PROYECTO DE RESOLUCIÓN	OBSERVACIONES, COMENTARIOS, SUGERENCIAS DE USUARIOS DIGITALES	PROPUESTA DE REFORMA DE USUARIOS DIGITALES
PROBLEMATICA	**La norma incluye solo a infraestructura de telecomunicaciones, pero de acuerdo a nuestro monitoreo de información pública, detectamos que la mayor cantidad de vulneraciones se realizan en redes internacionales y servicios intermediario (OTT) que de alguna manera deberían ser contemplados en la norma para que Arcotel trabej también con ellos como actores de información y datos personales**	
OBSERVACIONES GENERALES	[observaciones, comentarios, notas]	[propuesta de reforma]
CONSIDERANDOS	[observaciones, comentarios, notas]	[propuesta de reforma]
EXPEDIR LA “NORMA TÉCNICA PARA COORDINAR LA GESTIÓN DE INCIDENTES Y VULNERABILIDADES QUE AFECTEN A LA SEGURIDAD DE LAS REDES Y SERVICIOS DE TELECOMUNICACIONES”	[observaciones, comentarios, notas]	[propuesta de reforma]
TÍTULO I ASPECTOS GENERALES	[observaciones, comentarios, notas]	[propuesta de reforma]
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 garantizar, con un nivel de seguridad adecuado al riesgo existente, el secreto de las comunicaciones y de la información transmitida por sus redes.	[observaciones, comentarios, notas]	[propuesta de reforma]
Artículo 2.- Ámbito.- La aplicación de esta Norma abarca a todas las personas naturales o jurídicas de derecho público o privado que sean prestadores de servicios 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.	[observaciones, comentarios, notas]	[propuesta de reforma]
Artículo 3.- Definiciones.- Los términos empleados en esta Norma Técnica y no definidos, tendrán el significado establecido en la Ley Orgánica de Telecomunicaciones, en el Reglamento General a la Ley Orgánica de Telecomunicaciones, los adoptados por la Unión Internacional de Telecomunicaciones (UIT), por los convenios y tratados internacionales ratificados por la República del Ecuador; y, en las regulaciones respectivas emitidas por la ARCOTEL.	[observaciones, comentarios, notas]	[propuesta de reforma]
Para efectos de la presente Norma, se aplicarán las siguientes definiciones: 1. Acuerdo de Confidencialidad y No divulgación.- Convenio suscrito entre dos o más partes mediante el cual las mismas se comprometen a no divulgar la información intercambiada en la gestión de incidentes y vulnerabilidades.	[observaciones, comentarios, notas]	[propuesta de reforma]
2. Anonimizar la Información.- Expresar un dato relativo a entidades o personas, eliminando la referencia a su identidad, con lo cual se disocian los datos que permitan la identificación de la identidad del propietario de la información o su relación con una vulnerabilidad o incidente de seguridad.	"disocian" deberia ser cambiado por "reservan", ya que el alcance de la disociación implicaría la renuncia a la información anonimizada	Anonimizar la información.- Expresar un dato relativo a entidades o personas, eliminando la referencia a su identidad, con lo cual se reservan los datos que permitan la identificación de la identidad del propietario de la información o su relación con una vulnerabilidad o incidente de seguridad.
3. ARCOTEL.- Agencia de Regulación y Control de las Telecomunicaciones	[observaciones, comentarios, notas]	[propuesta de reforma]

PROYECTO DE RESOLUCIÓN	OBSERVACIONES, COMENTARIOS, SUGERENCIAS DE USUARIOS DIGITALES	PROPUESTA DE REFORMA DE USUARIOS DIGITALES
4. Centro de Respuesta a Incidentes Informáticos (CRII) de la ARCOTEL.- Grupo de trabajo o unidad de la ARCOTEL que, conforme el Estatuto Orgánico de Gestión Organizacional por procesos institucional, tiene a su cargo el cumplimiento de las obligaciones, actividades y responsabilidades derivadas de la aplicación de la presente Norma en lo relacionado a la ARCOTEL. En general las referencias que se realicen a la ARCOTEL en la presente Norma, se entenderá que corresponden a las actividades y gestión que realizará el CRII, salvo donde se exprese lo contrario.	[observaciones, comentarios, notas]	[propuesta de reforma]
5. Comunidad Objetivo.- La Comunidad Objetivo es aquel grupo de personas naturales o jurídicas de derecho público o privado, sistemas u organismos partícipes de la coordinación y gestión de vulnerabilidades que afecten la seguridad de las redes y servicios de telecomunicaciones. Para fines de aplicación de la presente Norma Técnica, la Comunidad Objetivo de la ARCOTEL estará constituida por prestadores de servicios del régimen general de telecomunicaciones y abonados, clientes y usuarios de las redes públicas de telecomunicaciones.	[observaciones, comentarios, notas]	[propuesta de reforma]
6. Fuentes de Información.- Son personas naturales o jurídicas, nacionales o extranjeras u organismos internacionales que almacenan y administran información respecto a vulnerabilidades o incidentes de seguridad de la información y que reportan periódicamente a la ARCOTEL los eventos relacionados con los Números de Sistemas Autónomos (ASN) del país.	"y que reportan periódicamente", debería ser eliminado del texto por excluir a aquellas fuentes ocasionales que pudieran brindar infromación sin que se reporten específicamente a Arcotel	Fuentes de información.- Son personas naturales o jurídicas, nacionales o extranjeras u organismos internacionales que almacenan y administran información respecto a vulnerabilidades o incidentes de seguridad de la información sobre los eventos relacionados con los Números de Sistemas Autónomos (ASN) del país.
7. Hash.- Es una función criptográfica, que por medio de la aplicación de un algoritmo matemático transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud.	[observaciones, comentarios, notas]	[propuesta de reforma]
8. Evento de seguridad de la información (evento).- Un evento de seguridad de la información es la ocurrencia identificada de un estado de un sistema, servicio o red, que muestra una posible brecha de política de seguridad de la información o falla de protecciones, o una situación previa desconocida que puede ser relevante para la seguridad.	[observaciones, comentarios, notas]	[propuesta de reforma]
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 amenazan la seguridad de la información de la comunidad objetivo. Se define además, como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la Política de Seguridad de la Información, del prestador de servicios del régimen general de telecomunicaciones.	[observaciones, comentarios, notas]	[propuesta de reforma]
10. Encargados de Seguridad.- Son servidores públicos de la ARCOTEL y personal de las empresas prestadoras de servicios del régimen general de telecomunicaciones, designados como responsables de coordinar la gestión de incidentes y vulnerabilidades, así como de planificar, desarrollar, controlar y gestionar la aplicación de políticas, procedimientos y acciones, con la finalidad de mejorar la seguridad de los servicios y redes de telecomunicaciones, así como la seguridad de la información transmitida y la invulnerabilidad de la red, conforme lo establecido en la presente Norma.	Entre las actividades de los Encargados de Seguridad, debería incluirse establecer un plan de análisis de riesgo institucional.	10. Encargados de Seguridad.- Son servidores públicos de la ARCOTEL y personal de las empresas prestadoras de servicios del régimen general de telecomunicaciones, designados como responsables de coordinar la gestión de incidentes y vulnerabilidades, así como de planificar, desarrollar, controlar y gestionar la aplicación de políticas, establecer un plan de análisis de riesgo, procedimientos y acciones, con la finalidad de mejorar la seguridad de los servicios y redes de telecomunicaciones, así como la seguridad de la información transmitida y la invulnerabilidad de la red, conforme lo establecido en la presente Norma.

PROYECTO DE RESOLUCIÓN	OBSERVACIONES, COMENTARIOS, SUGERENCIAS DE USUARIOS DIGITALES	PROPUESTA DE REFORMA DE USUARIOS DIGITALES
11. Notificaciones.- Son las comunicaciones de vulnerabilidades o incidentes de seguridad de las redes o servicios de telecomunicaciones, que remite la ARCOTEL a los prestadores de servicios del régimen general de telecomunicaciones, que requieren acciones técnicas para solución o mitigación. Las notificaciones se originan en la ARCOTEL, prestadores de servicios del régimen general de telecomunicaciones, y personas naturales o jurídicas, conforme el ámbito de la presente Norma.	Las notificaciones por parte del usuario deben deberían poder reportar de forma anónima, sin solicitar datos personales como lo hace en la actualidad	Notificaciones.- Son las comunicaciones de vulnerabilidades o incidentes de seguridad de las redes o servicios de telecomunicaciones, que remite la ARCOTEL a los prestadores de servicios del régimen general de telecomunicaciones, que requieren acciones técnicas para solución o mitigación. Las notificaciones se originan en la ARCOTEL, prestadores de servicios del régimen general de telecomunicaciones, y personas naturales o jurídicas, de forma identificable o anónima, conforme el ámbito de la presente Norma.
12. Números de Sistemas Autónomos (ASN – Autonomous System Numbers).- Son números únicos a nivel mundial que se asignan a los sistemas autónomos, y es una parte importante de la arquitectura de enrutamiento de Internet. Los números de sistema autónomo se toman de un campo de números de 16 bits, que en la actualidad se ha extendido a 32 bits.	[observaciones, comentarios, notas]	[propuesta de reforma]
13. PGP / GPG (Pretty Good Privacy / GNU Privacy Guard - GnuPG).- Privacidad Bastante Buena, son aplicaciones cuya finalidad es proteger la información distribuida a través del internet mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos gracias a firmas digitales para tal fin. En el RFC4880 se define el estándar OpenPGP, el mismo que ha sido implementado con el nombre de GNUPG.	[observaciones, comentarios, notas]	[propuesta de reforma]
14. Política.- Intenciones y dirección de una organización, como las expresa formalmente su alta dirección.	[observaciones, comentarios, notas]	[propuesta de reforma]
15. Política de Seguridad.- Conjunto de reglas establecidas por la autoridad de seguridad que rigen la utilización y prestación de servicios y facilidades de seguridad	Los procesos es necesario también tomarlo en cuenta	Política de Seguridad.- Conjunto de reglas y procesos establecidas por la autoridad de seguridad que rigen la utilización y prestación de servicios y facilidades de seguridad
16. Redes de Confianza.- Es una agrupación de organismos, dentro de los cuales forma parte el Centro de Respuesta a Incidentes Informáticos de la ARCOTEL, que colaboran entre sí en la gestión de vulnerabilidades e incidentes de seguridad informática a través del intercambio de información exclusivamente entre sus miembros.	La afectación de las telecomunicación tiene que ver, además de las empresas de infraestructura de telecomunicaciones y de autoridades de control del gobierno, con actores que van desde organismos internacionales hasta agrupaciones de usuarios finales	Redes de Confianza.- Es una agrupación de actores del ecosistema de telecomunicaciones según estándares de gobernanza, dentro de los cuales forma parte el Centro de Respuesta a Incidentes Informáticos de la ARCOTEL, que colaboran entre sí en la gestión de vulnerabilidades e incidentes de seguridad informática a través del intercambio de información exclusivamente entre sus miembros.
17. Reporte.- Son los informes que remiten los prestadores de servicios del régimen general de telecomunicaciones a la ARCOTEL como respuesta a la gestión de incidentes y vulnerabilidades, de acuerdo a los formatos establecidos para tal fin.	[observaciones, comentarios, notas]	[propuesta de reforma]
18. Tiempo de Respuesta.- Tiempo en el cual los prestadores de servicios del régimen general de telecomunicaciones o la ARCOTEL deben remitir la respuesta de las acciones tomadas frente a las notificaciones de incidentes o vulnerabilidades.	[observaciones, comentarios, notas]	[propuesta de reforma]
19. TLP (Traffic Light Protocol).- Protocolo de semáforo o protocolo de señales de tráfico, es un esquema de clasificación de la información manejado a nivel de redes de confianza entre centros de respuesta a incidentes y vulnerabilidades de seguridad de las redes y servicios de telecomunicaciones.	[observaciones, comentarios, notas]	[propuesta de reforma]
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.	[observaciones, comentarios, notas]	[propuesta de reforma]
TÍTULO II CONSIDERACIONES TÉCNICAS	[observaciones, comentarios, notas]	[propuesta de reforma]

PROYECTO DE RESOLUCIÓN	OBSERVACIONES, COMENTARIOS, SUGERENCIAS DE USUARIOS DIGITALES	PROPUESTA DE REFORMA DE USUARIOS DIGITALES
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.	[observaciones, comentarios, notas]	[propuesta de reforma]
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. 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.	La comunidad objetivo también requiere información, más allá de recomendaciones de que no se debe hacer	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, además de 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.
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.	[observaciones, comentarios, notas]	[propuesta de reforma]
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 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.	[observaciones, comentarios, notas]	[propuesta de reforma]
TÍTULO III NOTIFICACIONES	[observaciones, comentarios, notas]	[propuesta de reforma]

PROYECTO DE RESOLUCIÓN	OBSERVACIONES, COMENTARIOS, SUGERENCIAS DE USUARIOS DIGITALES	PROPUESTA DE REFORMA DE USUARIOS DIGITALES
CAPÍTULO I GENERACIÓN DE NOTIFICACIONES	[observaciones, comentarios, notas]	[propuesta de reforma]
Artículo. 8.- Generación de Notificaciones.- Las notificaciones de vulnerabilidades e incidentes de seguridad de las redes o servicios de telecomunicaciones pueden generarse por:	[observaciones, comentarios, notas]	[propuesta de reforma]
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.	[observaciones, comentarios, notas]	[propuesta de reforma]
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.	[observaciones, comentarios, notas]	[propuesta de reforma]
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 denuncias deben también permitir que se realicen de manera anónima	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, incluso de manera anónima, 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 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.	[observaciones, comentarios, notas]	[propuesta de reforma]
CAPÍTULO II CLASIFICACIÓN DE LA INFORMACIÓN Y PRIORIZACIÓN DE NOTIFICACIONES	[observaciones, comentarios, notas]	[propuesta de reforma]
Artículo 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:	[observaciones, comentarios, notas]	[propuesta de reforma]

PROYECTO DE RESOLUCIÓN	OBSERVACIONES, COMENTARIOS, SUGERENCIAS DE USUARIOS DIGITALES	PROPUESTA DE REFORMA DE USUARIOS DIGITALES
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 el criterio de prioridad “Media” hasta que se le asigne el criterio de prioridad.	[observaciones, comentarios, notas]	[propuesta de reforma]
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 Titulo 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:	[observaciones, comentarios, notas]	[propuesta de reforma]
	[observaciones, comentarios, notas]	[propuesta de reforma]
a. Información Pública General (TLP: Blanco.- Difusión sin restricción) La información clasificada con TLP Blanco, es aquella información que la ARCOTEL o el prestador de servicios del régimen general de telecomunicaciones podrán difundir entre los miembros de su comunidad o el público en general. Este tipo de información debe cumplir con las siguientes consideraciones: i. Su divulgación no representa riesgo para el dueño o usuario al cual se relaciona la información. ii. Para su tratamiento no es necesario establecer restricciones especiales, más allá de las recomendaciones sobre el buen uso y conservación de la información. iii. Su difusión o utilización no transgrede derechos de autor.	[observaciones, comentarios, notas]	[propuesta de reforma]

PROYECTO DE RESOLUCIÓN	OBSERVACIONES, COMENTARIOS, SUGERENCIAS DE USUARIOS DIGITALES	PROPUESTA DE REFORMA DE USUARIOS DIGITALES
b. Información Pública Comunitaria (TLP: Verde.- Difusión dentro de la comunidad) La ARCOTEL o el prestador de servicios del régimen general de telecomunicaciones podrán compartir la información con miembros específicos de la Comunidad Objetivo, anonimizando la información para no causar perjuicio al propietario de la misma. Este tipo de información nunca debe ser publicada en internet o cualquier medio al cual el público en general pueda acceder. i. Se debe observar la no transgresión de los derechos de autor. ii. Se puede compartir con miembros que no pertenezcan al mismo sector, siempre y cuando sirva para prevenir que sean afectados por la misma vulnerabilidad o incidente.	La anonimización no permite una investigación, y la reserva debe existir mientras se haga el debido proceso	b. información Pública Comunitaria (TLP: Verde.- Difusión dentro de la comunidad) La ARCOTEL o el prestador de servicios del régimen general de telecomunicaciones podrán compartir la información con miembros específicos de la Comunidad Objetivo, reservando la información de identificación para no causar perjuicio al propietario de la misma. Este tipo de información ser no será publicada en internet o cualquier medio al cual el público en general pueda acceder, mientras duren las investigaciones. Se debe observar la no transgresión de los derechos de autor. Se puede compartir con miembros que no pertenezcan al mismo sector, siempre y cuando sirva para prevenir que sean afectados por la misma vulnerabilidad o incidente.
Información Sensible (TLP: Ámbar.- Difusión limitada) Este tipo de información puede ser difundida por la ARCOTEL o por los prestadores de servicios del régimen general de telecomunicaciones, a los miembros de su equipo de seguridad, o con prestadores de servicios del régimen general de telecomunicaciones que tengan relación directa en la solución del incidente o vulnerabilidad a la que se relaciona la información; y, con los clientes, abonados o usuarios que necesitan conocerla, para dar solución a una vulnerabilidad o incidente de seguridad de la información. El dueño de la información deberá autorizar el uso de la misma cuando se requiera su utilización para un propósito distinto al original, y que no se encuentre enmarcado en cualquiera de los aspectos establecidos en esta norma; es decir, que no sea para la gestión de un incidente o vulnerabilidad, por lo que bajo ninguna circunstancia se trasmitirá a terceros de forma verbal, escrita, o electrónica, sin autorización expresa del dueño de la información. i. Se debe asegurar la existencia de controles que garanticen la integridad y seguridad de información sensible, cuando sea transmitida por cualquier medio, de conformidad con lo indicado en el Anexo 1 “Protección de la Información”. ii. Se evitará imprimir documentos que contengan información sensible, más allá de lo estrictamente necesario, por lo cual se recomienda el intercambio de información a través de correo electrónico firmado y encriptado conforme el Anexo 1.	Integrar a miembros d ela red de confianza que permita un análisis desde las diferentes realidades	c. información Sensible (TLP: Ámbar.- Difusión limitada) Este tipo de información puede ser difundida por la ARCOTEL o por los prestadores de servicios del régimen general de telecomunicaciones, a los miembros de su equipo de seguridad, o con prestadores de servicios del régimen general de telecomunicaciones, o con redes de confianza que tengan relación directa en la solución o mitigación del incidente o vulnerabilidad a la que se relaciona la información; y, con los clientes, abonados o usuarios que necesitan conocerla, para dar solución o mitigación a una vulnerabilidad o incidente de seguridad de la información. El dueño de la información deberá autorizar el uso de la misma cuando se requiera su utilización para un propósito distinto al original, y que no se encuentre enmarcado en cualquiera de los aspectos establecidos en esta norma; es decir, que no sea para la gestión de un incidente o vulnerabilidad, por lo que bajo ninguna circunstancia se trasmitirá a terceros de forma verbal, escrita, o electrónica, sin autorización expresa del dueño de la información. Se debe asegurar la existencia de controles que garanticen la integridad y seguridad de información sensible, cuando sea transmitida por cualquier medio, de conformidad con lo indicado en el Anexo 1 “ProtecciOn de la información”. Se evitará imprimir documentos que contengan información sensible, más allá de lo estrictamente necesario, por lo cual se recomienda el intercambio de información a través de correo electrónico firmado y encriptado conforme el Anexo 1.
Información Confidencial (TLP: Rojo.- Solo para destinatarios específicos) La información catalogada como confidencial sólo podrá ser difundida por la ARCOTEL o por los prestadores de servicios del régimen general de telecomunicaciones, a miembros específicos de éstas, y será únicamente accedida por los destinatarios de la misma, prohibiéndose la compartición de este tipo de información, incluso a un nivel superior, ya que su difusión fuera del grupo deseado, podría tener un impacto en la privacidad, reputación o en la operación del negocio; si es mal utilizada. i. Si la información necesita ser extendida fuera del grupo deseado, se requiere autorización explícita por escrito del dueño de la información. ii. En general se debe evitar imprimir este tipo de información. iii. La transmisión de esta información se la debe realizar únicamente a través de medios seguros que garanticen la prohibición de acceso por parte de personas no autorizadas. iv. Este tipo de información debe cumplir con las medidas de seguridad establecidas en el Anexo 1.	Integrar a miembros d ela red de confianza que permita un análisis desde las diferentes realidades	d. información Confidencial (TLP: Rojo.- Solo para destinatarios específicos) La información catalogada como confidencial sólo podrá ser difundida por la ARCOTEL o por los prestadores de servicios del régimen general de telecomunicaciones, a miembros específicos de éstas o de la red de confianza, y será únicamente accedida por los destinatarios de la misma, prohibiéndose la compartición de este tipo de información, incluso a un nivel superior, ya que su difusión fuera del grupo deseado, podría tener un impacto en la privacidad, reputación o en la operación del negocio; si es mal utilizada. Si la información necesita ser extendida fuera del grupo deseado, se requiere autorización explícita por escrito del dueño de la información. En general se debe evitar imprimir este tipo de información. La transmisión de esta información se la debe realizar únicamente a través de medios seguros que garanticen la prohibición de acceso por parte de personas no autorizadas. Este tipo de información debe cumplir con las medidas de seguridad establecidas en el Anexo 1.
	[observaciones, comentarios, notas]	[propuesta de reforma]

PROYECTO DE RESOLUCIÓN	OBSERVACIONES, COMENTARIOS, SUGERENCIAS DE USUARIOS DIGITALES	PROPUESTA DE REFORMA DE USUARIOS DIGITALES
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 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.	Integrar a miembros d ela red de confianza que permita un análisis desde las diferentes realidades	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. La ARCOTEL elaborará, tomando en consideración los datos estadísticos existentes, un documento con la asignación inicial de prioridad a los incidentes y vulnerabilidades conocidos. El documento deberá ser puesto en conocimiento de los prestadores del régimen general de telecomunicaciones y la red de confianza, mediante publicación en su página web o vía comunicaciones por correo electrónico, por escrito o cualquier otro medio válido. 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. La ARCOTEL analizará las observaciones recibidas, y procederá, de ser necesario, a modificar las prioridades asignadas. Luego del análisis realizado, ARCOTEL publicará el listado definitivo de las prioridades asignadas a los incidentes y vulnerabilidades.
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 vulnerabilidad.	Integrar a miembros d ela red de confianza que permita un análisis desde las diferentes realidades	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, o de miembros de la red de confianza, 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 o miembros de la red de confianza que haya sido aceptada o negada su solicitud de cambio de prioridad de un determinado incidente o vulnerabilidad.
	[observaciones, comentarios, notas]	[propuesta de reforma]
Artículo 12.- 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.	[observaciones, comentarios, notas]	[propuesta de reforma]
TÍTULO IV PROTECCIÓN DE LA INFORMACIÓN	[observaciones, comentarios, notas]	[propuesta de reforma]

PROYECTO DE RESOLUCIÓN	OBSERVACIONES, COMENTARIOS, SUGERENCIAS DE USUARIOS DIGITALES	PROPUESTA DE REFORMA DE USUARIOS DIGITALES
Artículo 13.- Acuerdo de Confidencialidad y No Divulgación.- El (los) encargado (s) de seguridad del prestador de servicios del régimen general de telecomunicaciones, previo al comienzo de sus actividades para gestionar incidentes o vulnerabilidades, deberán proceder de acuerdo a lo siguiente: 1. Firmar Acuerdo (s) de Confidencialidad con el representante legal de la empresa prestadora de servicios del régimen general de telecomunicaciones o persona natural titular de una habilitación para prestar servicios del régimen general de telecomunicaciones, en el que se establezca (n) las obligaciones respecto a la no divulgación y tratamiento de información, una copia del mismo será remitido a la ARCOTEL, en un plazo no mayor a cinco (5) días hábiles, luego de su suscripción. 2. Los Acuerdos de confidencialidad deberán contener como mínimo lo contemplado en el Anexo 2 “Modelo de Acuerdo de Confidencialidad y No Divulgación de Información” de la presente Norma. 3. El Acuerdo de Confidencialidad y No Divulgación de Información respetará los niveles de prioridad y confidencialidad establecidos en la presente Norma Técnica, Título III, Capítulo II Clasificación de la Información y Priorización de Notificaciones.	[observaciones, comentarios, notas]	[propuesta de reforma]

PROYECTO DE RESOLUCIÓN	OBSERVACIONES, COMENTARIOS, SUGERENCIAS DE USUARIOS DIGITALES	PROPUESTA DE REFORMA DE USUARIOS DIGITALES
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.	La excepción debe ser que la información sea sensible, la regla debe ser que la información sea pública, siendo responsabilidad de los emisores su correcta clasificación en caso de requerirlo	Artículo 14.- Consideraciones para el intercambio de información.- Para el intercambio de información, se deberá considerar lo siguiente: 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. Toda información que ha sido remitida sin otorgarle un criterio de confidencialidad, se tratará como pública (TLP: VERDE). 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. 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] 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.
	[observaciones, comentarios, notas]	[propuesta de reforma]
	[observaciones, comentarios, notas]	[propuesta de reforma]
Artículo 15.- Consideraciones para el intercambio de información a través de correo electrónico.- Los mensajes de correo electrónico generados por la ARCOTEL hacia los prestadores de servicios del régimen general de telecomunicaciones, y de los prestadores hacia la ARCOTEL, deberán incluir una Cláusula de Confidencialidad, de acuerdo a lo que consta en el Anexo 3 “Cláusula de confidencialidad para correo electrónico” de la presente Norma Técnica. La ARCOTEL y los prestadores de servicios del régimen general de telecomunicaciones, implementarán controles de seguridad, para el intercambio cifrado de los mensajes de correo electrónico y otros documentos necesarios en la gestión de vulnerabilidades e incidentes, tanto para la transmisión de información como para su almacenamiento, de acuerdo al Anexo 4 “Firmado y cifrado en el intercambio de correo electrónico y documentos” de la presente Norma Técnica.	[observaciones, comentarios, notas]	[propuesta de reforma]

PROYECTO DE RESOLUCIÓN	OBSERVACIONES, COMENTARIOS, SUGERENCIAS DE USUARIOS DIGITALES	PROPUESTA DE REFORMA DE USUARIOS DIGITALES
Artículo 16.- Requerimientos de Autoridad Competente.- Ante un requerimiento de la autoridad competente, que involucre la entrega de información clasificada como Sensible o Confidencial, el prestador de servicios del régimen general de telecomunicaciones proporcionará la referida información salvaguardando sus propiedades de seguridad, indicando la clasificación de la misma respecto de la confidencialidad.	siempre se debe observar el debido proceso	Artículo 16.- Requerimientos de Autoridad Competente.- Ante un requerimiento de la autoridad competente, que involucre la entrega de información clasificada como Sensible o Confidencial, y siguiendo el debido proceso judicial de ser necesario, el prestador de servicios del régimen general de telecomunicaciones proporcionará la referida información salvaguardando sus propiedades de seguridad, indicando la clasificación de la misma respecto de la confidencialidad.
TÍTULO V RESPALDO Y CONSERVACIÓN DE LA INFORMACIÓN	[observaciones, comentarios, notas]	[propuesta de reforma]
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; es obligación del prestador el mantener adicionalmente la evidencia documentada, con los respaldos correspondientes de dichas comprobaciones.	[observaciones, comentarios, notas]	[propuesta de reforma]
Artículo 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.	[observaciones, comentarios, notas]	[propuesta de reforma]
TÍTULO VI DIFUSIÓN DE INFORMACIÓN	[observaciones, comentarios, notas]	[propuesta de reforma]

PROYECTO DE RESOLUCIÓN	OBSERVACIONES, COMENTARIOS, SUGERENCIAS DE USUARIOS DIGITALES	PROPUESTA DE REFORMA DE USUARIOS DIGITALES
Artículo 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.	Se deben emitir informes periodicos de transparecia donde incluyan todos los casos de incidentes y vulnerabilidades. respetando siempre un lapso prudencial que permita la corrección de las vulnerabilidades desde su notificación.	Artículo 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, con información personal reservada, de las comunicaciones realizadas. La ARCOTEL realizará publicaciones trimestrales públicas de transparencia de incidentes y vulnerabilidades donde se registrarán de manera histórica los mismos de manera general y concreta, su tratamiento, detalles del proceso, estatus a la fecha de publicación del informe, comunidad o entes involucrados, su prioridad y confidencialidad. Estos reportes no deberán presentar información personal de las personas naturales involucradas.
	[observaciones, comentarios, notas]	[propuesta de reforma]
TÍTULO VII GESTIÓN Y REPORTE DE VULNERABILIDADES E INCIDENTES	[observaciones, comentarios, notas]	[propuesta de reforma]
CAPÍTULO I GESTIÓN DE NOTIFICACIONES EMITIDAS POR LA ARCOTEL A LOS PRESTADORES DE SERVICIOS DEL RÉGIMEN GENERAL DE TELECOMUNICACIONES.	[observaciones, comentarios, notas]	[propuesta de reforma]

PROYECTO DE RESOLUCIÓN	OBSERVACIONES, COMENTARIOS, SUGERENCIAS DE USUARIOS DIGITALES	PROPUESTA DE REFORMA DE USUARIOS DIGITALES
Artículo 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: (ver tabla en el proyecto de norma)	[observaciones, comentarios, notas]	[propuesta de reforma]
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 vulnerabilidades e incidentes de seguridad de la información que le sean notificadas por la ARCOTEL o que hayan sido detectadas por sí mismos.	Esta información debe ser entregada de forma general y en ningún momento incluir datos especificos de destinatarios finales.	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, reservando datos de destinatarios finales, 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 sí mismos.
	[observaciones, comentarios, notas]	
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.	[observaciones, comentarios, notas]	[propuesta de reforma]
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: (Ver tabla en el proyecto de norma)	[observaciones, comentarios, notas]	[propuesta de reforma]

PROYECTO DE RESOLUCIÓN	OBSERVACIONES, COMENTARIOS, SUGERENCIAS DE USUARIOS DIGITALES	PROPUESTA DE REFORMA DE USUARIOS DIGITALES
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: (Ver tabla en el proyecto de norma)	[observaciones, comentarios, notas]	[propuesta de reforma]
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 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.	[observaciones, comentarios, notas]	[propuesta de reforma]
CAPÍTULO II GESTIÓN DE NOTIFICACIONES DE PERSONAS NATURALES O JURÍDICAS	[observaciones, comentarios, notas]	[propuesta de reforma]

PROYECTO DE RESOLUCIÓN	OBSERVACIONES, COMENTARIOS, SUGERENCIAS DE USUARIOS DIGITALES	PROPUESTA DE REFORMA DE USUARIOS DIGITALES
Artículo 24.- Gestión de vulnerabilidades e incidentes que involucren a la comunidad objetivo de la ARCOTEL.- Las notificaciones originadas en información generada por personas naturales o jurídicas, organismos nacionales o internacionales, en relación con el 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.	[observaciones, comentarios, notas]	[propuesta de reforma]
CAPÍTULO III REPORTE DE GESTIÓN POR PARTE DE PRESTADORES DE SERVICIOS DEL RÉGIMEN GENERAL DE TELECOMUNICACIONES A LA ARCOTEL	[observaciones, comentarios, notas]	[propuesta de reforma]
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:	[observaciones, comentarios, notas]	[propuesta de reforma]
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.	[observaciones, comentarios, notas]	[propuesta de reforma]
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.	[observaciones, comentarios, notas]	[propuesta de reforma]
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.	[observaciones, comentarios, notas]	[propuesta de reforma]

PROYECTO DE RESOLUCIÓN	OBSERVACIONES, COMENTARIOS, SUGERENCIAS DE USUARIOS DIGITALES	PROPUESTA DE REFORMA DE USUARIOS DIGITALES
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 incidente@ecucert.gob.ec, para su registro.	[observaciones, comentarios, notas]	[propuesta de reforma]
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:	[observaciones, comentarios, notas]	[propuesta de reforma]
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.	[observaciones, comentarios, notas]	[propuesta de reforma]
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.	[observaciones, comentarios, notas]	[propuesta de reforma]
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. Los tiempos de atención de los incidentes y vulnerabilidades deben estar de acuerdo a lo dispuesto en el artículo 22 de la presente Norma.	[observaciones, comentarios, notas]	[propuesta de reforma]
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.	[observaciones, comentarios, notas]	[propuesta de reforma]

PROYECTO DE RESOLUCIÓN	OBSERVACIONES, COMENTARIOS, SUGERENCIAS DE USUARIOS DIGITALES	PROPUESTA DE REFORMA DE USUARIOS DIGITALES
Artículo 29.- Escalamiento de incidentes detectados y que requieren apoyo de ARCOTEL.- Para el caso de incidentes de seguridad en las redes y servicios detectados por el prestador de servicios 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.	[observaciones, comentarios, notas]	[propuesta de reforma]
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 régimen general de telecomunicaciones involucrados.	[observaciones, comentarios, notas]	[propuesta de reforma]
TÍTULO VIII DERECHOS Y OBLIGACIONES DE LOS PRESTADORES DE SERVICIOS DEL RÉGIMEN GENERAL DE TELECOMUNICACIONES	[observaciones, comentarios, notas]	[propuesta de reforma]
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:	[observaciones, comentarios, notas]	[propuesta de reforma]
1. Cumplir con los tiempos de gestión y reporte, establecidos en la presente Norma.	[observaciones, comentarios, notas]	[propuesta de reforma]
2. Entregar la información en los formularios que para el efecto publique la ARCOTEL.	[observaciones, comentarios, notas]	[propuesta de reforma]
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.	[observaciones, comentarios, notas]	[propuesta de reforma]

PROYECTO DE RESOLUCIÓN	OBSERVACIONES, COMENTARIOS, SUGERENCIAS DE USUARIOS DIGITALES	PROPUESTA DE REFORMA DE USUARIOS DIGITALES
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 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, conforme lo señala el artículo 79 de la Ley Orgánica de Telecomunicaciones.	usuarios debría cambiarse por "usuarios en general"	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 en general 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 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, conforme lo señala el artículo 79 de la Ley Orgánica de Telecomunicaciones.
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 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:	[observaciones, comentarios, notas]	[propuesta de reforma]
1. Disponer de los formatos para la presentación de reportes establecidos en la presente norma.	[observaciones, comentarios, notas]	[propuesta de reforma]
2. Disponer del documento con los niveles de prioridad asignados por la ARCOTEL.	[observaciones, comentarios, notas]	[propuesta de reforma]
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.	[observaciones, comentarios, notas]	[propuesta de reforma]
4. Sugerir a los clientes, abonados o suscriptores adoptar medidas a fin de salvaguardar la integridad de la red y las comunicaciones.	[observaciones, comentarios, notas]	[propuesta de reforma]
TÍTULO IX SEGURIDAD DE REDES Y SERVICIOS	[observaciones, comentarios, notas]	[propuesta de reforma]

PROYECTO DE RESOLUCIÓN	OBSERVACIONES, COMENTARIOS, SUGERENCIAS DE USUARIOS DIGITALES	PROPUESTA DE REFORMA DE USUARIOS DIGITALES
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, 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:	el proceso de auditorías internas por parte de los prestadores de servicio, debe ser un proceso persistente y continuo. Por lo cual una frecuencia semestral subiría los estandares de seguridad	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 semestralmente, 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 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:
	[observaciones, comentarios, notas]	[propuesta de reforma]
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.	[observaciones, comentarios, notas]	[propuesta de reforma]
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.	[observaciones, comentarios, notas]	[propuesta de reforma]
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.	[observaciones, comentarios, notas]	[propuesta de reforma]
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:	[observaciones, comentarios, notas]	[propuesta de reforma]
1. Análisis preliminar de riesgos respecto de las vulnerabilidades en los servicios y redes de telecomunicaciones.	[observaciones, comentarios, notas]	[propuesta de reforma]
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.	¿Quíen establecera cuando una empresa o persona es competente y bajo que cirterios? Será a juicio del prestador de servicios o se debe regir por alguna recomendación especifica de ARCOTEL.	[propuesta de reforma]

PROYECTO DE RESOLUCIÓN	OBSERVACIONES, COMENTARIOS, SUGERENCIAS DE USUARIOS DIGITALES	PROPUESTA DE REFORMA DE USUARIOS DIGITALES
3. Alcance y objetivos.	[observaciones, comentarios, notas]	[propuesta de reforma]
4. Estándares o procedimientos adoptados para llevar a cabo la auditoría.	[observaciones, comentarios, notas]	[propuesta de reforma]
5. Plan de ejecución, actividades y acciones.	[observaciones, comentarios, notas]	[propuesta de reforma]
6. Resultados de riesgos y vulnerabilidades detectados.	[observaciones, comentarios, notas]	[propuesta de reforma]
7. Medidas preventivas implementadas o por implementar.	[observaciones, comentarios, notas]	[propuesta de reforma]
8. Se deberá adjuntar el informe de la empresa o persona que ejecutó la auditoría.	[observaciones, comentarios, notas]	[propuesta de reforma]
9. Reporte de Equipos críticos.	[observaciones, comentarios, notas]	[propuesta de reforma]
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:	En cuanto a la información que se pide almacenar por 3 años en texto plano, de "equipos criticos", ¿a qué información se refiere especificamente?. Desde nuestro entender esto seria creear un punto vulnerable en el tratamiento de la información	[propuesta de reforma]
1. Como resultado de la auditoría se ha determinado que presentan vulnerabilidades.	[observaciones, comentarios, notas]	[propuesta de reforma]
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.	[observaciones, comentarios, notas]	[propuesta de reforma]
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.	[observaciones, comentarios, notas]	[propuesta de reforma]
El reporte de equipos críticos deberá contener como mínimo: 1. El nombre del equipo	[observaciones, comentarios, notas]	[propuesta de reforma]
2. Ubicación del equipo (Dirección, coordenadas geográficas DATUM WGS84, formato decimal)	[observaciones, comentarios, notas]	[propuesta de reforma]
3. Vulnerabilidades detectadas.	[observaciones, comentarios, notas]	[propuesta de reforma]
4. Historial de incidentes propios (ocurridas en el mencionado equipo)	[observaciones, comentarios, notas]	[propuesta de reforma]
5. Historial de incidentes (ocurridos en otras empresas para el mismo tipo de equipos)	[observaciones, comentarios, notas]	[propuesta de reforma]
6. Tipo de información afectada en caso de ocurrencia de un incidente.	[observaciones, comentarios, notas]	[propuesta de reforma]

PROYECTO DE RESOLUCIÓN	OBSERVACIONES, COMENTARIOS, SUGERENCIAS DE USUARIOS DIGITALES	PROPUESTA DE REFORMA DE USUARIOS DIGITALES
Artículo 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.	[observaciones, comentarios, notas]	[propuesta de reforma]
TÍTULO X CONTACTOS Y NOTIFICACIONES	[observaciones, comentarios, notas]	[propuesta de reforma]
Artículo 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 continuas.	[observaciones, comentarios, notas]	[propuesta de reforma]
DISPOSICIONES GENERALES	[observaciones, comentarios, notas]	[propuesta de reforma]
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 y en general para la aplicación de la presente Norma Técnica.	[observaciones, comentarios, notas]	[propuesta de reforma]
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.	[observaciones, comentarios, notas]	[propuesta de reforma]
DISPOSICIONES TRANSITORIAS	[observaciones, comentarios, notas]	[propuesta de reforma]

PROYECTO DE RESOLUCIÓN	OBSERVACIONES, COMENTARIOS, SUGERENCIAS DE USUARIOS DIGITALES	PROPUESTA DE REFORMA DE USUARIOS DIGITALES
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.	[observaciones, comentarios, notas]	[propuesta de reforma]
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.	[observaciones, comentarios, notas]	[propuesta de reforma]
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.	[observaciones, comentarios, notas]	[propuesta de reforma]
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 sus respectivos instructivos de llenado.	[observaciones, comentarios, notas]	[propuesta de reforma]
La presente Norma, entrará en vigencia a partir de su publicación en el Registro Oficial.	[observaciones, comentarios, notas]	[propuesta de reforma]
ANEXO 1 PROTECCIÓN DE LA INFORMACIÓN.	le damos robustez para no tener usuarios y claves admin/admin	1.2. información Sensible y Confidencial. a) La información Sensible y Confidencial debe ser almacenada en sistemas o repositorios centralizados y para su acceso al menos se debe implementar un mecanismo de autenticación de usuario/clave (password) con formato que tenga en cuenta mejores prácticas, y tendrán acceso los encargados de seguridad y las personas a las que expresamente el prestador de servicios del régimen general de telecomunicaciones haya establecido conforme a sus políticas internas. ... c) La información sensible y confidencial deberá ser encriptada, con un tipo de cifrado robusto, para garantizar la confidencialidad e integridad de la información.
ANEXO 2 MODELO DE ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE INFORMACIÓN.	[observaciones, comentarios, notas]	[propuesta de reforma]
ANEXO 3 CLÁUSULA DE CONFIDENCIALIDAD PARA CORREO ELECTRÓNICO.	[observaciones, comentarios, notas]	[propuesta de reforma]
ANEXO 4 FIRMADO Y CIFRADO EN EL INTERCAMBIO DE CORREO ELECTRÓNICO Y DOCUMENTOS	[observaciones, comentarios, notas]	[propuesta de reforma]