Alerta Temprana re-notifica el aviso al organismo afectado cada siete días hasta recibir respuesta.
CRITICO	Sí	120	

Tabla 6 - Tipo de seguimiento a realizar por parte del CCN-CERT, según Nivel de Peligrosidad

Acerca de las vulnerabilidades, es importante mencionar que la UIT (Unión Internacional de Telecomunicaciones) en la serie de Recomendaciones X ha establecido arquitecturas multidimensionales en la que se definen las diferentes capas y planos en cada uno de los cuales existen proceso de seguridad y protección de la Red, los mismos que son cumplidos por gran parte de los operadores de redes. Este sistema permite que cualquier vulnerabilidad dependiendo de su explotabilidad, implique riesgos mínimos para el operador gracias a la arquitectura multidimensional, es por ello que en muchas ocasiones estas vulnerabilidades no afectan a los operadores incluso cuando están abiertas mucho tiempo.

Revisemos la definición de la vulnerabilidad de la Recomendación UIT-T X.800 y la que consta en la Norma Técnica:

> ITU: "(…) *Vulnerabilidad es toda debilidad que pudiera explotarse para violar un sistema o las informaciones que éste contiene*" (Cursivas nuestras).

Proyecto de Norma Técnica: "(...) *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*" (Cursivas nuestras).

Estas definiciones tienen una diferencia fundamental, y es el hecho de que la UIT determina la posibilidad de una violación del sistema, mientras que la definición del proyecto de Norma, el hecho de que exista la vulnerabilidad ya permite atentar contra la "*confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones*". La realidad no es así, ya que a pesar de que existe una vulnerabilidad, es muy baja la probabilidad de que se puedan superar todas las seguridades disponibles y, de esta manera, afectar realmente la seguridad de la red y los datos personales de los usuarios.

Por lo expuesto, en OTECEL, S.A. consideramos que los tiempos de respuesta no deben ser establecidos como de cumplimiento obligatorio, sino únicamente como sugeridos y exclusivamente para los casos de incidentes de seguridad; **en ningún caso** para tratar las vulnerabilidades de red.

Respecto a los tiempos de atención, es necesario que ARCOTEL revise la fuente y el criterio técnico utilizado para establecer los tiempos establecidos en el Artículo 23, letras a) y b); y que, en su lugar, considere los tiempos establecidos en la Guía de Seguridad de las TIC CCN-STIC 817, la misma que fue establecida dentro del marco de seguridad de la red y de datos personales de la Unión Europe. Así mismo, bajo este mismo criterio, consideramos que los incidentes medios, bajos y altos, deberían cerrarse automáticamente transcurrido un tiempo determinado (60 días); mientras que los incidentes muy altos y críticos, necesariamente deberían ser reportados a EcuCERT, pero en un marco de colaboración, en ningún caso como "obligación" sujeto a posibles sanciones.

Es necesario recalcar nuevamente la importancia que tiene el establecimiento de un CERT nacional (EcuCERT), cuya principal función a criterio de OTECEL, S.A:, tiene que ver con la verificación de que los PST dispongan de Políticas de Seguridad; y, en caso que no las cumplan o no las dispongan, intervenir con la emisión de guías que permitan adoptar políticas mínimas de seguridad (tal como lo realizan en España y Colombia); y, en este caso, con disposiciones de cumplimiento obligatorio, conforme lo contempla la LOT.

La importancia del EcuCERT tiene mayor relevancia en caso de ataques que tengan alcances nacionales, regionales o globales, ya que la coordinación que realice con los diferentes actores será fundamental para evitar daños mayores. Para ello, consideramos que el carácter colaborativo, tal como se lo ha realizado con los casos de fraude y bypass, es la herramienta adecuada, ya que permite la canalización de recursos en esta dirección, y, no como ocurriría con el desvío de fondos para cumplir con obligaciones que no aportan para la seguridad de la red, pero de esta manera se evitaría incurrir en sanciones.

2. PRIORIZACIÓN

En los artículos 9 y 10 del Proyecto de Norma, se establece que ARCOTEL realizará la asignación de prioridades, en función de los datos estadísticos existentes.

A fin de realizar una clasificación adecuada, consideramos que se debe utilizar estándares que tomen en cuenta factores como el vector de ataque, la complejidad, los privilegios que se requieren en el elemento bajo amenaza, etc. Por ejemplo: CVVS (Common Vulnerability Score System) que es estándar abierto y utilizan puntuaciones estandarizadas en métricas de

explotabilidad e impacto, y es de común uso por National Vulnerability Database (NVDB), Common Vulnerabilities and Exposures (CVE) u Open Source Vulnerability Database (OSVDB).

https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

Respecto a los incidentes, se debe considerar si existe afectación significativa a los usuarios, de tal forma que la clasificación se realice dependiendo de la duración del incidente y de la cantidad de usuarios afectados.

3. INFORMACIÓN CONFIDENCIAL y RESPALDO

El Proyecto de Norma, en los artículos 9, 13 y 14, establece un protocolo sobre la forma en que se clasificaría la información que se cursaría entre el EcuCERT y Telefónica, y, en el Anexo 1 los mecanismos de protección de la misma.

El contrato de Concesión y la LOT obligan a OTECEL, S.A. a dar el tratamiento adecuado a la información confidencial, razón por la cual consideramos innecesario, excesivo y poco transparente, establecer como obligación mecanismos específicos para tratar la información confidencial. Solamente en caso que algún PST no cumpla con mantener confidencial la información, se podría aplicar los mecanismos señalados.

Respecto al respaldo de la información, es suficiente con que se indique el tiempo máximo que se conservará la información; todo lo demás es excesivo e innecesario. Igualmente, debe permitirse que los respaldos de información relacionados con los incidentes se puedan almacenar de forma digital.

4. DIFUSIÓN

El artículo 79 de la LOT establece que en caso de que exista un riesgo particular de violación de la seguridad de la red pública o del servicio de telecomunicaciones, el PST informará a sus abonados, clientes y usuarios sobre dicho riesgo y sobre las medidas a adoptar.

Considerando la clasificación que se realice tanto a las vulnerabilidades como a los incidentes de seguridad, se deberían establecer tiempos y mecanismos diferentes para informar a los usuarios. Los casos clasificados como Bajo y Medio, no deberían ser informados por su bajo impacto, mientras que los restantes casos se podrían informar en plazos razonables de hasta quince (15) días. De cualquier forma, se considera que debe realizarse siempre en un marco colaborativo; y, solo en casos de incumplimiento, intervenir con disposiciones de carácter vinculante.

En relación con el numeral 3 del Artículo 31, consideramos que no es obligación de los PST adoptar acciones para la solución o mitigación de vulnerabilidades e incidentes cuando los usuarios no han realizado los cambios que correspondían, ya que esto se encuentra fuera de nuestro alcance (e.g., es imposible que nuestros técnicos ingresen a las instalaciones del usuario y realice cambios en las claves de acceso de los routers). Esta disposición consideramos que está en contra de lo dispuesto en el artículo 22, numerales 1 y 2, y artículo 25, numeral 2, de la LOT; mismos que se transcriben a continuación:

> *"Artículo 22.- Derechos de los abonados, clientes y usuarios.*
> *Los abonados, clientes y usuarios de servicios de telecomunicaciones tendrán derecho:*
>
> *1. A disponer y recibir los servicios de telecomunicaciones contratados de forma continua, regular, eficiente, con calidad y eficacia.*

2. A escoger con libertad al prestador del servicio, el plan de servicio, así como a la modalidad de contratación y el equipo terminal en el que recibirá los servicios contratados.

Artículo 25.- Derechos de los prestadores de servicios de telecomunicaciones. Son derechos de los prestadores de servicios de telecomunicaciones, con independencia del título habilitante del cual se derive tal carácter, los siguientes:

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." (Cursivas nuestras).

Adicionalmente, se sugiere que ARCOTEL disponga de una BDD en la que se registren los casos en que el PST comunicó las vulnerabilidades al usuario, de tal forma que no se repitan en la siguiente revisión que realice EcuCERT, esto, independientemente de que se establezca el intercambio en un marco colaborativo.

5. SEGURIDAD DE LAS REDES

En relación con las auditorías que establece el artículo 85 de la LOT, al ser auditorías internas, tienen el carácter de confidencial, que tienen acceso restringido dentro de la empresa, por lo crítico que puede resultar la filtración de los resultados de la misma. Razón por la cual, consideramos que el informe no debe remitirse a ARCOTEL, y que, los resultados pueden revisarlos en las mismas instalaciones de Telefónica.

En esta misma línea, es importante mencionar que las vulnerabilidades a las que se refiera la Norma Técnica, deben ser únicamente de carácter externo; es decir las vulnerabilidades internas y los equipos que puedan ser calificados como críticos, producto de las auditorías que se realicen, en ningún caso pueden salir de la operadora, ya que el riesgo de afectación a la seguridad de la red y de los datos personales puede ser extremadamente alto. Se debe incluir en la norma técnica que para la revisión de los informes de auditoría, por su criticidad, los funcionarios de ARCOTEL se someterán a las normas y políticas de seguridad que disponga cada prestador del servicio.

Finalmente, respecto al artículo 33 relacionado con las auditorías parece excesivo realizar una auditoría anual que, además de ser innecesaria si se adoptan en la primera vez las medidas correctivas, representa un costo y esfuerzo operativo totalmente innecesario.

Atentamente,

Hernán Ordóñez
VICEPRESIDENTE DE REGULACIÓN Y ESTRATEGIA

OBSERVACIONES A LA NORMA TÉCNICA

Art.	Descripción	Observación
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 acecuadas para preservar la seguridad de sus servicios y la invulnerabilidad de la red y garantizar, con un nivel de seguridad adecuado al riesgo existente, el secreto de las comunicaciones y de la información transmitida por sus redes	La verificación de que los PST hayan establecido políticas de seguridad debería ser el objeto de la Norma Técnica. En caso de no hacerlo, se deberían establecer las medidas que deberían adoptar los PST.
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 del régimen general 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, clientes o usuarios de los servicios del régimen general 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.	-
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	-
	20. 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.	Adoptar la definición establecida por la UIT en la Recomendación X.800: "Vulnerabilidad es toda debilidad que pueda explotarse para violar un sistema o la información que éste contiene"
	9. Incidente.- Es la ocurrencia de uno o varios eventos de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones y amenazar 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 del régimen general de telecomunicaciones	Un incidente de seguridad se produce una vez que se ha producido el acceso; por lo que se requiere suprimir "intento de acceso".
	TÍTULO II CONSIDERACIONES TÉCNICAS	
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	Debería modificarse en función del cambio del Artículo 1.
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. 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.	Debería modificarse en función del cambio del Artículo 1.
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.	Debería modificarse en función del cambio del Artículo 1. Se debe considerar que los procedimientos de gestión de Vulnerabilidades y de Incidentes, son solo una parte de todas las políticas de seguridad que deben establecerse. Por lo que, al establecer estos procedimientos, y, si no existe una política de seguridad integral, no se estaría dando una real seguridad a la red y a los datos personales de los usuarios.
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 vulnerabilidades e incidentes detectados en su red; con la finalidad de cumplir de manera obligatoria con los plazos de atención de incidentes o vulnerabilidades establecidas en esta norma.	En caso que no se dispongan políticas de seguridad, la gestión de incidentes y vulnerabilidades sería solo una de las tantas medidas que deberían adoptar los prestadores de servicios de telecomunicaciones
	TÍTULO III NOTIFICACIONES	
	CAPÍTULO I GENERACIÓN DE NOTIFICACIONES	
8.- 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 del régimen general de telecomunicaciones, sobre vulnerabilidades e incidentes presentes en la red del prestador o de sus abonados o clientes. Este reporte se realiza a través de un sistema de gestión de vulnerabilidades e incidentes. 2. Notificaciones de los prestadores de servicios del régimen general 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) del régimen general de telecomunicaciones involucrados para que procedan con la atención correspondiente 3. Notificaciones dirigidas a la ARCOTEL y que son generadas por abonados, clientes o usuarios, sobre incidentes de seguridad relacionados con las redes y servicios de los prestadores de servicios del régimen general de telecomunicaciones, conforme el ámbito de la presente Norma. Se realiza a la ARCOTEL a través del formulario de la página web, correo electrónico, comunicación escrita, o vía telefónica. Posterior a la notificación realizada por las personas naturales o jurídicas, la ARCOTEL comunicará al (los) prestador (es) de servicios del régimen general de telecomunicaciones correspondientes para que procedan con la atención debida. La información de los medios disponibles para la notificación de incidentes o vulnerabilidades de seguridad, por parte de los abonados, clientes o usuarios, estará disponible en la página web de la ARCOTEL, así mismo los prestadores de servicios del régimen general de telecomunicaciones deberán informar a su abonados/clientes acerca de los medios disponibles para que realicen dichas notificaciones.	Las notificaciones de vulnerabilidades e incidentes debería realizarse en un marco colaborativo, a través de acuerdos bilaterales. Esto principalmente debido a que las políticas de seguridad para tratar vulnerabilidades e incidentes, puede variar dependiendo del prestador de servicios de telecommunicaciones, los servicios que presta y las redes implementadas.
9.- Clasificación y Priorización	Todas las notificaciones y reportes así como la información contenida en las mismas, que se intercambien entre la ARCOTEL y los prestadores de servicios del régimen general de telecomunicaciones, ya sea a través del sistema de gestión de incidentes y vulnerabilidades así como por otros medios, relacionadas con la gestión de incidentes y vulnerabilidades, deberán ser clasificadas siguiendo los siguientes criterios:	Las prioridades deberían ser clasificadas por los operadores, siempre dentro de un marco colaborativo, a menos que el PST no disponga de políticas de seguridad. Adicionalmente, a fin de realizar una clasificación adecuada, consideramos que se debe utilizar estándares que tomen en cuenta factores como el vector de ataque, la complejidad, los privilegios que se requieren en el elemento bajo amenza, etc. Por ejemplo, CVVS (Common Vulnerability Score System) que es estándar abierto y utilizan puntuaciones estandarizadas en métricas de explotabilidad e impacto, y es de común uso por National Vulnerability Database (NVDB), Common Vulnerabilities and Exposures (CVE) u Open Source Vulnerability Database (OSVDB).
	1. Criterio de 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 10 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 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	

Art	Descripción	Observación
	OBSERVACIONES A LA NORMA TÉCNICA	
	2 Criterio de confidencialidad: Para la determinación del criterio de confidencialidad 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 Título XV Secreto de la Comunicación y Protección de Datos Se utilizará el protocolo TLP, según el cual quien remite la información debe clasificarla de acuerdo a uno de los siguientes criterios de confidencialidad: Pública General, Pública Comunitaria, Sensible y Confidencial, con base al detalle que se describe a continuación:	El proyecto de Norma, en los artículos 9, 13 y 14, establece un protocolo sobre la forma en que se va a clasificar la información que se cursará entre el EcuCERT y Telefónica y, en el Anexo 1 los mecanismos de protección de la misma El contrato de Concesión y la LOT obligan a Telefónica a dar el tratamiento adecuado a la información confidencial, razón por la cual consideramos innecesario, excesivo y poco transparente, establecer como obligación mecanismos específicos para tratar la información confidencial. Solamente en caso que algún PST no cumpla con mantener
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 cualquier otro medio valido 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.	las prioridades deberían ser clasificadas por los operadores, siempre dentro de un marco colaborativo, a menos que el PST no disponga de políticas de seguridad. Adicionalmente, a fin de realizar una clasificación adecuada, consideramos que se debe utilizar estándares que tomen en cuenta factores como el vector de ataque, la complejidad, los privilegios que se requieren en el elemento bajo amenza, etc. Por ejemplo: CVVS (Common Vulnerability Score System) que es estándar abierto y utilizan puntuaciones estandarizadas en metricas de explotabilidad e impacto, y es de comun uso por National Vulnerability Database (NVDB), Common Vulnerabilities and Exposures (CVE) u Open Source Vulnerability Database (OSVDB)
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	
12.- Asignación de Niveles de Prioridad a nuevos Incidentes o Vulnerabilidades	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	
	TÍTULO V: RESPALDO Y CONSERVACIÓN DE LA INFORMACIÓN	El contrato de Concesión y la LOT obligan a Telefónica a dar el tratamiento adecuado a la información confidencial, razón por la cual consideramos innecesario, excesivo y poco transparente, establecer como obligación mecanismos específicos para tratar la información confidencial. Solamente en caso que algún PST no cumpla con mantener confidencial la información, se podría aplicar los mecanismos señalados Respecto al respaldo de la información, es suficiente con que se indique el tiempo maximo que se conservará la información, todo lo demás es excesivo e innecesario. Se debería establecer como obligación en caso que dentro de las politicas de los PST no se disponga de procedimientos para tratar la información confidencial. Se trata de regular el QUÉ no el CÓMO
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 utilizaran 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; es obligación del prestador el mantener adicionalmente la evidencia documentada, con los respaldos correspondientes de	
18.- Conservación	Toda información referente a la gestión de vulnerabilidades e incidentes, ya sea notificada por la ARCOTEL, o los casos detectados por los prestadores de servicios del régimen general de telecomunicaciones, será conservada por éstos últimos de acuerdo al siguiente detalle: 1. Información clasificada como Pública General o Pública Comunitaria durante un (1) año; 2 Información sensible: durante tres (3) años; 3 Información Confidencial: durante cinco (5) años.	
	TÍTULO VI: DIFUSIÓN DE INFORMACIÓN	El artículo 79 de la LOT efectivamente establece que en caso de que exista un riesgo particular de violación de la seguridad de la red pública o del servicio de telecomunicaciones, el PST informará a sus abonados, clientes y usuarios sobre dicho riesgo y sobre las medidas a adoptar. Considerando la clasificación que se realice tanto a las vulnerabilidades como a los incidentes de seguridad, se debería establecer tiempos y mecanismos diferentes para informar a los usuarios. Los casos clasificados como Bajo y Medio, podrían incluso no deberían ser informados por su bajo impacto, mientras que los restantes se podría informar en plazos razonables de hasta 15 días. De cualquier forma, se considera que debe realizarse siempre en un marco colaborativo; y, solo en casos de incumplimiento, intervenir con disposiciones de carácter vinculante
19.- Obligación de Información	En caso de presentarse el riesgo particular de violación de la red pública o de un servicio de telecomunicaciones, el o los prestadores de servicios del régimen general de telecomunicaciones deberán informar de manera inmediata a sus abonados, clientes o usuarios sobre dicho riesgo y las medidas que adoptará para atenuar o eliminar el riesgo, así como, de ser el caso, las medidas que debe adoptar el abonado, cliente o usuario. Esta información podrá ser enviada de manera general o en particular a determinados abonados clientes o usuarios, de acuerdo al ámbito de afectación. En caso de violación de los datos de un abonado, cliente o usuario particular, el prestador notificará de tal violación a dicho abonado, cliente o usuario 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. El prestador de servicios del régimen general de telecomunicaciones deberá mantener un registro de las comunicaciones realizadas. La ARCOTEL podrá además 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 del (los) prestador (es) de servicios del régimen general 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 DEL RÉGIMEN GENERAL DE TELECOMUNICACIONES	Respecto a la regulación para GESTIONAR las vulnerabilidades e incidentes de seguridad, que reporta un CERT nacional, de la revisión realizada, en ningún caso se ha podido encontrar alguna norma que establezca como obligación un tiempo maximo de respuesta ante incidentes de seguridad y vulnerabilidades, y, peor aún que establezca todo un sistema de atención a través de tickets de las vulnerabilidades e incidentes de red, reportados por un CERT de alcance nacional De la revisión realizada se ha determinado que en España si disponen de las herramientas para gestionar
20.- Sistema de Gestión de Comprobantes	La ARCOTEL para cada vulnerabilidad o incidente receptado, generará una notificación dirigida a quién remitió la información, así como al prestador de servicios del régimen general de telecomunicaciones que debe gestionar la vulnerabilidad o incidente. El objetivo es confirmar la recepción de lo informado, el inicio de las acciones para su atención, y dar a conocer el número asignado al caso (número de ticket o comprobante), para facilitar su seguimiento. 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 del régimen general de telecomunicaciones contendrán al menos la siguiente información:	

Observaciones a la Norma Técnica

Art.	Descripción	Observación
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 vulnerabilidades e incidentes de seguridad de la información que le sean notificadas por la ARCOTEL o que hayan sido detectadas por el	referenciales: "Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información"; y, "Guía de Seguridad de las TIC CCN-STIC 817", respectivamente. Las dos guías se refieren a tiempos "recomendados" para tratar únicamente incidentes de seguridad, en ningún caso para gestionar vulnerabilidades y menos como obligación. En relación a los incidentes de seguridad, revisando la Guía española, una vez notificado el incidente al organismo afectado por parte del CCN-CERT, se realizará un seguimiento del mismo, dependiendo de la peligrosidad del incidente. En el cuadro que se muestra a continuación, se observa que para los "incidentes" no hay obligación de realizar ningún reporte para los casos bajo y medio; mientras que para los casos Alto a Crítico, los tiempos de respuesta varían de 45 días para un nivel alto, hasta 120 días para un nivel crítico.
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 [illegible] a la vulnerabilidad, se deberán cumplir los siguientes tiempos: b) Para Incidentes.- Frente a cada notificación enviada por la ARCOTEL al prestador de servicios del régimen general de telecomunicaciones y considerando la prioridad asignada al incidente, se deberán cumplir los siguientes tiempos:	Acerca de las vulnerabilidades, es importante mencionar que la ITU en la serie de Recomendaciones X ha establecido arquitecturas multidimensionales en la que se definen las diferentes capas y planos en cada uno de los cuales existen procesos de seguridad y protección de la Red, los mismos que son complejos por gran parte de los operadores de redes. Este sistema permite que cualquier vulnerabilidad dependiendo de su explotabilidad, implique riesgos mínimos para el operador por gracias a su la arquitectura multidimensional, es por ello que en muchas ocasiones estas vulnerabilidades no afectan a los operadores incluso cuando estan abiertas mucho tiempo. Revisemos la definición de la vulnerabilidad de la Recomendación UIT-T X.800 y la que consta en la Norma Técnica. ITU: "Vulnerabilidad es toda debilidad que pudiera explotarse para violar un sistema o las informaciones que éste contiene" Proyecto de Norma Técnica: "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" Estas definiciones tienen una diferencia fundamental, y es el hecho de que la ITU determina la posibilidad de una violación del sistema, mientras que la para la definición del proyecto de Norma, el hecho de exista la vulnerabilidad de hecho ya permite atentar contra la "confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones". La realidad no es así, ya que el hecho a pesar de que existea una vulnerabilidad, es muy baja la probabilidad de que se puedan superar todas las seguridades disponibles, y de esta manera afectar realmente la seguridad de la red y los datos personales de los usuarios, no necesariamente implica que exista el riesgo de que se afecte la seguridad de la red o se este en riesgo la seguridad de las BDD de usuarios
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 [illegible] 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 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 reporte.	
24.- Gestión de vulnerabilidades e incidentes que involucren a la comunidad objetivo de la ARCOTEL	II. GESTIÓN DE NOTIFICACIONES DE PERSONAS NATURALES O JURÍDICAS Las notificaciones originadas en información generada por personas naturales o jurídicas, organismos nacionales o internacionales, en relación con el 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 del régimen general de telecomunicaciones que correspondan, para su gestión.	
25.- Reporte del estado de gestión a la ARCOTEL	III. REPORTE DE GESTIÓN POR PARTE DE PRESTADORES DE SERVICIOS DEL RÉGIMEN GENERAL DE TELECOMUNICACIONES 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 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 FO- CCDR-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	Las mismas observaciones realizadas al Título VII, Capítulo I, Artículos 20 al 23.
26.- Reporte de vulnerabilidades o incidentes detectados y solucionados por el prestador de servicios del régimen general de	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 incidente@ecucert.gob.ec, para su registro.	Las mismas observaciones realizadas al Título VII, Capítulo I, Artículos 20 al 23
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 la presente Norma, y remitirla en caso de que la ARCOTEL lo solicite. En términos de atención de los incidentes y vulnerabilidades deben estar de acuerdo a lo que consta en el artículo 22 de la presente Norma.	Las mismas observaciones realizadas al Título VII, Capítulo I, Artículos 20 al 23.

Art.	Observación	Observación
29.- Notificación de incidentes que pertenezcan a un proveedor de servicios de telecomunicaciones diferente o cuya fuente de origen no se encuentre dentro del	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 de 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	
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 del régimen general de telecomunicaciones en su red, o en la de sus clientes, abonados o usuarios, y que no puedan ser solucionados, podrán solicitar apoyo técnico a la ARCOTEL remitiendo el Formato FO- CCDR-06, publicado por la ARCOTEL. Se dispondrán los mismos tiempos para la respuesta y gestión que han sido definidos en el artículo 22, letra b) de la presente Norma Técnica	
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 régimen general de telecomunicaciones involucrados	Los formularios deberían ser aprobados conjuntamente con la Norma Técnica
	CAPÍTULO VI. DERECHOS Y OBLIGACIONES DE LOS PRESTADORES DE SERVICIOS DEL RÉGIMEN GENERAL	**UNICACIONES**
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: 1. Cumplir con los tiempos de gestión y reporte, establecidos en la presente Norma 2. Entregar la información en los formularios que para el efecto publique la ARCOTEL. 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. 4. 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, clientes y usuarios sobre dicho riesgo y sobre las medidas a adoptar. Si como resultado del evento se determine la ocurrencia de violación de los datos de un abonado, cliente o usuario particular, el prestador de servicios deberá comunicar al abonado o cliente de manera inmediata describiendo al menos la naturaleza	Las notificaciones de vulnerabilidades e incidentes debería realizarse en un marco colaborativo, tal como se lo ha realizado con los casos de fraude y bypass, consideramos que es la herramienta adecuada, ya que permite la canalización de recursos en esta dirección, y, no como ocurriría con el desvío de fondos para cumplir con obligaciones que no aportan para la seguridad de la red, pero de esta manera se evitaría incurrir en sanciones En relación con el numeral 3 del Artículo 31, consideramos que no es obligación de los PST adoptar acciones para la solución o mitigación de vulnerabilidades e incidentes cuando los usuarios no han realizado los cambios que correspondían, ya que esto se encuentra fuera de nuestro alcance, ya que, por ejemplo, es imposible que nuestros técnicos ingresen a las instalaciones del usuario y realice cambios en las claves de acceso de los routers. Esta disposiciones, consideramos que está en contra de lo dispuesto en el artículo 22, numerales 1 y 2; y, artículo 25, numeral 2, de la Ley Orgánica de Telecomunicaciones, los mismos que transcribo a continuación: Artículo 22 - Derechos de los abonados, clientes y usuarios Los abonados, clientes y usuarios de servicios de telecomunicaciones tendrán derecho: 1. A disponer y recibir los servicios de telecomunicaciones contratados de forma continua, regular, eficiente, con calidad y eficacia 2. A escoger con libertad al prestador del servicio, el plan de servicio, así como a la modalidad de contratación y el equipo terminal en el que recibirá los servicios contratados. Artículo 25.- Derechos de los prestadores de servicios de telecomunicaciones. Son derechos de los prestadores de servicios de telecomunicaciones, con independencia del título habilitante del cual se derive tal carácter, los siguientes: 2. Suspender el servicio provisto por falta de pago de los abonados o clientes o uso ilegal del servicio calificado por
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 contemplados en el artículo 58 de la Ley Orgánica de 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.	
	CAPÍTULO VII. SEGURIDAD DE REDES Y SERVICIOS	
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, 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 en 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 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.	En relación con las auditorías que establece el artículo 95 de la LOT, al ser auditorías internas, tienen el carácter de confidencial, que tienen acceso restringido dentro de la empresa, por lo crítico que puede resultar la filtración de los resultados de la misma. Razón por la cual, consideramos que el informe no debe remitirse a ARCOTEL, y que, los resultados pueden revisarlos en las mismas instalaciones de Telefónica En esta misma línea, es importante mencionar que las vulnerabilidades a las que se refiera la Norma Técnica, deben ser únicamente de carácter externo; es decir las vulnerabilidades internas y los equipos que puedan ser calificados como críticos, producto de las auditorías que se realicen, en ningún caso pueden salir de la operadora, ya que el riesgo de afectación a la seguridad de la red y de los datos personales puede ser extremadamente alto. Se debe incluir en la norma técnica, que para la revisión de los informes de auditoría, por su criticidad, los funcionarios de ARCOTEL se someterán a las normas y políticas de seguridad que disponga cada prestador del servicio

Art.	Descripción	Observación
	OBSERVACIONES A LA NORMA TÉCNICA	
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) 3. Vulnerabilidades detectadas 4. Historial de incidentes propios (ocurridas en el mencionado equipo)	
35.- Acciones para la identificación de ataques o eventos de seguridad de redes	La ARCOTEL, a fin de 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 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 del régimen general 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.	
	TITULO X CONTACTOS Y NOTIFICACIONES	
36.- Encargados de Seguridad	Para la coordinación de las acciones contempladas en la presente Norma Técnica, es obligación de los prestadores de servicios del régimen general de telecomunicaciones, que previa solicitud de ARCOTEL, procedan a designar al menos un funcionario, 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 y Acuerdo de Confidencialidad 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 de 24 horas contadas.	
	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 plazo no mayor a treinta (30) días hábiles 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	
SEGUNDA	La información de contacto, direcciones de correo electrónico, accesos a la plataforma de gestión de incidentes, 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 para la gestión de incidentes.	
	DISPOSICIONES TRANSITORIAS	
PRIMERA	En un plazo máximo de 30 días hábiles, desde la publicación de la presente Norma Técnica en el Registro Oficial, la ARCOTEL notificará por escrito a los prestadores de servicios del régimen general de telecomunicaciones, que inicialmente y en un plazo máximo de 60 días calendario contados a partir de la notificación, deberán proporcionar a la ARCOTEL, información técnica de los controles, procedimientos, mecanismos y políticas de seguridad implementados para mantener la integridad de sus servicios y redes de acuerdo a lo establecido en el numeral 1 del artículo 85 de la Ley Orgánica de Telecomunicaciones, y artículo 6 de la presente Norma	
SEGUNDA	En un plazo de treinta (30) días hábiles, a partir de la publicación de la presente Norma técnica en el Registro Oficial, la ARCOTEL notificará por escrito a los prestadores de servicios del régimen general de telecomunicaciones que en un inicio deben remitir la información del (los) encargado (s) de seguridad designados de acuerdo a lo indicado en el artículo 36 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 plazo de cuarenta y cinco (45) días hábiles, a partir de la publicación de la presente Norma Técnica en el Registro Oficial, la ARCOTEL realizara la publicación y notificación del listado inicial de prioridades asignadas a los incidentes y vulnerabilidades conocidos, de acuerdo al procedimiento indicado en el artículo 10 de la presente Norma	
CUARTA	La ARCOTEL publicará en su página WEB, en un plazo máximo de treinta (30) días hábiles, los formatos actualizados FO-CCDR-01, FO-CCDR-02, FO-CCDR-03, FO-CCDR-04, FO-CCDR-05 y FO- CCDR-06, mencionados en la presente Norma, así como las respectivas instructivas de llenado.	