2017

ARCOTEL

Guayaquil, 07 de Diciembre de 2017

INFORME DE OBSERVACIONES A “NORMA TÉCNICA PARA COORDINAR LA GESTIÓN DE INCIDENTES Y VULNERABILIDADES QUE AFECTEN A LA SEGURIDAD DE LAS REDES Y SERVICIOS DE TELECOMUNICACIONES”

Agencia de Regulación y Control de las Telecomunicaciones

telconet

Aviso de confidencialidad

Contenido

Control de Cambios

Versión	Responsable	Comentarios
1.0	zespinoza	Elaboración
1.0	psamaniego	Verificación
1.0	aaranda	Aprobación

Introducción

El presente informe tiene como objetivo emitir las observaciones al proyecto de **"NORMA TÉCNICA PARA COORDINAR LA GESTIÓN DE INCIDENTES Y VULNERABILIDADES QUE AFECTEN A LA SEGURIDAD DE LAS REDES Y SERVICIOS DE TELECOMUNICACIONES**".

Observaciones de contenido.

1.1 TÍTULO II, CONSIDERACIONES TÉCNICAS

- No se contempla consideraciones técnicas para el **Cliente Final**, en los casos en que este es responsable del buen uso de las IPs asignadas por el portador de servicio. Por favor incluir la responsabilidad del cliente final.

> **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.

- Se recomienda se incluya que los integrantes de las unidades especializadas firmen un acuerdo de confidencialidad con ARCOTEL, esto a fin de proteger la información procesada en funciones y posterior a la relación laboral. Las unidades especializadas pueden ser conformadas por terceros.

1.2 TÍTULO III NOTIFICACIONES, CAPÍTULO I GENERACIÓN DE NOTIFICACIONES

> 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.

- A fin de poder cumplir con los tiempos establecidos, se solicita que ARCOTEL establezca un protocolo de comunicación para automatizar el proceso de reporte de incidentes de seguridad y el seguimiento respectivo.

1.3 TÍTULO III NOTIFICACIONES, CAPÍTULO II CLASIFICACIÓN DE LA INFORMACIÓN Y PRIORIZACIÓN DE NOTIFICACIONES

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 prioridad de los incidentes de seguridad puede cambiar en función de las condiciones cibernéticas presentes así como la información de contexto que se vaya agregando a la investigación. Se solicita ARCOTEL establezca un protocolo de cambio de prioridad mas dinámico, a fin de poder cumplir con los tiempos establecidos, se recomienda que este pueda ser automatizado.

1.4 TÍTULO IV PROTECCIÓN DE LA INFORMACIÓN

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.

- Que el acuerdo de confidencialidad se extienda a los responsables de la gestión de vulnerabilidades e incidentes de seguridad designados por el prestador de servicios.
- Por favor incluir un Acuerdo de Confidencialidad de los representantes designados para la atención de Vulnerabilidades o Incidentes por parte del ARCOTEL al Proveedor de Servicios.

1.5 TÍTULO VI DIFUSIÓN DE INFORMACIÓN

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.

- Incluir ARCOTEL protegerá de identidad de prestador de servicios sea esto comunicándolo directamente, por ejemplo usando el propio nombre, o indirectamente, por ejemplo indicando la IP afectada, banners y demás.

1.6 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.

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:

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

- Para los casos que involucran IPs, salvando la situación de Incidentes que puedan tener varias IPs involucradas; se solicita que ARCOTEL que asigne un Ticket por IP afectada. El objetivo es que el prestador de Servicios pueda cumplir con los tiempos asignados según la realidad de cada vulnerabilidad o incidente reportado.

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.

- El tiempo de gestión debe contemplar que las acciones que puede tomar el Proveedor de Servicios no puede afectar los Servicios brindados al cliente salvo que sea una disposición del ente regulador ARCOTEL; por lo que las instrucciones de atención/gestión de los incidentes y vulnerabilidades deben explícitamente indicar qué acciones puede ejercer el Prestador de Servicios y en qué tiempo, como por ejemplo el bloqueo de puertos, IP o la suspención de Servicios, esto en función de la prioridad asignada y congruente con los tiempos de gestión establecidos.
- Dado que no existe una regulación clara de las acciones que puede tomar el Proveedor de Servicios para la atención de vulnerabilidades e incidentes, se considera

que la retroaliementación del cliente solicitando tiempo adicional para la gestión es una opción válida, así como la incapacidad declarada para atender el mismo (sea esta técnica o económica). Aceptar este tipo de retroalimentación por parte del cliente va a afectar directamente al Proveedor de Servicios en el cumplimiento de los tiempos establecidos. Se solicita que estos casos sean escalados a la ARCOTEL para su gestión directa con el cliente y el Ticket sea cerrado por parte del proveedor o en su defecto se aclare como se va a atender estos casos.

- Existirán vulnerabilidades o incidentes, donde luego de la gestión sea por parte del Cliente o por parte del Proveedor de Servicios, no existan mecanismos de validación salvo la base de información de ARCOTEL, quienes asignaron el caso. Se solicita que ARCOTEL disponga de un API WEB o algún mecanismo de validación automática para el cierre de estos casos.

1.7 TÍTULO VI GESTIÓN Y REPORTE DE VULNERABILIDADES E INCIDENTES, CAPÍTULO III REPORTE DE GESTIÓN POR PARTE DE PRESTADORES DE SERVICIOS DEL RÉGIMEN GENERAL DE TELECOMUNICACIONES A LA ARCOTEL.

- Se solicita que ARCOTEL establezca mecanismos de automatización de reportes de gestión de tickets asignados (vulnerabilidades o incidentes). Para ISPs con elevado número de IPs asignadas, la gestión manual resulta inviable por los costos operativos y los tiempos asignados.

> **Artículo 27.- Forma de reporte de vulnerabilidades o incidentes detectados y solucionados por el prestador de servicios del régimen general de telecomunicaciones.-** Para el reporte de vulnerabilidades e incidentes por parte de los prestadores de servicios del régimen general de telecomunicaciones, se deberá cumplir lo siguiente:
>
> 1. **Reporte de vulnerabilidades.-** Las vulnerabilidades detectadas y solucionadas por los prestadores de servicios del régimen general de telecomunicaciones, en su red o en sus clientes, abonados o usuarios, y que no correspondan a los notificados por ARCOTEL, serán reportados mensualmente a dicha Agencia de manera consolidada por cada tipo de vulnerabilidad y tipo de usuario, dentro de los cinco (5) primeros días hábiles del mes siguiente, utilizando el Formato FO-CCDR-03, publicado por la ARCOTEL.
>
> 2. **Reporte de incidentes.-** Los incidentes detectados y solucionados por los prestadores de servicios del régimen general de telecomunicaciones, en su red o en sus clientes, abonados o

- Se está solicitando reportar mensualmente información sensible, como lo es la vulnerabilidad gestionada por parte del Proveedor en su red, proceso continuo, confidencial e interno, de ser necesario se debe esclarecer el alcance de la información que se va a intercambiar (IPs privada, Públicas), el nivel de detalle (Ejecutivo, Técnico).

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.

- Existen formularios no especificados, se solicita que estos formatos contemplen la automatización de operaciones.

- Para proteger la información en tránsito y evitar puntos de fuga de información, se recomienda que el Proveedor de Servicios ofrezca un portal donde ARCOTEL pueda accede a ver la información solicitada.

1.8 TÍTULO VIII DERECHOS Y OBLIGACIONES DE LOS PRESTADORES DE SERVICIOS DEL RÉGIMEN GENERAL 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:

1. Disponer de los formatos para la presentación de reportes establecidos en la presente norma.
2. Disponer del documento con los niveles de prioridad asignados por la ARCOTEL.
3. Reportar ante la ARCOTEL acerca de incidentes y vulnerabilidades originados en otros prestadores de servicios del régimen general de telecomunicaciones, para que se coordinen las acciones de atención correspondientes.
4. Sugerir a los clientes, abonados o suscriptores adoptar medidas a fin de salvaguardar la integridad de la red y las comunicaciones.

- Agregar como derecho lo siguiente o similar: Adoptar medidas de bloqueo de puertos o suspención de Servicios de clientes cuando estos representen una amenaza Crítica que puedan comprometer el servicio del propio cliente, otros clientes o la infraestructura del proveedor.
- ¿Qué mecanismos tiene el proveedor para protegerse contra una cantidad desmesurada de notififaciones del ARCOTEL cuando estos dependen del cliente final y que esto afecte a sus operaciones, recursos y finalmente tiempos de respuesta?

1.9 TÍTULO IX SEGURIDAD DE REDES Y SERVICIOS.

> 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:

- Este es un proceso interno, el Proveedor de Servicios debe disponer del derecho de manejar los tiempos a sus condiciones y no necesariamente esto permitirá notificar con 15 días de antelación.
- El proceso de auditoría contempla datos internos sensibles, se necesita establecer claramente la participación del ARCOTEL y el Proveedor tiene el derecho de rechazar esta participación si así lo considera necesario.

> Como resultado de la auditoría anual el prestador de servicios del régimen general de telecomunicaciones deberá presentar un informe ante la ARCOTEL en un plazo no superior a 30 días hábiles luego de finalizada la misma, el cual deberá incluir como mínimo lo siguiente:
>
> 1. Análisis preliminar de riesgos respecto de las vulnerabilidades en los servicios y redes de telecomunicaciones.
> 2. Información de la empresa, organismo o personas que ejecutaron la auditoría, lo que debe incluir datos de la experiencia relacionada con la realización de este tipo de auditorías.
> 3. Alcance y objetivos.
> 4. Estándares o procedimientos adoptados para llevar a cabo la auditoría.
> 5. Plan de ejecución, actividades y acciones.
> 6. Resultados de riesgos y vulnerabilidades detectados.
> 7. Medidas preventivas implementadas o por implementar.
> 8. Se deberá adjuntar el informe de la empresa o persona que ejecutó la auditoría.
> 9. Reporte de Equipos críticos.

- El informe de auditoria externa de ISO27001 debería cumplir este requisito, confirmar.
- El informe a ser entregado deberá ser de tipo ejecutivo, en caso se requiera detalles se deberá realizar en sitio mediante una visita coordinada previamente con el Proveedor de Servicios.

> **Artículo 34.- Equipos Críticos.-** Como resultado de la auditoría y con el fin de preservar la seguridad de los servicios y la invulnerabilidad de la red, los prestadores de servicios del régimen general de telecomunicaciones identificarán los equipos críticos de su infraestructura sobre la cual brindan el servicio, así como también deberán almacenar en una ubicación específica, los registros referentes a seguridad e invulnerabilidad de la red que generen éstos, en formato texto plano. Los registros deberán almacenarlos al menos por tres (3) años.
>
> Se consideran equipos críticos aquellos que:
>
> 1. Como resultado de la auditoría se ha determinado que presentan vulnerabilidades.
> 2. Históricamente se ha identificado que son susceptibles a incidentes relacionados con seguridad de las redes y servicios, sobre la base de registros de la propia empresa o de otras empresas.
> 3. Equipos, cuya afectación originada por un incidente o que como resultado de la materialización de una vulnerabilidad, implique la violación de la seguridad de la red, servicios y de los datos personales de los usuarios, entendiéndose como tal la destrucción, accidental o ilícita, la pérdida, la revelación o el acceso no autorizados, de datos personales transmitidos, almacenados o tratados en la prestación de un servicios de telecomunicaciones.

- Se solicita que esta información no salga de la infraestructura del Proveedor, este ofrezca un portal donde el ARCOTEL pueda acceder y no descargar la misma.

Observaciones de generales.

- Por favor indicar cuanto tiempo se asignará a los Proveedores para implementar esta norma.
- En el caso que un ISP tiene como cliente a otro ISP, quién será el responsable de atender los tickets asignados al cliente final?
- Cuáles son las responsabilidades y compromisos tiempo de respuesta de ARCOTEL cuando un prestador de Servicios le reporte inceidentes a esta entidad?
- Para cumplir con los tiempos de respuesta establecidos, se requiere que el ARCOTEL designe mecanismos automatizados de gestión, estableciendo un protocolo de comunicación “máquina – máquina” con el proveedor.
- Que opciones de respuesta y respaldo tiene el Proveedor de Servicios por parte del ARCOTEL cuando el cliente exige, no permite o amenaza con reclamos al ente regulador en caso de bloqueo de puertos, servicios o IPs como parte de la respuesta a un incidente. Por parte del proveedor, se declarará que el cliente no debe o puede tomar acciones y se escalará al ARCOTEL.
- Cómo se garantizará que la información de bloques de ip no salga de los Dominios de ARCOTEL? De existir un riesgo, sugerimos que antes de solicitar toda la base de información de IP de clientes, provisionar una consulta automática de forma individual por IP. Donde responderemos únicamente por el registro consultado.
- ARCOTEL: Crear un Ranking de eficacia de manejo de incidentes por ISPs.
- ARCOTEL: Realizar jornadas de manejo de incidentes mínimo de 1 vez al año para compartir buenas prácticas, con exponentes extranjeros.
- En general darle un enfoque positivo a la gestión de incidentes y no impositivo.
- Para mejoras de fondo en la ciberseguridad debemos incluir un Análisis de causas raiz y sus opciónes de tratamiento basado como mínimo en un modelo PAR (Prevenir. suceda, Alertar si está sucediendo y Reducir el Daño).