OBSERVACIONES POR PARTE DE ETAPA EP 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”

En la página 5/30 cuarto párrafo se expresa que La Dirección Nacional de Procesos, Calidad, Servicios y Cambio y Cultura Organizacional, con memorando Nro. ARCOTEL-CPDP-2017-0039-M de 04 de julio de 2017, emite la siguiente codificación: (i) **FO-CCDR-01:** INFORME TÉCNICO DE GESTIÓN DE INCIDENTES REPORTADOS POR ECUCERT. (ii) **FO-CCDR-02:** REPORTES DE INCIDENTES QUE PERTENEZCAN A UN PROVEEDOR DE SERVICIOS DE TELECOMUNICACIONES DIFERENTE O CUYA FUENTE DE ORIGEN NO SE ENCUENTRE DENTRO DEL TERRITORIO NACIONAL. (iii) **FO-CCDR-03:** ESCALAMIENTO DE INCIDENTES DETECTADOS EN LA RED DEL PRESTADOR DE SERVICIOS DE TELECOMUNICACIONES Y QUE REQUIERA APOYO DE ECUCERT (iv) **FO-CCDR-04:** VULNERABILIDADES REPORTADAS POR EL ECUCERT. (v) **FO-CCDR- 05:** REPORTE MENSUAL DE GESTIÓN DE VULNERABILIDADES DETECTADAS Y SOLUCIONADAS POR EL PRESTADOR DE SERVICIOS DE TELECOMUNICACIONES.(vi) **FO-CCDR-06:** REPORTE DE GESTIÓN DE INCIDENTES DETECTADOS Y SOLUCIONADOS POR EL PRESTADOR DE SERVICIOS DE TELECOMUNICACIONES, sin embargo dichos documentos no han sido dados a conocer a los Prestadores de servicios, por tanto, observando que la aplicación y tratamiento de los formatos normalmente implica la necesidad de recursos a nivel técnico y administrativo, solicitamos que dicha información se dé a conocer a los Prestadores a la brevedad posible al ser un aspecto fundamental de la aplicación de la Norma, y que se permita las observaciones correspondientes.

Sobre el Artículo 8, numeral 3 de la página 10/30, es necesario que ARCOTEL realice el filtrado de los requerimientos de los abonados, clientes y usuarios de modo que no se deriven al Prestador pedidos que recaen en el ámbito de responsabilidad del abonado, cliente o usuario como la operación y mantenimiento de la infraestructura interna. Tener en cuenta en la cadena de tratamiento del reclamo del cliente, abonado o usuario los mecanismos para mantener anónima la información (Anonimizar la información, según numeral 2 del Artículo 3 de la página 7/30).

En el Artículo 9, numeral 2 de la página 11/30 se expresa: “Su divulgación no representa riesgo para el dueño o usuario al cual se relaciona la información.” Siendo necesario que el criterio se detalle, como está redactado deja abierta la posibilidad de interpretación subjetiva.

Adicionalmente, esta disposición se refiere a la notificación y reportes, así como la información contenida en las mismas, que se intercambian entre la ARCOTEL y los prestadores de servicios del régimen general de telecomunicaciones estableciendo criterios de prioridad y confidencialidad para ser clasificada, es decir tanto el ARCOTEL como los prestadores de servicios deberían clasificar todas las notificaciones.

Tal como está la norma entenderíamos que aquellas notificaciones de vulnerabilidad que realiza el abonado, cliente o usuario deberían ser clasificadas por el ARCOTEL, si no es así, aclarar la disposición.

Por otro lado, el criterio de confidencialidad vemos que está con un alto grado de subjetividad, hay que tener presente además que como prestadores de servicios de telecomunicaciones debemos garantizar la protección de datos de carácter personal, esto con base al derecho de intimidad y protección de datos que se reconoce a las personas en la Constitución, por lo que, la transferencia de datos no sería posible si no se cuenta con la autorización o consentimiento previo del usuario. Sugerimos se revise más detenidamente esta disposición.

En el Artículo 11, página 12/30 se expresa: “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”, al respecto es importante expresar que se debería considerar que con un análisis fundamentado de la instancia correspondiente de ARCOTEL se podrá cambiar la prioridad a un incidente o vulnerabilidad con periodicidad menor ya que una vulnerabilidad puede aumentar su impacto en tiempos muy cortos.

En el Artículo 17, página 14/30 se expresa: “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”, en este aspecto existen Prestadores pequeños que pueden optar por contratar sus respaldos en Data Centers de otros prestadores que tengan la infraestructura desplegada en el territorio nacional, esto se constituye en un sistema comercial, por tanto, se recomienda revisar este aspecto para evitar ser restrictivos innecesariamente.

En el Artículo 22, página 16/30, en la tabla del literal (a) en los tiempos máximos se tiene dos columnas, en referencia a la columna de “Recepción y análisis” cómo ARCOTEL verificará este plazo? Si la Respuesta tiene un plazo mayor en el tiempo, se sugiere dejar únicamente la columna “Gestión y Respuesta” considerando además que toda acción que se tome sobre la vulnerabilidad es parte de la gestión de la misma, incluso el análisis.

En el Artículo 22, página 17/30, en la tabla del literal (a) en los tiempos máximos se tiene dos columnas, en referencia a la columna de “Recepción y análisis” cómo ARCOTEL verificará este plazo? Si la Respuesta tiene un plazo mayor en el tiempo, se sugiere dejar únicamente la columna “Gestión y Respuesta” considerando además que toda acción que se tome sobre la vulnerabilidad es parte de la gestión de la misma, incluso el análisis.

En el Artículo 23, página 17/30 se dice: “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”, sin embargo es preciso tener en cuenta que durante la atención de incidentes los especialistas que atienden los casos y realizan los informes correspondientes están dedicados a gestionar el o los incidentes, por tanto, es conveniente que para la presentación de los justificativos se extienda el plazo en un tiempo prudente (al menos 8 horas adicionales).

Sobre el Artículo 30 de la página 19/30, por favor, se solicita se presente a los Prestadores los formatos existentes para revisión y emisión de observaciones previo a su aprobación.

En el Artículo 31 de la página 20/30 literal 3, se expresa: “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.” tener en cuenta que la responsabilidad de la red e infraestructura interna del abonado, cliente, usuario es del mismo y el Prestador no está facultado a intervenir en la misma, y de persistir la inobservancia del cliente, abonado, usuario a las correcciones y estando en riesgo la infraestructura del Prestador o en riesgo el servicio prestado y siendo necesario medidas de contención y propagación de vulnerabilidades es necesario la suspensión del servicio acorde a las cláusulas correspondientes que deben constar en contrato entre el Prestador y el cliente, abonado.

En el Artículo 33, hoja 20/30 se expresa que los prestadores deberán realizar auditorías de seguridad, de infraestructura tecnológica, de seguridad de redes, seguridad de las comunicaciones y datos personales una vez al año y que estas auditorias 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, en este aspecto tener en cuenta que en el caso de Prestadores del sector público los Presupuestos, PAC deben contemplar los procesos a efectuarse el siguiente año, por tanto, es conveniente que en primera instancia ARCOTEL notifique hasta el 30 de octubre de cada año la necesidad de la auditoría, y que se emita un Anexo a la norma de parte de ARCOTEL con los lineamientos mínimos para la consultoría y con el formato de los entregables, teniendo en cuenta que para respetar el principio de anonimizar los datos en los resultados a presentar a ARCOTEL se omitirán los datos de clientes, abonados, usuarios.

En la Transitoria 4, página 23/30, por favor poner a disposición de los Prestadores los formatos para revisión y emisión de observaciones que motiven notificaciones previo a aprobación.