CONSEJO DIRECTIVO DEL
INSTITUTO DOMINICANO DE LAS TELECOMUNICACIONES
(INDOTEL)

RESOLUCIÓN NÚM. 126-2021

QUE DICTA EL REGLAMENTO DE CIBERSEGURIDAD PARA LA PRESTACIÓN DEL SERVICIO DE ACCESO A INTERNET.

El **INSTITUTO DOMINICANO DE LAS TELECOMUNICACIONES (INDOTEL),** por órgano de su Consejo Directivo, en ejercicio de las atribuciones que le confiere la Ley General de Telecomunicaciones, núm. 153-98, promulgada el 27 de mayo de 1998, reunido válidamente, previa convocatoria, dicta la presente **RESOLUCIÓN:**

Con motivo de la aprobación del **REGLAMENTO DE CIBERSEGURIDAD PARA LA PRESTACIÓN DEL SERVICIO DE ACCESO A INTERNET**, puesto en consulta mediante la Resolución del Consejo Directivo del **INDOTEL** núm. 082-2021 en fecha 5 de agosto del 2021.

Para una comprensión más clara del presente acto administrativo, se ha organizado su contenido de la manera siguiente:

Índice temático **Pág.**

I. Antecedentes

1. En noviembre de 2020, la Dirección de Ciberseguridad, Comercio Electrónico y Firma Digital del **INDOTEL** elaboró un Documento de Análisis para formular el Reglamento de Ciberseguridad para el Sector de las Telecomunicaciones, el cual entre sus principales conclusiones indica que r*esulta de alta prioridad la formulación de un* ***Reglamento de Ciberseguridad para el Sector de las Telecomunicaciones*** *que tenga como objetivo, establecer las normas de ciberseguridad que deben cumplir para implementar una política de ciberseguridad de anticipación en la que estén identificados los requisitos de ciber resiliencia para cada servicio esencial que presten para evitar que se vean comprometidos; resistir para continuar con los servicios esenciales, en caso de sufrir un ciberataque o cualquier otro incidente cibernético; recuperarse en un lapsus de tiempo en el que se vea comprometido el servicio; y evolucionar para cambiar las funciones y las capacidades con el fin de rediseñar las estrategias, a fin de minimizar los impactos negativos de los ciberataques reales o previstos.*

2. En fecha 5 de agosto de 2021, el Consejo Directivo del **INDOTEL** mediante la Resolución núm. 082-2021 colocó en consulta pública el **REGLAMENTO DE CIBERSEGURIDAD PARA LA PRESTACIÓN DEL SERVICIO DE ACCESO A INTERNET,** cuyo dispositivo reza textualmente de la siguiente forma:

> **PRIMERO: ORDENAR** el inicio del proceso de Consulta Pública para dictar el **"REGLAMENTO DE CIBERSEGURIDAD PARA LA PRESTACIÓN DEL SERVICIO DE ACCESO A INTERNET",** cuyo texto se encuentra anexo a la presente resolución, formando parte integral de la misma.
>
> **SEGUNDO: ORDENAR** a la Dirección Ejecutiva la publicación de la parte dispositiva de esta resolución en un periódico de amplia circulación nacional, inmediatamente a partir de lo cual deberá estar a disposición de los interesados en las oficinas del **INDOTEL**, ubicadas en la primera planta del Edificio Osiris, situado en la Avenida Abraham Lincoln núm. 962, de esta ciudad de Santo Domingo de Guzmán, Distrito Nacional, así como en la página Web que mantiene esta institución en la red de Internet, en la dirección www.indotel.gob.do.
>
> **TERCERO: DISPONER** un plazo de treinta (30) días calendario, contados a partir de la fecha de la publicación de la parte dispositiva de la presente Resolución en un periódico de amplia circulación nacional, para que los interesados presenten las observaciones y comentarios que estimen convenientes al **"REGLAMENTO DE CIBERSEGURIDAD PARA LA PRESTACIÓN DEL SERVICIO DE ACCESO A**

INTERNET", que conforma el anexo de esta Resolución, al tenor de las previsiones del artículo 93 de la Ley General de Telecomunicaciones, núm. 153-98

PÁRRAFO I: Los comentarios y las observaciones a los que hace referencia la parte capital del presente ordinal deberán ser depositados en formato papel y electrónico redactados en idioma español, dentro del plazo anteriormente establecido, en las oficinas del **INDOTEL**, ubicadas en el Edificio Osiris, marcado con el número 962 de la Avenida Abraham Lincoln de esta ciudad de Santo Domingo de Guzmán, Distrito Nacional, Capital de la República Dominicana, de lunes a viernes, en horario de 8:30 a.m. a 4:00 P.M.; o dirigidos al correo electrónico Consultapublica@indotel.gob.do, indicando en el asunto el número de la presente resolución.

PÁRRAFO II: Vencido el plazo de treinta (30) días calendario establecido en este ordinal "Tercero", no se recibirán más observaciones o comentarios y no se concederán prórrogas.

3. En fecha 18 de agosto de 2021, fue publicado un extracto de la Resolución núm. 082-2021 en el periódico "*Listín Diario*" con la indicación de que el texto completo se encontraba disponible en el sitio Web del **INDOTEL.**

4. Que, en ese sentido, conforme se indica precedentemente, durante el período de consulta pública habilitado por este Consejo Directivo fueron recibidos comentarios no vinculantes por parte de: **AENOR DOMINICANA S. R. L., 5G AMÉRICAS, BANCO CENTRAL DE LA REPÚBLICA DOMINICANA, ALTICE DOMINICANA, S. A. (ALTICE), COMPAÑÍA DOMINICANA DE TELÉFONOS, S. A. (CLARO), ONEMAX, S. A.** y **TRILOGY DOMINICANA, S. A. (VIVA)**, los cuales han sido debidamente ponderados por este Consejo Directivo, y cuyas consideraciones al respecto son presentadas en el cuerpo de la presente Resolución.

5. El 27 de agosto de 2021, **AENOR DOMINICANA S. R. L.,** remitió al **INDOTEL** sus observaciones a dicha propuesta regulatoria a través del correo electrónico marcado con el número de correspondencia 224816, firmada por Ariel Espejo Combes.

6. Posteriormente, en fecha 7 de septiembre de 2021, fueron recibidas, las observaciones realizadas por **5G AMÉRICAS**, firmado por su VP CALA, José F. Otero, marcado con el número de correspondencia 225375.

7. En fecha 7 de septiembre de 2021, el **INDOTEL**, con el objetivo de presentar el **REGLAMENTO DE CIBERSEGURIDAD PARA LA PRESTACIÓN DEL SERVICIO DE ACCESO A INTERNET,** se realizó la primera Mesa Técnica de Ciberseguridad del sector de las Telecomunicaciones, luego de haber recibido las observaciones al Reglamento puesto en consulta pública, para mejorar la ciberseguridad del sector de las telecomunicaciones, con la participación de los representantes del **INDOTEL**, **CENTRO NACIONAL DE CIBERSEGURIDAD** y las prestadoras de servicio de acceso a Internet **ALTICE DOMINICANA, S. A. (ALTICE), COMPAÑÍA DOMINICANA DE TELÉFONOS, S. A. (CLARO)**, **TRILOGY DOMINICANA, S. A. (VIVA), WIND TELECOM, S. A. (WIND), CAPCANATEL, S.A (CAPCANATEL), GOLD DATA DOMINICANA, S.A.S.**

8. El 17 de septiembre de 2021, fueron recibidos en las oficinas del **INDOTEL** los comentarios y observaciones realizados por el **BANCO CENTRAL DE LA REPÚBLICA DOMINICANA**, firmados por su Gobernador, Héctor Valdez Albizu, mediante correspondencia marcada con el número 225968.

9. Adicionalmente, el 20 de septiembre de 2021, la prestadora **ALTICE DOMINICANA, S. A. (ALTICE)** depositó en el **INDOTEL** sus observaciones a dicha propuesta regulatoria a través de la comunicación núm. 226002, firmada por su Gerente Regulatorio Desirée Escoto Sánchez.

10. En fecha 20 de septiembre de 2021, fueron recibidos en las oficinas del **INDOTEL** los comentarios y observaciones realizados por parte de **COMPAÑÍA DOMINICANA DE TELÉFONOS, S. A. (CLARO),** firmados por su director Regulatorio, Robinson Peña Mieses, mediante correspondencia marcada con el número 226004.

11. Asimismo, el 20 de septiembre de 2021, se recibieron los comentarios a la citada Resolución núm. 082-2021, por parte de la Prestadora **ONEMAX**, **S. A.,** firmados por su Gerente General Manuel Enrique Tavares Navarro, mediante correspondencia marcada con el número 226003.

12. Finalmente, el 20 de septiembre de 2021, fueron recibidos en las oficinas del **INDOTEL** los comentarios y observaciones realizados por parte de **TRILOGY DOMINICANA, S. A. (VIVA),** firmados por su Abogada apoderada, Paola Díaz Tejeda, mediante correspondencia marcada con el número 226005.

13. En fecha 27 de octubre de 2021, fue publicado un aviso en el periódico "*Listín Diario*" haciendo de público conocimiento la convocatoria de audiencia pública de la Resolución del Consejo Directivo núm. 082-2021, a ser celebrada en fecha 4 de noviembre de 2021 en el Salón Multiusos del **INDOTEL**, con el objetivo de que los interesados presentaren de manera verbal ante el **INDOTEL** los comentarios y observaciones realizados por escrito a la citada Resolución, referentes al "**REGLAMENTO DE CIBERSEGURIDAD PARA LA PRESTACIÓN DEL SERVICIO DE ACCESO A INTERNET**".

14. El 4 de noviembre del presente año, fue celebrada en el Salón Multiusos del Quinto (5º) piso del **INDOTEL**, ubicado en la Avenida Abraham Lincoln núm. 962, Edificio Osiris, la audiencia pública previamente indicada, con la presencia de los representantes de **TRILOGY DOMINICANA, S.A. (VIVA), COMPAÑÍA DOMINICANA DE TELÉFONOS, S. A. (CLARO)**, **ALTICE DOMINICANA, S. A. (ALTICE), BANCO CENTRAL DE LA REPÚBLICA DOMINICANA, GRUPO BURGOS** y **CENTRO NACIONAL DE CIBERSEGURIDAD (CNCS),** durante la cual **VIVA, ALTICE** y **CLARO** expusieron los argumentos depositados en detalle vía los escritos referidos en los párrafos que anteceden.

15. En fecha 10 de noviembre de 2021, el **INDOTEL** realizó la segunda Mesa Técnica de Ciberseguridad del sector de las Telecomunicaciones, con la participación de los representantes del **CENTRO NACIONAL DE CIBERSEGURIDAD** y las prestadoras de servicio de acceso a Internet **ALTICE DOMINICANA, S. A. (ALTICE), COMPAÑÍA DOMINICANA DE TELÉFONOS, S. A. (CLARO)**, **WIND TELECOM, S. A. (WIND), TRILOGY DOMINICANA, S. A. (VIVA) y ONEMAX, S. A.**

II. Examen de la competencia del órgano regulador y consideraciones de Derecho

16. Considerando que la Constitución de la República Dominicana dispone en su artículo 147 la finalidad de los servicios públicos, estableciendo que esta radica en la satisfacción de las necesidades de interés colectivo, y disponiendo en su numeral 3 que "La regulación de los servicios públicos es facultad exclusiva del Estado. La Ley podrá establecer que la regulación de estos servicios y de otras actividades económicas se encuentren a cargo de organismos creados para tales fines".

17. De conformidad con el precitado artículo 147 de la Carta Magna, el Estado por medio de la Ley General de Telecomunicaciones, núm. 153-98, ha delegado en el **Instituto Dominicano de las Telecomunicaciones (INDOTEL)** la regulación y supervisión del desarrollo de los servicios públicos de telecomunicaciones en nuestro país.

18. Por su parte, la Ley General de Telecomunicaciones, núm. 153-98, constituye el marco regulatorio básico aplicable en todo el territorio nacional para la instalación, mantenimiento, operaciones de redes, prestación de servicios y la provisión de equipos de telecomunicaciones; estatuto legal que es complementado con los reglamentos que dicte el **INDOTEL** al respecto.

19. Conforme al mandato de la Constitución de la República y de la Ley General de Telecomunicaciones, núm. 153-98, el **INDOTEL**, en nombre del Estado debe regular y mantener la vigilancia en la prestación de los servicios públicos, asegurando la correcta, efectiva, eficaz y continua prestación de los servicios públicos de telecomunicaciones, garantizando mayores estándares de calidad, igualdad, servicio universal y transparencia en la contratación y prestación de estos servicios.

20. Que, sin embargo, la responsabilidad de hacer cumplir dichos principios no solo recae sobre el órgano regulador, sino también que es una obligación de los concesionarios responsables de la prestación de los servicios públicos de telecomunicaciones, de acuerdo al artículo 30 de dicha Ley núm.153-98.

21. Adicionalmente, en lo que respecta a la Ley núm. 172-13 sobre la protección integral de los datos personales, la misma tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados. En el artículo 5 reconoce como parte de sus principios rectores de esta materia los principios de Seguridad y Deber de Secreto. Disponiendo que el responsable del archivo de datos personales deberán adoptar e implementar las medidas de índole técnica, organizativa y de seguridad necesarias para salvaguardar los datos de carácter personal y eviten su alteración, pérdida, tratamiento, consulta o acceso no autorizado, así como que el responsable del archivo de datos personales y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del archivo de datos personales o, en su caso, con el responsable del mismo, salvo que sea relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública.

22. La Resolución del Consejo Directivo del **INDOTEL**, núm. 129-06, que aprueba la Norma de Calidad de Servicio y Seguridad de la Red, de aplicabilidad a todas las redes de servicios

públicos de telecomunicaciones, analógicas o digitales, que operan las prestadoras de servicios portadores, servicios finales y servicios de valor agregado, establece los parámetros, mediciones y niveles de satisfacción, que se obligan a cumplir. Además, contiene disposiciones que regulan aspectos de la calidad de servicio y la seguridad de las redes, que garantiza la disponibilidad del servicio.

23. Asimismo, la Resolución del Consejo Directivo del **INDOTEL,** núm. 033-2020, que dicta el Reglamento General del Servicio de Acceso a Internet, tiene como objetivo regular las relaciones entre las Prestadoras de Servicio Público de Acceso a Internet y sus clientes y usuarios, para la prestación del servicio. En ese sentido, el artículo 9 del referido reglamento al hacer referencia a las obligaciones de las prestadoras señala en su numeral 5 y 6 que las prestadoras del servicio de acceso a Internet tendrán la obligación del implementar medidas que garanticen la seguridad e integridad de las comunicaciones y que protejan a los usuarios del servicio de acceso a Internet de ataques y afecciones al servicio, de conformidad con las recomendaciones de la serie X del UIT-T, de manera particular las recomendaciones X.800, X.805, X.1121 y X.1122 y de tomar medidas y planes de mejoras ante vulnerabilidades de su red o del servicio, de formas esenciales aquellas identificadas por el **INDOTEL** o el **CENTRO NACIONAL DE CIBERSEGURIDAD**.

24. Por su parte, el Decreto Presidencial núm. 230-18 mediante el cual se establece la Estrategia Nacional de Ciberseguridad, en el Pilar núm. 2 sobre Protección de Infraestructuras Críticas Nacionales e Infraestructuras de tecnologías de la información (TI) del Estado, establece en su objetivo general: Asegurar el continuo funcionamiento y la protección de la información almacenada en las infraestructuras críticas nacionales e infraestructuras TI relevantes del Gobierno. En tal sentido, cada órgano regulador debe definir, en coordinación con su sector, las acciones de lugar para mejorar la ciberresiliencia de las infraestructuras tecnológicas.

25. Que, de igual forma, el Objetivo 2 de ese mismo pilar establece como meta elaborar e implementar un plan de robustecimiento de la seguridad de las infraestructuras críticas nacionales y de las infraestructuras TI relevantes del Gobierno y de los servicios colaterales que las soportan, frente a las amenazas cibernéticas. Así en la línea de acción 2.2 de dicho objetivo se establece "Analizar, mejorar e implementar las normas emitidas por los entes reguladores correspondientes" y la línea de acción 2.3 se establece "Implementar los esquemas de gobernabilidad que permitan la supervisión y evaluación adecuada de infraestructuras críticas nacionales y de las infraestructuras TI relevantes del Gobierno".

26. Que finalmente, la Estrategia Nacional de Ciberseguridad les atribuye a los entes reguladores de los operadores de las infraestructuras críticas establecer mecanismos de seguridad a sus regulados para anticipar, resistir, recuperarse y evolucionar frente a condiciones adversas, como los ataques contra los recursos de información o tecnológicos.

27. Que tal y como hemos podido observar en los párrafos que sirvieron de motivación para la aprobación de la citada resolución del Consejo Directivo núm. 082-2021, el citado **REGLAMENTO DE CIBERSEGURIDAD PARA LA PRESTACIÓN DEL SERVICIO DE ACCESO A INTERNET** como objetivo establecer las normas que deben cumplir las empresas prestadoras de servicio público de telecomunicaciones e internet para asegurar la continuidad del servicio a los usuarios, de manera que las mismas implementen los procedimientos para la anticipación de los incidentes de cibernéticos, la resistencia para minimizar los efectos de los mismos cuando se produzcan, tomar las medidas de recuperación necesarias y evolucionar hacia la consolidación de un nivel óptimo de ciberseguridad.

28. En este sentido, el literal "b" del artículo 84 de la Ley núm. 153-98, expresamente establece entre las funciones del Consejo Directivo del **INDOTEL** "*dictar reglamentos de alcance general y normas de alcance particular, dentro de las reglas y competencias fijadas por la presente ley y manteniendo el criterio consultivo de las empresas prestadoras de los diversos servicios públicos regulados y de sus usuarios*".

29. Asimismo, la precitada Ley núm. 153-98, establece en su artículo 78 que son: "*Funciones del órgano regulador, dictar normas técnicas que garanticen la compatibilidad técnica, operativa y funcional de las redes públicas de telecomunicaciones, la calidad mínima del servicio y la interconexión de redes. Dichas normas se adecuarán a las prácticas internacionales y a las recomendaciones de los organismos internacionales de que forme parte la República Dominicana*".

30. Que el artículo 23 de la Ley General de Libre Acceso a la Información Pública, núm. 200-04, señala que: "*Las entidades o personas que cumplen funciones públicas o que administran recursos del Estado tienen la obligación de publicar a través de medios oficiales o privados de amplia difusión, incluyendo medios o mecanismos electrónicos y con suficiente antelación a la fecha de su expedición, los proyectos de regulaciones que pretendan adoptar mediante reglamento o actos de carácter general, relacionadas con requisitos o formalidades que rigen las relaciones entre los particulares y la administración o que se exigen a las personas para el ejercicio de sus derechos y actividades".*

31. Que, de igual forma, el artículo 31 de la Ley sobre los Derechos de las Personas en sus Relaciones con la Administración y de Procedimiento Administrativo, núm. 107-13, establece como principios del procedimiento aplicable para la elaboración de reglamentos; (i) la audiencia de los ciudadanos afectados en sus derechos e intereses y la (ii) la participación del público.

32. Que el artículo 93.1 de la Ley General de Telecomunicaciones núm. 153-98 establece que, *antes de dictar resoluciones de carácter general, el órgano regulador deberá consultar a los interesados, debiendo quedar constancia escrita de la consulta y sus respuestas*.

33. Visto lo precedentemente señalado, este Consejo Directivo tiene el deber de ponderar los comentarios que ha recibido con ocasión de la puesta en consulta pública de ***"*REGLAMENTO DE CIBERSEGURIDAD PARA LA PRESTACIÓN DEL SERVICIO DE ACCESO A INTERNET"**, contenida en su Resolución núm. 082-2021 de fecha 5 de agosto de 2021.

34. En este sentido, conforme se indica anteriormente, durante el período de consulta pública habilitado por este Consejo Directivo, se recibieron comentarios no vinculantes por parte de: **AENOR DOMINICANA S. R. L., 5G AMÉRICAS, BANCO CENTRAL DE LA REPÚBLICA DOMINICANA, ALTICE DOMINICANA, S. A. (ALTICE), COMPAÑÍA DOMINICANA DE TELÉFONOS, S. A. (CLARO), ONEMAX, S. A.,** y **TRILOGY DOMINICANA, S. A. (VIVA)**, los cuales han sido debidamente ponderados por este Consejo Directivo, y cuyas consideraciones al respecto son presentadas en el cuerpo de la presente Resolución.

35. Que, a continuación, se presentan de manera sucinta las observaciones y comentarios expuestos por los interesados, los cuales luego de su justa ponderación y pausado análisis, han conducido a que este Consejo Directivo adopte modificaciones sobre la propuesta original, que parten estrictamente de las observaciones recibidas, las cuales se incorporan en la parte dispositiva de esta resolución.

III. Comentarios recibidos de las Partes y motivación del INDOTEL

Consideraciones a los argumentos generales presentados sobre la Resolución del Consejo Directivo núm. 082-2021

36. Que, el **BANCO CENTRAL DE LA REPÚBLICA DOMINICANA,** de manera general sobre la indicada propuesta regulatoria en su escrito de observaciones, señala lo siguiente:

> *[...] tomando en consideración los trabajos que se han ejecutado en conjunto entre nuestras instituciones (Banco Central e INDOTEL), es por lo que entiendo prudente, salvo su distinto parecer, coordinar reuniones entre los técnicos de ambas instituciones, donde se aclaren y armonicen los aspectos contenidos en los dos reglamentos citados en esta comunicación (Reglamento de Ciberseguridad para el Sistema Financiero y de Pagos y Reglamento de Ciberseguridad para la Prestación del Servicio de Acceso a Internet), que pudiesen estar en contraposición con las acciones ya ejecutadas en esta materia, tanto por nosotros como reguladores, como por parte de nuestros respectivos regulados. Damos constancia, mediante esta comunicación, que tenemos observaciones de fondo sobre el documento puesto en consulta.*
>
> *Finalmente, deseo expresar (Gobernador del Banco Central dixit) que hacemos esta sugerencia, ya que entiendo, al igual que usted, que el diálogo franco es la mejor herramienta para apoyar el avance de nuestro país, y que, para ese fin, es importante que los reguladores de los distintos sectores proyecten una imagen de colaboración y alineación, tal como el Honorable Presidente de la República, Luis Abinader, expresó en el reciente lanzamiento de la Agenda Digital 2030, y tal como siempre ha sido entre el INDOTEL y el Banco Central de la República Dominicana.*

37. Que, por su parte la prestadora de servicios públicos de telecomunicaciones, **ALTICE** en sus argumentos iniciales destaca lo transcrito a continuación:

> *Finalmente, a modo general solicitamos, tomen en consideración los siguientes puntos: Que se establezcan Mesas Técnicas de Trabajo en las que se puedan:*
>
> *a. Buscar consenso para los criterios de acción, funciones y responsabilidades de las partes, de cara a las diferentes iniciativas que hoy existen, algunas en fase de implementación, otras en fase de conceptualización.*
>
> *b. Tratar los diferentes aspectos y entregables esperados por el regulador de suerte que se tenga la oportunidad de hacer los ajustes necesarios para proveer las informaciones y se establezca visibilidad de los canales de comunicación y el flujo de las mismas entre las partes interesadas.*
>
> *c. Desarrollar las plantillas y forma de recolección de los datos para la reportería que se estaría implementando una vez aprobado el Reglamento, de suerte que se nos permita la oportunidad de revisar y solicitar aclaraciones o mejoras que sean de utilidad del sector telecomunicaciones, previo a la entrada en vigencia.*

Estas conversaciones tienen que ser sostenidas previo a que se decida aprobar la nueva Norma, para poder contar con la posibilidad de plasmar en ellas los ajustes que se tengan a bien convenir durante las labores de las Mesas.

Que junto con la publicación de la resolución que dicte el nuevo Reglamento, y con el fin de la correcta implementación de los reportes, sean puestas en circulación las plantillas para la presentación de los reportes correspondientes.

38. Que, por su parte, **AENOR**, tiene a, bien señalar en su escrito lo siguiente:

Como acciones concretas, se pueden considerar las certificaciones basadas en normas internacionales de resiliencia y continuidad de negocio, como la ISO 22301 y la norma de Calidad Seguridad y Continuidad, en los servicios de TI como la ISO/IEC 20000-1.

39. En este mismo sentido **AENOR** solicita *Incluir el posible reconocimiento de la norma/estándar ISO 27001 como referente internacional de mejores prácticas para la ciberseguridad*.

40. Que en torno a lo expresado por el **BANCO CENTRAL DE LA REPÚBLICA DOMINICANA**, se sostuvo una reunión entre su equipo técnico y el **INDOTEL**, en la cual no expresaron las diferencias de fondo con la propuesta regulatoria, sino más bien externaron su deseo de colaborar con **INDOTEL** desde su Equipo de Respuesta a Incidentes Cibernéticos.

41. Que, sobre lo señalado por **ALTICE**, con la participación de todos los que presentaron interés durante el proceso de consulta pública de la Resolución del Consejo Directivo núm. 082-2021, fueron celebradas dos Mesas Técnicas de Ciberseguridad del sector de las Telecomunicaciones, los días 7 de septiembre y 10 de noviembre del presente año, en las cuales el equipo técnico del **INDOTEL** respondió y atendió a las dudas y requerimientos de las Partes interesadas, logrando un consenso en torno a las disposiciones del "**REGLAMENTO DE CIBERSEGURIDAD PARA LA PRESTACIÓN DEL SERVICIO DE ACCESO A INTERNET**".

42. Que respecto a los reportes que deben ser presentados, el **INDOTEL** implementará una plataforma donde las prestadoras podrán acceder y realizar sus reportes de incidentes de ciberseguridad y métricas de manera eficiente y segura. Esto le permitirá a la institución un seguimiento eficiente y rápido acceso a métricas de incidentes de ciberseguridad y disponibilidad.

43. Sobre lo solicitado por **AENOR**, este Consejo Directivo entiende prudente aclarar que el reglamento anexo a la presente resolución está basado en recomendaciones de la UIT como referente y organismo internacional especializado de las Naciones Unidas para las tecnologías de la información y la comunicación, así como estándares y mejores prácticas de otros organismos internacionales (NIST, IETF, 3GPP, CITEL, entre otros). La UIT trabajó conjuntamente con ISO en el desarrollo de sus recomendaciones, como, por ejemplo, la Recomendación UIT-T X.1051, que define las categorías de controles de seguridad para telecomunicaciones, o de forma más específica, el código de prácticas en materia de controles de seguridad de la información basados en la serie de normas ISO/CEI 27000 para organizaciones de telecomunicaciones. Por tanto, este Consejo Directivo del **INDOTEL** entiende no pertinente acoger la solicitud de **AENOR** debido a que el sector de normalización de la Unión

Internacional de las Telecomunicaciones (UIT-T) en sus recomendaciones de ciberseguridad ha tomado como marco las citadas normas ISO con un enfoque al sector telecomunicaciones.

Consideraciones a los argumentos presentados sobre el artículo 1. Objeto y artículo 2. Ámbito de aplicación

44. Que, sobre el artículo 1, en su escrito **CLARO** argumenta lo transcrito a continuación:

> *La regulación de la ciberseguridad debe incluir a todos los actores que, de una u otra manera, pueden afectar el funcionamiento de los sistemas de información e infraestructuras soportadas por las tecnologías de la información y comunicación. En ese sentido, es propicio incluir también en el objeto y el alcance de esta norma a los revendedores del servicio de Internet y a cualquier tercero que disponga de cualquier tipo de título habilitante para proveer estos servicios de telecomunicaciones, así como también a los usuarios del servicio de Internet (cuando aplique), para crear las condiciones que permitan exigir a estos un nivel de cumplimiento y responsabilidad adecuado, así como de colaboración con la protección del ciberespacio. Para lograr esto, sugerimos modificar tanto el objeto como el alcance de la norma, para incluir a los terceros que proveen servicios de Internet y al usuario del servicio (cuando aplique) en la contribución y apego al buen uso del servicio de Internet, para lograr un ciberespacio seguro y disminuir los riesgos de afectación de la ciberseguridad. De igual modo, conocido es por todos que ni las prestadoras, ni los organismos e instituciones de prevención y combate de la delincuencia pueden garantizar la infalibilidad de los sistemas, sino más bien la aplicación de medidas de prevención y gestión de su funcionamiento. Es por esta razón que, luego de analizar y comparar otros textos sobre el tema, sugerimos la siguiente variación en la definición del objeto y el alcance:*
>
> ***Artículo 1.- Objeto.*** *Este Reglamento tiene por objeto establecer medidas de alcance general, que servirán de base a las prestadoras de servicios de acceso a internet,* ***así como a los revendedores y cualquier otro tercero que provea los servicios de acceso a internet, y de apego en el uso del servicio de Internet a los usuarios, para la prevención, gestión y respuestas a las amenazas e incidentes de ciberseguridad, que permitan*** *el continuo funcionamiento de los sistemas de información, proporcionar las salvaguardas necesarias a las infraestructuras soportadas por las tecnologías de la información y comunicación, como también asegurar la integridad, disponibilidad y confidencialidad de la información que se transmite, almacena y/o procesa a través y/o por medio de estas infraestructuras.*

45. Que, por su parte la Prestadora de Servicios Públicos de Telecomunicaciones **ALTICE** sobre el citado artículo 1, argumenta en su escrito de comentarios, lo que a continuación se transcribe:

> *Se requiere la revisión del alcance del objetivo, considerando, en la ciberseguridad intervienen otros actores distintos de las prestadoras de servicio, como, por ejemplo: proveedores de soluciones tecnológicas para empresas y particulares, que incluyen, pero no se limitan a integración, configuración y programación de*

equipos y softwares, también están los revendedores de internet, los propios usuarios finales, entre otros.

Por otro lado, la referencia a "proporcionar las salvaguardas necesarias a las infraestructuras soportadas por las tecnologías de la información y comunicación" es una obligación amplia, y ambigua, pues no crea un límite definido de nuestra responsabilidad como prestadora de servicios, considerando que las amenazas pueden originarse en las infraestructuras y o facilidades de los usuarios finales, como las redes internas de bancos, de entidades de gobierno, etc., y afectar nuestra red, situación que escapar de nuestro control.

*El reconocimiento e identificación de todos los entes que tienen potencial de incidir en la ciberseguridad deben ser identificados en el reglamento y definida su responsabilidad. Sin esto, solo se está protegiendo una parte de l*a red.

46. Que, finalmente sobre este mismo artículo, **ONEMAX** observa lo siguiente:

Conforme lo establecido por el órgano regulador en este artículo, a nuestro parecer el objeto planteado en el Reglamento es muy amplio, es imposible que un operador de servicios pueda cumplir con todo lo establecido en el mismo, pues la responsabilidad del operador es y debe ser siempre sobre lo que pasa sobre su red.

Es importante señalar, que en el proceso para la prestación del servicio hay otros agentes activos, situaciones externas importantes en la transmisión del internet como red de redes, que son determinantes para garantizar el funcionamiento continuo del servicio y para la salvaguarda necesaria de lo que corresponde a la transmisión y que se encuentran fuera del control directo del prestador.

En tal sentido, en lo que respecta a este artículo, el regulador debe delimitar el objeto del reglamento, tomando en consideración las particularidades requeridas para la prestación del servicio, las acciones de los demás agentes que intervienen y que escapan de las obligaciones del prestador de servicio, y debe crear obligaciones particulares propias y específicas para el prestador.

47. Que en lo referente al artículo 2, la Prestadora de Servicios Públicos de Telecomunicaciones **CLARO,** tiene a bien exponer en sus observaciones, los argumentos siguientes:

El presente Reglamento…. Servicios de acceso a internet, ***así como a los revendedores y cualquier otro tercero que provea los servicios de acceso a internet, y el cumplimiento y apego de los usuarios del servicio con el buen uso de este.*** *En tal virtud, son de aplicación para las prestadoras de servicios públicos de acceso a internet,* ***así como a los revendedores y cualquier tercero que provea los servicios de acceso a Internet****, de manera independiente de su participación en el mercado,* ***y para los usuarios del servicio.***

El presente Reglamento establece las disposiciones generales por las cuales ha de regirse la gobernanza de ciberseguridad, para orientar los procesos

> *organizacionales de las prestadoras de servicios públicos de telecomunicaciones, específicamente las que prestan servicios de acceso a internet,* ***así como a los revendedores y cualquier otro tercero que provea los servicios de acceso a internet, y el cumplimiento y apego de los usuarios del servicio con el buen uso de este.*** *En tal virtud, son de aplicación para las prestadoras de servicios públicos de acceso a internet,* ***así como a los revendedores y cualquier tercero que provea los servicios de acceso a Internet,*** *de manera independiente de su participación en el mercado,* ***y para los usuarios del servicio.***

48. Que **ALTICE** en sus observaciones respecto al artículo 2 , señala lo siguiente:

> *El presente Reglamento establece las disposiciones generales por las cuales ha de regirse la gobernanza de ciberseguridad* ***de los que prestan servicios de acceso a internet****. En tal virtud, son de aplicación para todas las* ***personas físicas o jurídicas que comercializan, proveen, configuran o instalan facilidades y servicios para el acceso a internet. Siendo esto una realidad innegable, se requiere la revisión del ámbito de aplicación para reflejar la inclusión de otros actores.***

49. Que sobre lo expresado en sus respectivos escritos por las Prestadoras de Servicios Públicos de Telecomunicaciones **CLARO, ALTICE** y **ONEMAX**, es importante aclarar que para los casos de adquisición de equipos de telecomunicación, software, plataformas y servicios Cloud, el reglamento en sus artículos 29 y 30 plantea las obligaciones y las normas a cumplir para la contratación o compra a proveedores externos o terceros. En consecuencia, no se hace necesario hacer estos señalamientos.

50. Que, en otro orden, este Consejo considera válido el señalamiento que realizan tanto **CLARO** como **ALTICE** y **ONEMAX** de que se debe definir el alcance del reglamento, porque a pesar de que las infraestructuras críticas están soportadas por el servicio de acceso a internet, las prestadoras no administran y tampoco tienen responsabilidad sobre esta. No obstante, este Consejo Directivo debe aclarar que cualquier eventualidad en materia de ciberseguridad sobre el servicio de acceso a internet y su infraestructura es responsabilidad de la prestadora. La responsabilidad de la prestadora se extiende hasta el punto de terminación de sus redes (conforme lo indica el artículo 10.2 de la Ley General de Telecomunicaciones núm. 153-98), que no siempre es el punto de acceso del usuario. Es cierto que algunas amenazas pueden originarse del lado usuario, pero dicho límite ya está definido en la Ley.

51. Por otro lado, es importante señalar que, durante la celebración de la segunda mesa técnica de ciberseguridad, las Partes llegaron a un consenso sobre lo que sería la inclusión de las definiciones de Prestador(a) y Prestador(a) de Infraestructura activa de Telecomunicaciones, las cuales contemplan los diferentes tipos de proveedores o agentes que pueden estar involucrados en la prestación del servicio de internet. Por lo que las mismas serán incluidas en la versión final del indicado Reglamento que se aprueba mediante el presente acto administrativo.

Consideraciones a los argumentos presentados sobre el artículo 3. Definiciones

52. Que, en relación al artículo 3, tenemos que señalar que **CLARO**, expresa en sus comentarios, lo siguiente:

*Para mayor precisión se sugiere modificar el término "**Incidente**", colocándole "**Incidente de Ciberseguridad**". Adicionalmente en la definición eliminar la parte de "(…) o **inminentemente pueda tener un efecto adverso"**; Esto para evitar un error de interpretación por parte del sector respecto a incidentes de seguridad (con impacto perceptible comprobado) o bien riesgos de seguridad (eventos de alta probabilidad de ocurrencia sin impacto perceptible).*

*Sugerimos la siguiente variación en la definición del concepto **Incidente**:*

***Incidente de Ciberseguridad:** es todo evento que tenga un efecto adverso sobre la ciberseguridad de un sistema de información o la información que es procesada, almacenada o transmitida por el mismo, constituya una violación a las políticas de seguridad o procedimientos de ciberseguridad vigentes o de las políticas de uso aceptable.*

53. Que, por su parte, **ALTICE,** argumenta lo transcrito a continuación:

Sugerimos usar la definición de amenaza establecida en la parte introductoria del reglamento, entendemos esta es más apegada al concepto de amenaza y vulnerabilidad, a saber:

***Amenaza** es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. Es decir, que podría tener un potencial efecto negativo sobre algún elemento de nuestros sistemas. Las amenazas pueden proceder de ataques (fraude, robo, virus), sucesos físicos (incendios, inundaciones) o negligencia y decisiones institucionales (mal manejo de contraseñas, no usar cifrado). Desde el punto de vista de una organización pueden ser tanto internas como externas.*

***Vulnerabilidad** (en términos de informática) es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de esta, por lo que es necesario encontrarlas y eliminarlas lo antes posible.*

Sugerimos además que se considere sustituir el término de prestadora de servicio, por uno más inclusivo, que reúna a todas las personas, físicas o jurídicas, que de alguna forma provee servicios de acceso, configuración, programación e instalación de acceso a redes públicas y privadas para el acceso a internet.

54. Que, sobre la sugerencia de **CLARO** respecto a la definición de incidente, este Consejo Directivo estima pertinente acoger lo sugerido, por lo que los cambios serán reflejados en la versión final del Reglamento que se aprueba mediante la presente resolución.

55. Que respecto a lo solicitado por **ALTICE** este órgano regulador considera no procedente los cambios sugeridos sobre las definiciones de Amenaza y Vulnerabilidad en el entendido que estos son términos y definiciones que están basados en las recomendaciones y estándares de los referidos organismos internacionales. Ahora bien, en lo que respecta a la definición de Prestadora, tal y como expusimos anteriormente, en la celebración de la segunda mesa técnica

de ciberseguridad se llegó a un conceso sobre la misma, por lo que será incluida en la versión final del Reglamento.

Consideraciones a los argumentos presentados sobre el artículo 4. Marco de trabajo y gobernanza.

56. Que, sobre lo dispuesto en el artículo 4, **CLARO** tiene a bien argumentar lo transcrito a continuación:

> *En este capítulo I del título II, asumimos que sin proponérselo ni que sea la intención de los redactores de la propuesta reglamentaria, se ha colado una ligera intención de intromisión en aspectos organizativos y administrativos interno, propio de las empresas y que pretenden, de alguna manera, establecer lineamientos de administración de la estructura y organigrama de las prestadoras.*
>
> *Sobre el particular, es importante recordar que la responsabilidad sobre el cumplimiento regulatorio recae sobre la prestadora como ente jurídico, y no sobre una área, departamento, dirección o gerencia interna de la entidad, por lo que no es propio de un reglamento disponer en qué área, departamento, dirección o gerencia interna de los regulados debe recaer el cumplimiento de la regulación a dictar; así como tampoco el grado o nivel de las competencias que deben tener los empleados internos.*
>
> *En ese sentido, debe referirse, más bien, a los aspectos generales y a las exigencias de ese cumplimiento por parte de los regulados, dejando en libertad a las empresas de establecer sus estructuras internas y el nivel de preparación y competencias de sus recursos humanos para responder a las obligaciones frente a la regulación exigible a la empresa.*
>
> *Es por esta razón que sugerimos la siguiente variación en este capítulo I del título II:*
>
> ***Artículo 4.- Marco de trabajo y gobernanza.*** *Las prestadoras de servicios de acceso a internet deben contar con una estructura organizacional definida para desempeñar las funciones de ciberseguridad dentro de la entidad y velar por el cumplimiento de lo dispuesto en el presente Reglamento.*
>
> ***Párrafo I****. Las prestadoras de servicios de acceso a internet deben contar con un Comité de Ciberseguridad encargado de garantizar e impulsar la gestión de ciberseguridad, y dirigir el plan de estrategia de ciberseguridad en la organización. El Comité de Ciberseguridad debe estar conformado por áreas estratégicas para el desarrollo* ***y cumplimiento*** *de la ciberseguridad en la organización.*
>
> ***Párrafo II****. La estructura organizacional de ciberseguridad de las prestadoras de servicio acceso a internet, debe contar con un Equipo de Respuesta ante Incidentes de Seguridad Cibernética, encargado de gestionar los reportes de incidentes y coordinar las acciones de respuesta ante los mismos.*
>
> ***Párrafo III. El representante designado por la prestadora de servicio de acceso a Internet, en su*** *estructura organizacional de ciberseguridad, debe mantener una comunicación continua con la Dirección de Ciberseguridad,*

Comercio Electrónico y Firma Digital del INDOTEL para el tratamiento de temas como:

a. Seguimiento a los *planes* de mejoras;

b. Intercambio de información e inteligencia sobre ciberseguridad;

c. Esfuerzos en conjunto orientados a la promoción de una cultura de ciberseguridad; y

d. Cumplimiento de lo dispuesto en el presente Reglamento.

57. Que, sobre el particular, **ALTICE** tiene a bien sugerir en su escrito lo siguiente:

El alcance de este artículo debe ser revisado o bien eliminado, la estructura organizacional y operativa de las empresas no es objeto ni materia de regulación, por tanto, las disposiciones de este artículo transgreden las facultadas del regulador.

58. Que, sobre este mismo artículo, **ONEMAX**, tiene a bien tomar en consideración en su escrito de argumentos lo siguiente:

Siguiendo con el estudio del referido Reglamento, y haciendo referencia a lo textualmente indicado en el título ll, luego de citado, más abajo indicamos lo siguiente:

*Es una preocupación para **ONEMAX, S.A**., como entidad comercial, el planteamiento realizado sobre la estructura organizacional de la empresa impuesta por el INDOTEL en este artículo 4, de manera específica, en lo señalado en el párrafo I, sobre la no dependencia del área de ciberseguridad de las áreas organizacionales establecidas. A nuestro entender el regulador está actuando fuera de lo establecido en la Ley General de Telecomunicaciones y que de manera exclusiva marca su competencia.*

Conviene señalar, que la organización estructural de una empresa es una función administrativa que constituye un factor importante en el buen funcionamiento de la misma, ayudando a alcanzar las metas u objetivos fijados.

Por ello, es importante entender que dicha estructura organizacional se realiza tomando como parámetros muchos aspectos en consideración, cuya variación repercute de manera directa en el quehacer de la empresa. Estructurar e integrar unidades orgánicas es una responsabilidad de la empresa en base a los recursos disponibles y posibles.

*Por lo que es necesario, y es lo planteado por **ONEMAX, S.A.**, al respecto, que cada empresa conforme su estructura establecida, su presupuesto, su modo de operación, sus necesidades, decida el orden de jerarquía que dará a esa estructura de ciberseguridad que implementa el REGLAMENTO DE CIBERSEGURIDAD PARA LA PRESTACIÓN DEL SERVICIO DE ACCESO A INTERNET.*

59. Que en lo referente al artículo 4, **5G AMÉRICAS**, tiene a bien exponer en sus observaciones, los argumentos siguientes:

> *5G Américas sugiere considerar hacer más específico el alcance del párrafo de este artículo para los operadores de red móvil, ya que el proyecto de reglamento menciona que la función de ciberseguridad de las prestadoras de servicio de acceso a internet debe estar segregada de las funciones de gestión y operación de las redes. Esta sugerencia se realiza en función de que la arquitectura de redes 5G integra funciones de red que se consideran aptas para ayudar en labores de ciberseguridad y protección de la integridad de redes.*
>
> *Las redes 5G se diseñan como arquitectura basada en servicios (SBA) que soporta funciones "cloud native", desagregación, segmentación de secciones de la red, software abierto y que incorpora plenamente la automatización y los conceptos de SDN y NFV. El 3GPP ha generado estándares para redes 5G enfocándose en mejorar la protección de elementos como la confidencialidad de la información, integridad de la red, autenticación y aislamiento de elementos de la red, considerando las vulnerabilidades futuras, pero también las relacionadas con la operación de redes 3G y 4G, que convivirán con las redes 5G por lo menos de manera transitoria.*
>
> *En este sentido, la seguridad para los proveedores de acceso a internet por medio de redes móviles sugiere la importancia de tener una relación con las áreas de gestión operativa de las redes. Concretamente, la capacidad de network slicing (definida en el estándar TS 23.501 del 3GPP) se está tornando en una de las funciones de ciberseguridad más visibles para las redes 5G (y para la mayoría de sus casos de uso), ya que en términos simplificados es la habilidad que tienen estas redes para configurar y administrar de manera automatizada múltiples redes lógicas que operen virtualmente como independientes, aunque compartan una misma infraestructura física. En la práctica, esto equivale a la segmentación de una red móvil de manera virtual en porciones que pueden ser asignadas a diferentes fines o servicios, como una red privada.*
>
> *La capacidad de network slicing es distinta a las redes provadas virtuales o VPN: network slicing implica aislamiento de punta a punta de una porción de la red, incluyendo la red de acceso radioeléctrica (RAN), la red de transporte y el núcleo de la red; los VPN se implementan encima de una capa de recursos físicos de red.*

60. Durante la celebración de la segunda mesa técnica de ciberseguridad las Partes llegaron a un consenso sobre el artículo 4. En ese sentido, el equipo técnico de**l INDOTEL** explicó que se debe mantener la creación de la estructura de ciberseguridad y el principio de independencia. No obstante, se flexibilizará el hecho de que las empresas coloquen la estructura donde entiendan correcto, a pesar de que la tendencia de la industria y las buenas prácticas plantean que la estructura de ciberseguridad no se reporte a las áreas donde trazan directamente políticas y controles.

61. Con respecto al comentario realizado por **5G AMÉRICAS,** el reglamento explica en el artículo 4, párrafo I, la segregación de las funciones de ciberseguridad con respecto a la gestión y operación de las redes o tecnología en las Prestadoras de Servicio de Acceso a Internet. Aunque

sus funciones estén segregadas existe una colaboración mutua entre las gerencias, esto se basa en los estándares y mejores prácticas.

Consideraciones a los argumentos presentados sobre el artículo 5. Política de ciberseguridad

62. Que **CLARO** en sus observaciones respecto al artículo 5, señala lo siguiente:

> ***Artículo 5.- Política de ciberseguridad****. Las prestadoras de servicios de acceso a internet,* ***así como los revendedores y cualquier otro tercero que provea los servicios de acceso a internet,*** *deben establecer…. de las comunicaciones, informaciones y privacidad de sus usuarios.*
>
> ***Comentario y Propuesta:*** *Modificación propuesta en función del comentario introducido en el artículo 1.*

63. Que, sobre la observación anterior, este Consejo Directivo entiende pertinente acoger parcialmente la misma en virtud de las modificaciones realizadas al artículo 1, viéndose los cambios reflejados en la versión final del Reglamento que se aprueba mediante la presente resolución.

64. Que así mismo sobre el párrafo del citado artículo, **CLARO** argumenta lo transcrito a continuación:

> ***Comentario y Propuesta:*** *Consideramos importante delimitar o definir las terceras partes, a los fines de que no se preste a confusión con respecto a quiénes pueden tener acceso a esta información, cuyo manejo correcto puede incidir en el éxito o fracaso de las previsiones de ciberseguridad dispuestas por las prestadoras de servicio de acceso a Internet. Una tercera parte interesada puede ser un tercero cualquiera que no tenga nada que aportar o que pida conocer la política de seguridad para saber por dónde atacar las infraestructuras de las prestadoras de servicio de acceso a Internet.*
>
> *Sugerimos la siguiente variación en este párrafo del artículo 5:*
>
> ***Párrafo.*** *La política de ciberseguridad debe ser de conocimiento general por parte de todo el personal de la organización, así como de terceras partes* ***facultadas por las leyes y los reglamentos y*** *con incidencia en la* ***regulación, gestión y control de la*** *ciberseguridad. Debe estar alineada con los objetivos de negocio, los requisitos legales y regulatorios, el entorno de las amenazas y las tendencias tecnológicas de la industria.*

65. El Consejo Directivo estima no pertinente la observación realizada por **CLARO**, y, en consecuencia, no acoge la misma, debido a que entendemos que deben ser las mismas Prestadoras que tienen el deber de identificar las terceras partes interesadas o facultadas según sus políticas de ciberseguridad para recibir o tener acceso a dicha información.

Consideraciones a los argumentos presentados sobre el artículo 7. Capacitación sobre ciberseguridad

66. Que, en relación al artículo 7, tenemos que señalar que **CLARO**, expresa en sus comentarios, lo siguiente:

> *El artículo 6 de esta norma ya establece disposiciones sobre la gestión del riesgo. Dispone este artículo el "qué hacer" y el "cómo hacerlo". Ahora bien, en lo que se dispone aquí en este artículo 7, entendemos que se extralimita en cuanto a lo que puede ordenársele hacer a las prestadoras. Estas disposiciones, de manera indirecta, se adentran en mandatos respecto al manejo interno del personal de las empresas, cuando sólo deben disponer sobre el cumplimiento y preservación de la ciberseguridad y la responsabilidad de las empresas respecto ante faltas o violaciones.*
>
> *Para que las empresas cumplan con la preservación de la ciberseguridad, no es necesario un programa de capacitación a todo el personal, bastaría con tener políticas claras y orientación respecto del personal que no trabaja directamente con la ciberseguridad, y la capacitación o actualización en el tema no es necesario que este dentro de la empresa y tampoco aplicar los entrenamientos o preparación a todo el personal de la empresa.*
>
> *La inversión en la que tendría que incurrir la empresa para entrenamientos y capacitación al personal completo sería inmanejable, en términos de costos. Del mismo modo, lo dispuesto en el literal C de este artículo 7, es inaplicable. Cargar a las empresas prestadoras de servicios de acceso a Internet con la responsabilidad de entrenar a terceras partes interesadas es un despropósito (fíjense en el ejemplo: prestadoras, clientes y socios). Ese literal C debe ser eliminado de la propuesta. ¿Es entendible ofrecer orientación al respecto, pero entrenamientos?*
>
> *Sugerimos la siguiente variación en el texto del artículo 7:*
>
> ***Artículo 7.- Capacitación sobre ciberseguridad.** Las prestadoras de servicios de acceso a internet deben establecer y mantener un programa y **políticas** de **orientación** sobre ciberseguridad con el objetivo de **orientar** al personal, asociados y usuarios en la protección de los sistemas y activos de tecnología de información y comunicación de la organización, el manejo adecuado de los datos y la aplicación de salvaguardas ante las amenazas relevantes, así como el cumplimiento con las regulaciones aplicables. El programa **y la política** debe contemplar, como mínimo, los siguientes aspectos:*
>
> *a. **Orientación** para personal de nuevo ingreso en **el proceso de inducción**, así como **refrescamiento** regular o a raíz de cambios en la organización y el entorno que puedan afectar el grado de exposición ante las amenazas de ciberseguridad. **Este proceso de orientación cotidiana también aplicará a** usuarios finales, representantes de servicio al cliente y personal de nivel ejecutivo.*
>
> *b. Entrenamiento especializado para grupos específicos dentro de la organización, tales como **los integrantes de la estructura organizacional de ciberseguridad y el Equipo de Respuesta ante Incidentes de Seguridad Cibernética,** administradores de sistemas, desarrolladores de software, operadores; que abarque tópicos de ciberseguridad relevantes a cada grupo y las medidas de*

protección ante diversas amenazas, tales como Phising, ingeniería social, técnicas de programación segura, gestión de vulnerabilidades técnicas, respuesta ante incidentes, protección contra software malicioso, entre otros.

*c. **Orientación** a terceras partes interesadas (por ejemplo, clientes, socios), sobre las principales medidas ante amenazas relevantes tales como Phising, ingeniería social, protección de los medios de autenticación, notificación y respuesta ante los incidentes, entre otros aspectos.*

67. Que, por su parte, **AENOR,** señala que *sería interesante definir el contenido mínimo de los talleres a impartir, tanto al personal nuevo como los talleres recurrentes o, en su defecto, contemplar el establecimiento de una cantidad mínima de horas anuales.*

68. Que, sobre este mismo artículo, **5G AMÉRICAS**, tiene a bien tomar en consideración en su escrito de argumentos lo siguiente:

Se sugiere considerar una definición más específica en torno a la clasificación de personal de nuevo ingreso que debe ser capacitado en materia de ciberseguridad, ya que el inciso es ambiguo en este sentido y pueden existir cargos laborales en los que no se justifique una capacitación con respecto a esta clase de temas, dependiendo de sus funciones dentro de la organización.

69. Que sobre lo externado por **CLARO** y **5G AMÉRICAS** en el literal b), este Consejo Directivo entiende pertinente mantener la idea central sobre el entrenamiento de ciberseguridad, pero siendo más específicos en la redacción del artículo 7, en el sentido de que el entrenamiento especializado a que se hace referencia deberá ser impartido al personal de acuerdo a sus funciones y al área en que laboren. En tal virtud, este Consejo Directivo acoge parcialmente lo planteado por **CLARO** sobre los literales a, b y c, y se estarán reflejando dichos cambios en la versión final del reglamento que se aprueba en el presente acto.

70. Que, sobre lo expresado por **AENOR** en su escrito de comentarios, este Consejo Directivo entiende no pertinente las observaciones realizadas, en el sentido de que el artículo 7 define puntualmente los grupos que deben capacitarse, en adición a los temas que se deben tratar debido a que no todas las Prestadoras de Servicio de Acceso a Internet tienen el mismo nivel de madurez en ciberseguridad, por lo tanto, no se puede establecer un tiempo específico para las capacitaciones.

Consideraciones a los argumentos presentados sobre el artículo 9. Gestión de activos

71. Que, sobre el artículo 9, **CLARO** tiene a bien argumentar lo transcrito a continuación:

Comentario y Propuesta: *Es importante aclarar, en cuantos equipos en las premisas del cliente (CPE), que, como se indica al principio, se trata de equipos tecnológicos de la prestadora. No es posible para la prestadora inventariar o mantener un control de los equipos propios del cliente o adquiridos por su cuenta y manejados por estos. Sugerimos la siguiente modificación al texto:*

Párrafo I. *Las prestadoras de servicios de acceso a internet deben establecer y mantener un inventario exhaustivo y actualizado de todos los activos tecnológicos de la entidad, incluyendo servidores, dispositivos de usuario final (tales como*

*portátiles y móviles), elementos de red (incluyendo elementos core, de distribución y acceso), equipos en las premisas del cliente (CPE), dispositivos IoT, entre otros, **pertenecientes a la prestadora.***

72. Que el Consejo Directivo entiende pertinente acoger la sugerencia planteada por **CLARO**.

Consideraciones a los argumentos presentados sobre el artículo 10. Clasificación de los Datos.

73. Que, sobre el artículo 10 referente a la Clasificación de los datos, **CLARO** tiene a bien sugerir en su escrito lo siguiente:

> ***Artículo 10.- Clasificación de los datos.*** *Las prestadoras de servicios de acceso a internet, **así como los revendedores y cualquier otro tercero que provea los servicios de acceso a internet…**. o cuando ocurran cambios significativos en la empresa que puedan afectar esta medida.*
>
> ***Comentario y Propuesta:*** *Modificación propuesta en función del comentario introducido en el artículo 1.*

IV. Consideraciones a los argumentos presentados clasificación de los datos, artículo 11

74. Que, sobre el artículo 11 sobre Cumplimiento regulatorio, **CLARO**, tiene a bien tomar en consideración en su escrito de argumentos lo siguiente:

> ***Artículo 11.- Cumplimiento regulatorio.*** *Las prestadoras de servicios de acceso a internet, **así como los revendedores y cualquier otro tercero que provea los servicios de acceso a internet,** deben identificar… y el enfoque de la entidad para cumplir con estos requisitos.*
>
> ***Comentario y Propuesta:*** *Modificación propuesta en función del comentario introducido en el artículo 1.*

Consideraciones a los argumentos presentados cumplimiento regulatorio, artículo 12

75. Que, sobre el artículo 12 correspondiente a la Gestión de las identidades y el acceso, la Prestadora **CLARO** tiene a bien argumentar lo transcrito a continuación:

> ***Artículo 12.- Gestión de las identidades y el acceso.*** *Las prestadoras de servicios de acceso a internet, **así como los revendedores y cualquier otro tercero que provea los servicios de acceso a internet,** deben restringir el acceso físico y lógico… y los requisitos regulatorios y contractuales aplicables.*
>
> ***Comentario y Propuesta:*** *Modificación propuesta en función del comentario introducido en el artículo 1.*

Consideraciones a los argumentos presentados para la gestión de las identidades y el acceso, artículo 13

76. Que **CLARO**, sobre el artículo 13 referente a la Autenticación, en su escrito de comentarios señala lo que a continuación se transcribe:

> *Las prestadoras de servicios de acceso a internet, **así como los revendedores y cualquier otro tercero que provea los servicios de acceso a internet**, deben autenticar... deben abarcar, como mínimo, los siguientes aspectos:*
>
> ***Comentario y Propuesta:** Modificación propuesta en función del comentario introducido en el artículo 1*

Consideraciones a los argumentos presentados autenticación y artículo 15

77. Que sobre el artículo 15 sobre Seguridad y resiliencia de las redes, la Prestadora de Servicios Públicos de Telecomunicaciones **CLARO**, remitió sus observaciones, las cuales se transcriben a continuación:

> ***Artículo 15.- Seguridad y resiliencia de las redes.** Las prestadoras de servicios de acceso a internet, **así como los revendedores y cualquier otro tercero que provea los servicios de acceso a internet,** deben…, incluyendo, entre otras, las siguientes medidas:*
>
> ***Comentario y Propuesta:** Modificación propuesta en función del comentario introducido en el artículo 1.*
>
> ***Párrafo.** En adición a lo anterior, las prestadoras de servicios de acceso a internet, **así como los revendedores y cualquier otro tercero que provea los servicios de acceso a internet,** deben…, entre las que se encuentran:*
>
> ***Comentario y Propuesta:** Modificación propuesta en función del comentario introducido en el artículo 1.*

78. Que sobre las observaciones realizadas por **CLARO** precedentemente en torno a los artículos 10, 11, 12, 13 y 15 es importe señalar que durante la celebración de la segunda mesa técnica de ciberseguridad las Partes llegaron a un consenso sobre lo que sería la inclusión de las definiciones de Prestador(a) y Prestador(a) de Infraestructura Activa de Telecomunicaciones, por lo que las mismas serán incluidas en la versión final del indicado Reglamento que se aprueba mediante el presente acto administrativo.

Consideraciones a los argumentos presentados sobre los artículos 16 al 37

79. Que **CLARO** sobre los artículos 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 29, 31, 32, 33, 35, 36 y 37 solicitan la inclusión de la coletilla subrayada, para que se lea de la siguiente manera: "Las prestadoras de servicios de acceso a internet, así como los revendedores y cualquier tercero que provea los servicios de acceso a internet...".

80. Como se indicó previamente, este Consejo Directivo del **INDOTEL** tiene a bien acoger parcialmente la solicitud de **CLARO,** al entender que según se expresó en el numeral 51 de la presente resolución, sería la inclusión de las definiciones de Prestador(a) y Prestador(a) de Infraestructura activa de Telecomunicaciones, las cuales contemplan los diferentes tipos de proveedores o agentes que pueden estar involucrados en la prestación del servicio de internet.

Consideraciones a los argumentos presentados sobre el artículo 22. Gestión de vulnerabilidades

81. Que **VIVA** sobre el articulo 22 informa que tomando como punto de partida que la mayoría de las disposiciones consagradas en la Resolución constituyen elementos nuevos y no consignados en otras normas del sector y que conllevan una serie de adaptaciones que impactan significativamente al funcionamiento institucional de **VIVA,** entendemos que su entrada en vigencia amerita un plazo mayor en ciertos escenarios, razón por la cual proponemos sea dividido en dos (2) plazos que sean considerados de la siguiente manera: Para este caso proponen: Entrada en vigencia plazo de seis (6) meses.

82. En cuanto al comentario externado por **VIVA,** respecto de la entrada en vigencia del Reglamento. Este Consejo Directivo entiende pertinente la misma, y, por tanto, tiene a bien acoger parcialmente dicha solicitud. Sin embargo, deseamos puntualizar que tener dos plazos de entrada en vigencia para una pieza regulatoria puede prestarse a confusión para los sujetos regulados. En consecuencia, consideramos prudente otorgando un plazo de ocho (8) meses para la entrada en vigencia del reglamento, reflejando dicho cambio en la versión final del reglamento.

83. Con respecto a estos dos artículos (22 y 30), **5G AMÉRICAS** desea compartir algunas de las características de seguridad desarrolladas como parte de la estandarización de tecnología para redes 5G, para consideración del **INDOTEL**.

> *El Grupo SA3 del 3GPP he definido la arquitectura de seguridad para redes móviles 5G en la especificación TS 33.501, que incluye una estructura multidimensional en la que los operadores mantienen labores de monitoreo, partiendo de una premisa de riesgos continuos en el desarrollo de las redes. La evolución de la seguridad de la red se fundamenta en activar controles adecuados ante amenazas emergentes.*
>
> *En materia de autenticación, las redes 5G introducen funciones de protección en el plano del usuario, un elemento que no estaba presente en el diseño de redes móviles previas. Las técnicas de autenticación previstas para 5G mejoran las presentes en 4G desde áreas distintas, como con la adopción de un marco de autenticación unificado, por ejemplo. Las mejoras en protocolos y técnicas de autenticación también están diseñadas para mejorar la privacidad de la información de los usuarios, como se establece por ejemplo en la especificación TS 23.003 del 3GPP.*
>
> *Network Slicing es otra de las funcionalidades clave de seguridad de 5G por su capacidad para aislar de punta a punta una porción de la red. Se recomienda consultar el comentario al artículo 4 del proyecto expuesto previamente en esta carta.*
>
> *En la estandarización de 5G se observan beneficios de la adopción de software de código abierto, ya que esto permite a los operadores y fabricantes de tecnología trabajar con un entorno de desarrolladores más amplio que puede ayudar al personal con atribuciones de ciberseguridad dentro de las organizaciones. La revisión constante del software ayuda a mejorar su rendimiento y seguridad con la identificación y corrección constante de vulnerabilidades, creando un "repositorio*

confiable" que solo algunos desarrolladores confiables ("trusted developers") puede utilizar y modificar de manera directa. Este elemento es relevante conforme las redes van siendo definidas incrementalmente por software.

Para las redes 5G también se considera que la adopción de un modelo de seguridad "Zero-Trust" es adecuado por la incorporación de controles estrictos que incluye, por ejemplo, mejora en los procesos de encriptación para mitigar riesgos como el monitoreo por partes no autorizadas de dispositivos conectados. En este modelo es relevante la introducción de soluciones basadas en software y "nube". Para las redes móviles, este modelo se considera un complemento de la estrategia general que abarque la protección a infraestructura física más distribuida con ayuda de soluciones de virtualización. El modelo "Zero Trust" es relevante considerando sobre todo que los centros de datos de aplicaciones en uso en la República Dominicana pueden estar ubicados en otras jurisdicciones.

El énfasis de la industria de telecomunicaciones móviles en la seguridad ha sido un diferenciador muy importante con respecto a otras tecnologías inalámbricas. El uso de espectro bajo licencia y para uso exclusivo provee una capa adicional de protección contra el acceso sin consentimiento al tráfico de voz, video o datos.

84. Que este Consejo Directivo rechaza la solicitud de **5G AMÉRICAS** en virtud de que todo lo expuesto en este capítulo cuenta con las mejores prácticas de diferentes estándares internacionales. Las recomendaciones técnicas como la arquitectura de seguridad y/o herramientas tecnológicas de este reglamento no debe limitarse a una tecnología específica, sino que se debe de aplicar a todas las existentes.

Consideraciones a los argumentos presentados sobre el artículo 23. Gestión de eventos

85. Que **CLARO** sobre el artículo 23 solicita una modificación en función del comentario del artículo 1, en cuanto a la inclusión de la coletilla subrayada, para que se lea de la siguiente manera: Gestión de eventos. Las prestadoras de servicios de acceso a internet, *así como los revendedores y cualquier otro tercero que provea los servicios de acceso a internet*, deben producir, mantener…".

86. Que **VIVA** sobre el articulo 23 informa que "Tomando como punto de partida que la mayoría de las disposiciones consagradas en la Resolución constituyen elementos nuevos y no consignados en otras normas del sector y que conllevan una serie de adaptaciones que impactan significativamente al funcionamiento institucional de **VIVA**, entendemos que su entrada en vigencia amerita un plazo mayor en ciertos escenarios, razón por la cual proponemos sea dividido en dos (2) plazos que sean considerados de la siguiente manera: Para este caso proponen: Entrada en vigencia plazo de doce (12) meses.

87. En vista de lo indicado previamente en el numeral 82 de la presente Resolución, este Consejo Directivo del **INDOTEL** tiene a bien acoger parcialmente su solicitud, otorgando un plazo de ocho (8) meses para la entrada en vigencia del reglamento.

Consideraciones a los argumentos presentados sobre el artículo 24. Gestión de amenazas de ciberseguridad

88. Que sobre el artículo 24, **AENOR** solicita considerar las ISO 270001 – Seguridad de la Información como normas internacionales que ayudan al cumplimiento de este artículo. Y **CLARO** informa que, a los fines de evitar confusión, respecto a la entrega de la información a entregar, es importante indicar el tipo de información a entregar en los reportes. En ese sentido, sugerimos la siguiente enmienda en la redacción del literal (e): (e) Capacidad para reportar y compartir, tanto a nivel interno como externo, información *técnica y codificada (como por ejemplo direcciones IP) e* inteligencia sobre las amenazas e incidentes de ciberseguridad detectados.

89. Sobre lo solicitado por **AENOR**, este Consejo Directivo entiende prudente aclarar que el reglamento anexo a la presente resolución está basado en recomendaciones de la UIT como referente y organismo internacional especializado de las Naciones Unidas para las tecnologías de la información y la comunicación, así como estándares y mejores prácticas de otros organismos internacionales (NIST, IETF, 3GPP, CITEL, entre otros). La UIT trabajó conjuntamente con ISO en el desarrollo de sus recomendaciones, como, por ejemplo, la Recomendación UIT-T X.1051, que define las categorías de controles de seguridad para telecomunicaciones, o de forma más específica, el código de prácticas en materia de controles de seguridad de la información basados en la serie de normas ISO/CEI 27000 para organizaciones de telecomunicaciones. Por tanto, este Consejo Directivo del **INDOTEL** entiende no pertinente acoger la solicitud de **AENOR** debido a que el sector de normalización de la Unión Internacional de las Telecomunicaciones (UIT-T) en sus recomendaciones de ciberseguridad ha tomado como marco las citadas normas ISO con un enfoque al sector telecomunicaciones; y sobre la solicitud de **CLARO** este Consejo Directivo entiende pertinente acoger la redacción sugerida al literal e) de este articulo 24.

Consideraciones a los argumentos presentados sobre el artículo 25. Inteligencia sobre amenazas de ciberseguridad

90. Que sobre este articulo 25, **VIVA** por su parte informa que tomando como punto de partida que la mayoría de las disposiciones consagradas en la ***Resolución*** constituyen elementos nuevos y no consignados en otras normas del sector y que conllevan una serie de adaptaciones que impactan significativamente al funcionamiento institucional de **VIVA**, entendemos que su entrada en vigencia amerita un plazo mayor en ciertos escenarios, razón por la cual proponemos sea dividido en dos (2) plazos que sean considerados de la siguiente manera: Para este caso proponen: Entrada en vigencia plazo de seis (6) meses.

91. En vista de lo indicado previamente en el numeral 82 de la presente Resolución, este Consejo Directivo del **INDOTEL** tiene a bien acoger parcialmente su solicitud, otorgando un plazo de ocho (8) meses para la entrada en vigencia del reglamento.

Consideraciones a los argumentos presentados sobre los artículos 26, 27, 29 y **30**

92. Que sobre los artículos 26, 27, 29 y 30 la empresa **VIVA** informó que tomando como punto de partida que la mayoría de las disposiciones consagradas en la ***Resolución*** constituyen elementos nuevos y no consignados en otras normas del sector y que conllevan una serie de adaptaciones que impactan significativamente al funcionamiento institucional de **VIVA**, entendemos que su entrada en vigencia amerita un plazo mayor en ciertos escenarios, razón por la cual proponemos plazo de doce (12) meses.

93. En vista de lo indicado previamente en el numeral 82 de la presente Resolución, este Consejo Directivo del **INDOTEL** tiene a bien acoger parcialmente su solicitud, otorgando un plazo de ocho (8) meses para la entrada en vigencia del reglamento.

Consideraciones a los argumentos presentados sobre el artículo 26. Gestión de incidentes

94. **VIVA** informa que respecto al párrafo I y II del Artículo 26, entendemos necesario, que sea incluida la mención expresa relación al proceso de notificación a las partes interesadas e identificar taxativamente contra quien procede ejercer ese deber de comunicación, con la finalidad de evitar confusiones futuras y concentrar en el presente reglamento todas las disposiciones relativas al tema de incidentes y relacionados, pues su lectura resulta ambigua, debiéndose plasmar el mecanismo que se debe llevar a cabo para proceder con la notificación a terceros.

95. Que **CLARO** sobre el artículo 26 entiende que, para cuidar el éxito en el manejo del incidente, en términos legales y procesales, sugerimos la siguiente modificación al texto: **Párrafo II.** Los procedimientos de manejo de incidentes deben incluir procedimientos de investigación forense *y cumplimiento con el debido proceso de ley*, para una debida adquisición, preservación, análisis y documentación de la evidencia digital que sirva de apoyo a las acciones de remediación, disciplinarias y/o legales en torno al incidente.

96. Este Consejo Directivo decide no acoger la solicitud de **VIVA** en virtud de que las buenas prácticas de gestión de incidentes establecen que se debe establecer comunicación con las áreas afectadas e interesadas sean de carácter interno. En ese sentido, consideramos oportuno señalar que deben ser las Prestadoras quienes identifiquen en base a sus políticas de ciberseguridad a cuáles tipos de actores debe notificar. Es importante que no se debe confunda esta etapa de comunicación con la obligación de reporte a las instituciones del Estado que se plantea en el reglamento. Finalmente, vale la pena indicar que este artículo no hace referencia reportes externos sobre incidentes de ciberseguridad.

97. Que, sobre esta solicitud de **CLARO,** este órgano regulador tiene a bien acoger la solicitud del reglamento, en la versión final del reglamento, agregándole la coletilla “y cumplimiento con el debido proceso de ley”.

Consideraciones a los argumentos presentados sobre el artículo 30. Seguridad en ambientes de nube

98. Que sobre el artículo 30, **AENOR** informa por su parte que se consideren también la ISO 27001 – Seguridad de la Información, 27017/27018 como normas internacionales de seguridad y privacidad en la nube como normas internacionales que ayudan al cumplimiento de este artículo.

99. Que sobre este mismo artículo **5G AMÉRICAS**, informo sobre lo siguiente:

> *“5G Américas desea compartir algunas de las características de seguridad desarrolladas como parte de la estandarización de tecnología para redes 5G, para consideración del **INDOTEL**.*
>
> *El Grupo SA3 del 3GPP he definido la arquitectura de seguridad para redes móviles 5G en la especificación TS 33.501, que incluye una estructura multidimensional en la que los operadores mantienen labores de monitoreo, partiendo de una premisa de riesgos continuos en el desarrollo de las redes. La*

evolución de la seguridad de la red se fundamenta en activar controles adecuados ante amenazas emergentes.

En materia de autenticación, las redes 5G introducen funciones de protección en el plano del usuario, un elemento que no estaba presente en el diseño de redes móviles previas. Las técnicas de autenticación previstas para 5G mejoran las presentes en 4G desde áreas distintas, como con la adopción de un marco de autenticación unificado, por ejemplo. Las mejoras en protocolos y técnicas de autenticación también están diseñadas para mejorar la privacidad de la información de los usuarios, como se establece por ejemplo en la especificación TS 23.003 del 3GPP.

Network Slicing es otra de las funcionalidades clave de seguridad de 5G por su capacidad para aislar de punta a punta una porción de la red. Se recomienda consultar el comentario al artículo 4 del proyecto expuesto previamente en esta carta.

E*n la estandarización de 5G se observan beneficios de la adopción de software de código abierto, ya que esto permite a los operadores y fabricantes de tecnología trabajar con un entorno de desarrolladores más amplio que puede ayudar al personal con atribuciones de ciberseguridad dentro de las organizaciones. La revisión constante del software ayuda a mejorar su rendimiento y seguridad con la identificación y corrección constante de vulnerabilidades, creando un "repositorio confiable" que solo algunos desarrolladores confiables ("trusted developers") puede utilizar y modificar de manera directa. Este elemento es relevante conforme las redes van siendo definidas incrementalmente por software.*

Para las redes 5G también se considera que la adopción de un modelo de seguridad "Zero-Trust" es adecuado por la incorporación de controles estrictos que incluye, por ejemplo, mejora en los procesos de encriptación para mitigar riesgos como el monitoreo por partes no autorizadas de dispositivos conectados. En este modelo es relevante la introducción de soluciones basadas en software y "nube". Para las redes móviles, este modelo se considera un complemento de la estrategia general que abarque la protección a infraestructura física más distribuida con ayuda de soluciones de virtualización. El modelo "Zero Trust" es relevante considerando sobre todo que los centros de datos de aplicaciones en uso en la República Dominicana pueden estar ubicados en otras jurisdicciones.

El énfasis de la industria de telecomunicaciones móviles en la seguridad ha sido un diferenciador muy importante con respecto a otras tecnologías inalámbricas. El uso de espectro bajo licencia y para uso exclusivo provee una capa adicional de protección contra el acceso sin consentimiento al tráfico de voz, video o datos".

100. Este Consejo Directivo del **INDOTEL** sobre el comentario de **5G AMÉRICAS** informa que todo lo expuesto en este capítulo cuenta con las mejores prácticas de diferentes estándares internacionales. Sin embargo, sus recomendaciones técnicas como la arquitectura de seguridad y/o herramientas tecnológicas donde el reglamento no debe limitarse a una tecnología específica, sino que se debe de aplicar a todas las existentes.

101. Sobre el comentario de **AENOR**, este Consejo Directivo entiende prudente aclarar que el reglamento anexo a la presente resolución está basado en recomendaciones de la UIT como referente y organismo internacional especializado de las Naciones Unidas para las tecnologías de la información y la comunicación, así como estándares y mejores prácticas de otros organismos internacionales (NIST, IETF, 3GPP, CITEL, entre otros). La UIT trabajó conjuntamente con ISO en el desarrollo de sus recomendaciones, como, por ejemplo, la Recomendación UIT-T X.1051, que define las categorías de controles de seguridad para telecomunicaciones, o de forma más específica, el código de prácticas en materia de controles de seguridad de la información basados en la serie de normas ISO/CEI 27000 para organizaciones de telecomunicaciones. Por tanto, este Consejo Directivo del **INDOTEL** entiende no pertinente acoger la solicitud de **AENOR** debido a que el sector de normalización de la Unión Internacional de las Telecomunicaciones (UIT-T) en sus recomendaciones de ciberseguridad ha tomado como marco las citadas normas ISO con un enfoque al sector telecomunicaciones.

Consideraciones a los argumentos presentados sobre el artículo 31. Gestión de la privacidad

102. Que sobre el artículo 31, la empresa **VIVA** informa que:

> *Con las disposiciones que abarca el presente artículo el **INDOTEL** incurre en establecer obligaciones, que corresponden al ejercicio de redacción de una Ley especial a tales fines, que proteja íntegramente los datos personales de las personas (nótese que en nuestro ordenamiento tenemos la Ley 172-13); haciendo un ejercicio de comparación, esto lo constituye el Reglamento General de Protección de Datos en la Unión Europea.*
>
> *Así que, ante la aplicación de este texto estaríamos ante escenarios tales como: tratamiento de datos, categoría de datos, un eventual responsable del tratamiento de los datos y encargado de tratamiento, lo que, a su vez, genera una serie de medidas que las prestadoras deben tomar para evitar un tratamiento ilícito de los datos personales de sus usuarios, pues el simple hecho de informar al interesado constituye la creación de una base legitimadora.*
>
> *Aparte de que se estarían creando nuevos derechos, tales como el derecho a la portabilidad de datos y derecho a la limitación del tratamiento, que una vez asumidos tendríamos que generar información sobre el impacto técnico y económico de esos derechos, así como implantar controles y auditorías para que sean garantizados; así como modificaciones en los contratos, aplicando cláusulas de protección, formularios, etc. Por lo que a juicio de VIVA este artículo contempla extralimitaciones claras con lo pretendido, por tanto, sugerimos su eliminación.*

103. Sobre el artículo 31 **AENOR** informa que se pude considerar la ISO 27701 de gestión de la privacidad como una norma que ayuda al cumplimiento de este artículo.

104. Sobre la solicitud de **VIVA** este Consejo Directivo, entiende que no procede y no es necesario la redacción de una ley; en este orden sobre lo planteado por **AENOR**, este organismo rector informa que el reglamento está basado en varios estándares y sus mejores prácticas, en caso de fundamentarlo en una norma específica podrían causar desacuerdos a las Prestadoras de Servicio de Acceso a Internet que tengan otras normas aplicadas, por lo anterior, este Consejo Directivo del **INDOTEL** tiene a bien rechazar los pedimentos realizados.

Consideraciones a los argumentos presentados sobre el artículo 32. Continuidad del Servicio

105. Que sobre el artículo 32, la empresa **VIVA** establece que:

> Tomando como punto de partida que la mayoría de las disposiciones consagradas en la ***Resolución*** constituyen elementos nuevos y no consignados en otras normas del sector y que conllevan una serie de adaptaciones que impactan significativamente al funcionamiento institucional de **VIVA**, entendemos que su entrada en vigencia amerita un plazo mayor en ciertos escenarios, razón por la cual proponemos sea dividido en dos (2) plazos que sean considerados de la siguiente manera: Para este caso proponen: Entrada en vigencia plazo de doce (12) meses.

106. Que al respecto de este artículo 32, **AENOR** informa que se puede considerar la ISO 22301 de gestión de continuidad de negocio o ISO20000-1 Gestión de Servicios de TI, como normas internacionales que ayudan al cumplimiento de este artículo. Y **CLARO** solicita la inclusión de "revendedores o terceros", deben contar con un plan robusto de acción frente a incidentes de alto impacto o desastres que pongan en riesgo la continuidad de servicios esenciales de telecomunicaciones.

107. Este Consejo Directivo del **INDOTEL** tiene a bien acoger parcialmente la solicitud de **VIVA,** otorgando un plazo de 8 meses, por otro lado, y rechaza la solicitud de **AENOR** de conformidad a lo externado previamente por este órgano regulador; y, por otro lado, decida acoger parcialmente la solicitud de **CLARO**, reflejando los cambios en la versión final del reglamento.

Consideraciones a los argumentos presentados sobre el artículo 33. Revisión independiente de ciberseguridad

108. Que sobre el artículo 33, **ALTICE** sugiere revisar el alcance de la figura del Auditor Externo, considerando que carece de valor o sentido, tener esta figura, si el **INDOTEL** se reserva la facultad de ordenar que la auditoría sea repetida. Igualmente, cualquier objeción a la auditoria debe ser justificada, motivada y sustentada, los motivos no pueden ser subjetivos. En todo caso, si el informe tiene algún aspecto no satisfactorio debidamente sustentado, lo que procede es que se requiera la rectificación del punto objetado o bien que se presente las evidencias de cumplimiento de éste. **VIVA** informa que tomando como punto de partida que la mayoría de las disposiciones consagradas en la Resolución constituyen elementos nuevos y no consignados en otras normas del sector y que conllevan una serie de adaptaciones que impactan significativamente al funcionamiento institucional de **VIVA,** entendemos que su entrada en vigencia amerita un plazo mayor en ciertos escenarios, razón por la cual proponemos sea dividido en dos (2) plazos que sean considerados de la siguiente manera: Para este caso proponen: Entrada en vigencia plazo de doce (12) meses. **AENOR** informa que además de las auditorías técnicas que se indican, además de tener de referencia OWSASP, NIST, se puede considerarse la norma internacional ISO 27001 de seguridad de la información. Además, sería interesante contemplar que aquellas organizaciones que cuenten con una certificación internacional en la Norma ISO 27001 (Seguridad de la Información), ISO 27017/27018 (Seguridad en la nube), ISO 27701 (gestión de la privacidad), podrían estar exentas de otras auditorías adicionales. Sería interesante poder definir los criterios de las firmas de auditorías a ser autorizadas por el **INDOTEL.**

109. Este Consejo Directivo del **INDOTEL** acoge parcialmente las consideraciones expuestas por la prestadora, y en consecuencia decide eliminar los párrafos II y III, así como la coletilla "y que hayan sido autorizados previamente" en virtud de que no eran coherentes con lo que planteaba el artículo para las revisiones independientes de ciberseguridad.

Consideraciones a los argumentos presentados sobre el artículo 35. Reporte de incidentes de ciberseguridad

110. Que sobre el artículo 35, **CLARO** solicita la siguiente inclusión:

> **Párrafo I.** En tal virtud, las prestadoras, revendedores o terceros, tienen que reportar detalladamente sobre los incidentes de ciberseguridad que detecten en sus redes y aplicaciones, que alcance los umbrales de gravedad establecidos en las instrucciones pertinentes emitidas por **INDOTE**L. Los detalles específicos de la información sobre los incidentes de ciberseguridad son establecidos por el **INDOTEL** a través de su Dirección de Ciberseguridad, Comercio Electrónico y Firma Digital.
>
> **Comentario y Propuesta:** Sugerimos especificar el plazo en el que debe ser enviado el informe indicado en el Párrafo V.
>
> **Párrafo IV.** Las prestadoras de servicios de acceso a internet, así como los revendedores y cualquier otro tercero que provea servicios de acceso a internet, están obligadas a notificar a las personas posiblemente afectadas por estos incidentes, o al público en general, si las personas afectadas no pueden ser notificadas individualmente, en un plazo no mayor a las setenta y dos (72) horas, contadas a partir de tener conocimiento sobre los mismos. En caso de incumplimiento, esta notificación podrá ser realizada al público en general por el INDOTEL y el CSIRT-RD.
>
> **Párrafo V.** Las prestadoras de servicios de acceso a internet, así como los revendedores y cualquier otro tercero que provea servicios de acceso a internet, están obligadas a enviar al **INDOTEL** y al CSIRT-RD del Centro Nacional de Ciberseguridad, en el mismo plazo indicado en el Párrafo IV, un informe sobre la respuesta y resolución del incidente. Este informe incluirá información sobre las causas del incidente de ciberseguridad, indicadores de compromiso, el tiempo dedicado a su resolución, las medidas aplicadas, el impacto del mismo y toda otra información que sea pertinente sobre el incidente.

111. Que sobre el artículo 35, **VIVA** solicita en el párrafo III que se elimine el término "… en el más breve plazo posible". En el párrafo IV solicita la eliminación del último párrafo que establece lo siguiente: "En caso de incumplimiento, esta notificación podrá ser realizada al público en general por el **INDOTEL** y el CSIRT-RD. En adición a lo dispuesto en el artículo 35 y sus párrafos, sugerimos la creación de una plataforma o página web donde cada prestadora tenga un sistema de estatus y se proporcione la información de la disponibilidad de los elementos de la red a fin de que el proceso de notificación de algún evento que degrade algunos de los servicios ofertados por la operadora, a fin de que los interesados estén enterados por dicha vía. Tomando como referencia otros países, como Australia.

112. Que en lo que respecta a este artículo 35, el planteamiento de **ONEMAX, S.A**., es el llamado al regulador sobre el plazo establecido para los reportes de incidentes de ciberseguridad, que deben realizar las prestadoras. El plazo que ha sido contemplado en el reglamento es un plazo sumamente corto, sin embargo, dejamos a la consideración del regulador para que en la reunión que hemos acordado realizar antes de la vista pública discutir un plazo razonable que permita que los prestadores de servicio podamos dar respuesta sobre la situación ocurrida y poder tomar acciones correctivas pertinentes.

113. Este Consejo Directivo del **INDOTEL** tiene a bien acoger parcialmente la solicitud de **CLARO** reflejando los cambios en la versión final del reglamento.

114. Este Consejo Directivo del **INDOTEL** tiene a bien acoger parcialmente la solicitud de **VIVA** sobre la eliminación de la coletilla “más breve”, porque en el párrafo III indican los tiempos de compromiso. Se rechaza la eliminación del párrafo IV, los usuarios tienen derecho a conocer si sus datos han sido comprometidos o la causa de la afectación de su servicio a internet. Sobre la creación de una plataforma web, este Consejo Directivo se encuentra evaluando dicha herramienta para su implementación, y las Prestadoras serán informadas en su debido momento para asegurar su cumplimiento con el reglamento.

115. Este Consejo Directivo del **INDOTEL** tiene a bien informar que la solicitud de **ONEMAX** se acoge, y se modificará los tiempos para la notificación de incidentes en la versión final del reglamento.

Consideraciones a los argumentos presentados sobre el artículo 36. Reporte de métricas

116. Que sobre el artículo 36, **VIVA** informa que tomando como punto de partida que la mayoría de las disposiciones consagradas en la ***Resolución*** constituyen elementos nuevos y no consignados en otras normas del sector y que conllevan una serie de adaptaciones que impactan significativamente al funcionamiento institucional de **VIVA**, entendemos que su entrada en vigencia amerita un plazo mayor en ciertos escenarios, razón por la cual proponemos sea dividido en dos (2) plazos que sean considerados de la siguiente manera: Para este caso proponen: Entrada en vigencia plazo de doce (12) meses.

117. Que en lo que respecta a los artículos 35 y 36, **ALTICE** informo lo siguiente:

> “Entendemos que este artículo debe ser revisado, nuestra obligación de reportería es con el **INDOTEL**, no presentamos oposición a que el **INDOTEL** comparta información pertinente, no confidencial y de manera segura con el CSIRT-RD o cualquier otra entidad autorizada, sin embargo, este doble reporte no es conveniente.
>
> Los tiempos para reportar deben contabilizarse a partir del momento en que la prestadora, toma conocimiento, es informada o confirma la existencia de un incidente. También se tiene que considerar que a priori la prestadora no necesariamente tiene visibilidad del nivel de criticidad, pues los eventos son dinámicos y pueden escalar o desescalar inadvertidamente”.

118. Este Consejo Directivo del **INDOTEL** tiene a bien acoger parcialmente la solicitud de **VIVA** reflejando los cambios en la versión final del reglamento.

119. El Consejo Directivo del **INDOTEL** tiene a bien acoger parcialmente la solicitud de **ALTICE** reflejando los cambios en la versión final del reglamento. Por tanto, las métricas de disponibilidad serán de consumo únicamente del **INDOTEL** y con respecto a la información de incidentes de ciberseguridad solo se reportará al **INDOTEL,** pero éste tendrá la potestad de compartir dicha información con cualquier otro Equipo de Respuesta a Incidentes Seguridad Cibernética que entienda pertinente.

Consideraciones a los argumentos presentados sobre el artículo 37. Sanciones

120. Sobre el artículo 37, **ONEMAX** externó que conforme el estudio realizado a la propuesta de Reglamento y analizando lo referido al régimen sancionador, argumentamos lo siguiente:

> A pesar de que la Ley General de Telecomunicaciones, núm. 153-98, en su Título III, artículos 108 y 109 se refiere a las sanciones y a los montos de las mismas respectivamente, es necesario que el regulador al referirse en este artículo 37 a la violación de las obligaciones esenciales establecidas en el Título ll del **REGLAMENTO DE CIBERSEGURIDAD PARA LA PRESTACIÓN DEL SERVICIO DE ACCESO A INTERNET**, establezca de manera clara y precisa la sanción que se ha de aplicar en caso de infringir el Reglamento. Esto así, debido a que en la forma en que se encuentra redactado dicho artículo 37, deja a la discrecionalidad la categorización de la sanción.
>
> Es de conocimiento que el artículo 109 de la Ley contiene tres categorías. En ese sentido, solicitamos al **INDOTEL** la modificación del artículo 37, para que de manera específica establezca la categoría de la falta que será aplicada en caso de violación a este Reglamento.

121. Que sobre la solicitud de **ONEMAX** al artículo 37, este Consejo Directivo entiende pertinente acogerla, reflejando los cambios en la versión final del reglamento. Las obligaciones esenciales de los concesionarios de servicio público de Telecomunicaciones a que hace referencia el Título II, están facultadas en base al artículo 30 de la Ley. El incumplimiento de estas condiciones esenciales será tipificado como faltas muy graves según queda establecido en el Art. 105 literal (N) de la Ley. Se acoge y debe modificarse el párrafo para indicar la falta (tipo y categoría).

V. Textos revisados

VISTA: La Constitución de la República Dominicana de fecha 13 de junio de 2015, en sus disposiciones citadas;

VISTA: La Ley General de Telecomunicaciones, núm. 153-98, de fecha 27 de mayo de 1998;

VISTA: La Ley sobre sobre los Derechos de las Personas en sus Relaciones con la Administración y de Procedimiento Administrativo, núm. 107-13, de fecha 6 de agosto de 2013;

VISTA: La Ley General de Libre Acceso a la Información Pública, núm. 200-04, del 28 de julio de 2004;

VISTA: La Ley sobre la protección integral de los datos personales, núm. 172-13, del 15 de diciembre de 2013;

VISTA: La resolución del Consejo Directivo del **INDOTEL**, núm. 129-06, que aprueba la Norma de Calidad de Servicio y Seguridad de la Red, del 1ro de agosto de 2006;

VISTO: El Decreto Presidencial núm. 230-18, de fecha 19 de junio de 2018;

VISTA: La resolución del Consejo Directivo del **INDOTEL**, núm. 033-20, que dicta el Reglamento General del Servicio de Acceso a Internet del 20 de mayo de 2020;

VISTAS: Las actas de las Mesas Técnicas celebradas en fechas 7 de septiembre y 10 de noviembre del presente año;

VISTO: El Documento de Análisis para formular el Reglamento de Ciberseguridad para el Sector de las Telecomunicaciones elaborado por la Dirección de Ciberseguridad, Comercio Electrónico y Firma Digital del **INDOTEL** del 20 de noviembre de 2020;

VISTOS: Los comentarios depositados por **AENOR DOMINICANA S. R. L., 5G AMÉRICAS, BANCO CENTRAL DE LA REPÚBLICA DOMINICANA, ALTICE DOMINICANA, S. A. (ALTICE), COMPAÑÍA DOMINICANA DE TELÉFONOS, S. A. (CLARO), ONEMAX** y **TRILOGY DOMINICANA, S. A. (VIVA),** en ocasión del proceso de Consulta Pública de la resolución del Consejo Directivo núm. 082-2021;

OÍDAS: La posición de las Partes interesadas en la audiencia pública efectuada el 4 de noviembre del presente año, en el Salón Multiusos del 5to piso del **INDOTEL.**

VI. Parte dispositiva:

EL CONSEJO DIRECTIVO DEL INSTITUTO DOMINICANO DE LAS TELECOMUNICACIONES (INDOTEL), EN EJERCICIO DE SUS FACULTADES LEGALES Y REGLAMENTARIAS,

RESUELVE:

PRIMERO: ACOGER parcialmente, los comentarios presentados por **AENOR DOMINICANA S. R. L., 5G AMÉRICAS, BANCO CENTRAL DE LA REPÚBLICA DOMINICANA, ALTICE DOMINICANA, S. A. (ALTICE), COMPAÑÍA DOMINICANA DE TELÉFONOS, S. A. (CLARO), ONEMAX** y **TRILOGY DOMINICANA, S. A. (VIVA)**, con ocasión del proceso de Consulta Pública iniciado mediante la Resolución núm. 082-2021 de este Consejo Directivo y **DICTAR** el "**EL REGLAMENTO DE CIBERSEGURIDAD PARA LA PRESTACIÓN DEL SERVICIO DE ACCESO A INTERNET"**, cuyo texto se anexa a la presente resolución, incorporando todos los cambios señalados en el cuerpo de la presente resolución en su versión definitiva.

SEGUNDO: ORDENAR a la Dirección Ejecutiva la publicación de la parte dispositiva de la presente resolución, incluyendo el "**EL REGLAMENTO DE CIBERSEGURIDAD PARA LA PRESTACIÓN DEL SERVICIO DE ACCESO A INTERNET"**, anexo, en un periódico de circulación nacional, y de la resolución de manera íntegra en la página Web que mantiene esta institución en Internet, en la dirección www.indotel.gob.do, todo lo anterior de conformidad con el artículo 91.1 de la Ley General de Telecomunicaciones, núm. 153-98, toda vez que la presente Resolución contiene un Reglamento de alcance general y de interés público.

TERCERO: DECLARAR que la presente Resolución es de obligado cumplimiento, de conformidad con las disposiciones del artículo 99 de la Ley General de Telecomunicaciones, número 153-98, del 27 de mayo de 1998.

Así ha sido aprobada, adoptada y firmada la presente resolución a unanimidad de votos por el Consejo Directivo del Instituto Dominicano de las Telecomunicaciones **(INDOTEL)**, en la ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, hoy día dieciocho (18) del mes de noviembre del año dos mil veintiuno (2021).

Firmado:

Nelson Arroyo
Presidente del Consejo Directivo

Pavel Isa
En representación del Ministro de Economía, Planificación y Desarrollo
Miembro Ex Oficio del Consejo Directivo

Príamo Ramírez Ubiera
Miembro del Consejo Directivo

Hilda Patricia Polanco
Miembro del Consejo Directivo

Darío Rosario Adames
Miembro del Consejo Directivo

Julissa Cruz Abreu
Directora Ejecutiva
Secretaria del Consejo Directivo

REGLAMENTO DE CIBERSEGURIDAD PARA LA PRESTACIÓN DEL SERVICIO DE ACCESO A INTERNET

TÍTULO I
DISPOSICIONES GENERALES

CAPÍTULO I
OBJETO Y ÁMBITO DE APLICACIÓN

Artículo 1.- Objeto. Este Reglamento tiene por objeto establecer medidas de alcance general, que servirán de base a las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa, para garantizar el continuo funcionamiento y seguridad del servicio de acceso a internet, como también asegurar la integridad, disponibilidad y confidencialidad de la información que se transmite, almacena y/o procesa a través y/o por medio de las infraestructuras y/o plataformas pertenecientes, contratadas o asociadas directamente a las prestadoras de servicio de acceso a internet y prestadoras de infraestructuras activas.

Artículo 2.- Ámbito de aplicación. El presente Reglamento establece las disposiciones generales por las cuales ha de regirse la gobernanza de ciberseguridad, para orientar los procesos organizacionales de las prestadoras de servicios públicos de telecomunicaciones, específicamente los que prestan servicios de acceso a internet y prestadoras de infraestructura activa. En tal virtud, son de aplicación para las prestadoras de servicios públicos de acceso a internet, de manera independiente de su participación en el mercado.

Párrafo I. Este Reglamento deberá ser interpretado de conformidad con la Constitución dominicana, la Ley, la legislación supletoria y complementaria, los reglamentos y normas dictados por el **INDOTEL**, así como las normas y recomendaciones internacionales dictadas por los organismos multilaterales de los que forma parte la República Dominicana y ratificadas por ésta.

Párrafo II. Las menciones y remisiones a normas contenidas en este Reglamento se entenderán realizadas a aquellas que se encuentren vigentes en el momento de su aplicación, incluyendo sus posibles modificaciones y normas que las complementen o reemplacen.

Párrafo III. En caso de modificación de esas normas, las remisiones previstas en el presente Reglamento serán interpretadas de la forma que mejor se adapte al propósito inicial de tal remisión.

CAPÍTULO II
DEFINICIONES

Artículo 3.- Definiciones. A los efectos del presente Reglamento, además de las definiciones previstas en el Capítulo I de la Ley General de Telecomunicaciones, núm. 153-98, así como en los reglamentos dictados por el Instituto Dominicano de las Telecomunicaciones (**INDOTEL**), serán de aplicación las definiciones siguientes:

a. **Amenaza:** una amenaza es la actividad, conocida o sospechada, que, de producirse, tendría o podría tener un efecto adverso sobre la ciberseguridad de una o más infraestructuras críticas o alguno de sus componentes, incluyendo sistemas de información complementarios o accesorios.

b. **Base de Datos de la Gestión de Configuración (Configuration Management Data Base o CMDB por sus siglas en inglés):** es el sistema que permite registrar la información de la

infraestructura y gestión del servicio mediante entidades denominadas elementos de configuración.

c. **Biblioteca de Infraestructura de Tecnologías de Información (Information Technology Infrastructure Library o ITIL por sus siglas en inglés)**: es un conjunto de conceptos y buenas prácticas usadas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma en general.

d. **Ciberseguridad:** la ciberseguridad se refiere al estado, y al conjunto de prácticas orientadas a mantenerlo, en el que un activo, sistema de información o servicio tecnológico de información y comunicación reúne las siguientes condiciones:

   1. Está protegido contra acceso no autorizado;
   2. Se mantiene disponible y operativo;
   3. Se mantiene la integridad del activo, sistema o servicio; y,
   4. Se mantiene la integridad y confidencialidad de la información almacenada, procesada o transmitida a través del sistema de información.

e. **Cifrado:** procedimiento que utiliza un algoritmo y una clave para transformar un mensaje de forma tal que sea incomprensible o ilegible a cualquier sujeto sin posesión de la clave correspondiente.

f. **Cortafuegos (Firewall):** sistema o equipo cuyo propósito es controlar el acceso en las redes o sistemas de información mediante la inspección del tráfico que fluye entre ellos.

g. **Cortafuegos de Aplicaciones Web (Web Application Firewall o WAF por sus siglas en inglés):** protege de múltiples ataques al servidor de aplicaciones web en el backend. La función del WAF es garantizar la seguridad del servidor web mediante el análisis de paquetes de petición HTTP/HTTPS y modelos de tráfico.

h. **Denegación de servicios (DoS/DDoS):** es un ataque a un sistema de información o red de información que causa la indisponibilidad del servicio mediante la saturación de sus recursos o a través de errores que provocan fallos en los programas informáticos que lo componen.

i. **Dirección IP:** es un conjunto de números que identifica de manera lógica una interfaz en la red de un dispositivo informático que utilice el protocolo de internet basado en el modelo TCP/IP.

j. **Elemento de configuración (Configuration Item o CI, por sus siglas en inglés):** componentes de una infraestructura que están o estarán bajo manejo de configuración. Un CI puede ser un simple módulo, como un monitor o elementos más complejos, como un sistema completo.

k. **Equipo de Respuesta ante Incidentes de Seguridad Cibernética (CSIRT):** es la organización responsable de recibir, revisar y responder a los informes y la actividad de incidentes de seguridad informática.

l. **Equipo en las instalaciones del cliente (o CPE por sus siglas en inglés):** es cualquier equipo de telecomunicaciones utilizado tanto en interiores como en exteriores para originar,

encaminar o terminar una comunicación. El equipo puede proveer una combinación de servicios incluyendo datos, voz, video y un host de aplicaciones multimedia.

m. **Evento**: es cualquier ocurrencia observable en un sistema, red o activo tecnológico, la cual indica una posible violación de las políticas, la seguridad de la información o fallo en los controles, o una circunstancia previamente desconocida posiblemente relevante a la seguridad.

n. **Firmware:** es un programa informático que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo.

o. **Gestión de Dispositivos móviles (Mobile Device Management o MDM por sus siglas en inglés):** es un tipo de software que permite asegurar, monitorizar y administrar dispositivos móviles sin importar el operador de telefonía o proveedor de servicios.

p. **Incidente de Ciberseguridad:** es todo evento que tenga o inminentemente pueda tener un efecto adverso sobre la ciberseguridad de un sistema de información o la información que es procesada, almacenada o transmitida por el mismo, constituye una violación a las políticas de seguridad o procedimientos de ciberseguridad vigentes o de las políticas de uso aceptable.

q. **Indicadores de Compromiso:** son todas aquellas informaciones relevantes que describen cualquier incidente, evento, actividad y/o artefacto malicioso, mediante el análisis de sus patrones de comportamiento.

r. **Ingeniería social:** consiste en el acto de manipular a una persona a través de técnicas psicológicas y habilidades sociales para cumplir metas específicas.

s. **Inteligencia:** información sobre amenazas o actores de amenaza que ayuda a identificar las herramientas, técnicas y procedimientos utilizados por estos para comprometer los sistemas.

t. **Network Time Protocol (o NTP por sus siglas en inglés):** es un protocolo de internet para sincronizar los relojes de los sistemas informáticos a través del enrutamiento de paquetes en redes con latencia variable. NTP utiliza UDP como su capa de transporte, usando el puerto 123. Está diseñado para resistir los efectos de la latencia variable.

u. **Nodos de Acceso:** son aquellos Nodos que no forman parte del Núcleo de Red, que proveen un servicio directo al Usuario y que forman parte de la Red de Acceso.

v. **Phishing**: ataque de ingeniería social que hace uso de la suplantación de identidad, a menudo utilizando como vectores el correo electrónico y sitios web ilegítimos, con el objetivo de engañar al usuario y lograr acceder a datos o sistemas informáticos a los que no se tiene autorización.

w. **Prestador(a):** Persona jurídica facultada por la Ley para la explotación de servicios de telecomunicaciones, que controle, administre, opere, maneje, provea o revenda en todo o en parte, directa o indirectamente, cualquier línea, sistema, servicio o producto de telecomunicaciones en el país.

x. **Prestadora de Servicio de Acceso a Internet (PSAI):** Es toda prestadora de servicios debidamente autorizada para prestar el Servicio de Acceso a Internet.

y. **Prestador(a) de Infraestructura Activa:** se refiere a toda prestadora que sea propietaria u opere infraestructura tecnológica física (móvil, transporte o datos) que es parte directa de soportar el servicio de acceso a internet ofrecido por la prestadora.

z. **Protocolo de Puerta de Enlace de Borde (BGP por sus siglas en inglés):** en telecomunicaciones, el protocolo de puerta de enlace de borde o BGP (del inglés Border Gateway Protocol) es un protocolo mediante el cual se intercambia información de enrutamiento entre sistemas autónomos. Por ejemplo, las prestadoras de servicio registrados en Internet suelen componerse de varios sistemas autónomos y para este caso es necesario un protocolo como BGP.

aa. **Protocolo de transferencia de archivos (File Transfer Protocol o FTP por sus siglas en inglés):** es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.

bb. **Protocolo de transferencia de archivos trivial (Trivial file transfer Protocol o TFTP por sus siglas en inglés):** es un protocolo de transferencia muy simple semejante a una versión básica de FTP. TFTP a menudo se utiliza para transferir pequeños archivos entre computadoras en una red, como cuando u un terminal X Window o cualquier otro cliente ligero arranca desde un servidor de red.

cc. **Red Core (Núcleo de Red):** es la parte central de una red de telecomunicaciones que gestiona y controla los servicios de los usuarios que están interconectados por medio de la Red de Acceso.

dd. **Riesgo:** se refiere a la potencialidad de que una amenaza de ciberseguridad explote una vulnerabilidad en un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización.

ee. **Sistema de Información:** es todo dispositivo o conjunto de dispositivos que utilizan las tecnologías de información y comunicación, así como a cualquier sistema de alta tecnología, incluyendo, pero no limitando, a los sistemas electrónicos, informáticos, telemáticos y de telecomunicaciones que separada o conjuntamente sirvan para generar, enviar, recibir, archivar o procesar información, documentos digitales, mensajes de datos, entre otros. De igual forma, hace referencia a cualquier sistema de tecnología de la información y/o cualquier sistema de tecnología operacional como un sistema de control industrial, un controlador lógico programable, un sistema de control de supervisión y adquisición de datos, o un sistema de control distribuido.

ff. **Sistema de nombre de dominio (Domain Name Server o DNS por sus siglas en inglés):** es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como internet o una red privada. Este sistema asocia información variada con nombres de dominios asignados a cada uno de los participantes.

gg. **Sistemas de soporte a las operaciones (Operations support systems o OSS por sus siglas en inglés):** hacen referencia a sistemas de información empleados por las empresas operadoras de telecomunicaciones. El término OSS por lo general describe a los "sistemas de red" que están directamente vinculados a la red de telecomunicaciones misma, por ejemplo: procesos de soporte para el mantenimiento del inventario de red, servicios de provisionamiento, configuración de los elementos de red y software para la gestión de fallas.

hh. **Sistema de Soporte de Negocios (Business Support Systems o BSS por sus siglas en inglés):** son los componentes que utilizan las prestadoras de servicios de telecomunicaciones para dirigir sus operaciones comerciales hacia los clientes.

ii. **Software malicioso:** es un programa informático que ejecuta funciones dañinas y/o indeseables, a menudo ocultando su comportamiento para evadir la detección. Dentro de esta categoría se encuentran los virus informáticos, troyanos, gusanos, backdoor o puerta trasera, ransomware, mineros de criptomonedas y otras variantes.

jj. **Technical Report 069 o CWMP:** es un estándar técnico del DSL Forum (renombrado posteriormente a Broad band Forum) conocido como *CPE Wan Management Protocol* (CWMP), que define un protocolo como capa de abstracción para el mantenimiento remoto de los dispositivos del usuario final.

kk. **Telnet** (***Tel****etype* ***Net****work*) es el nombre de un protocolo de red que nos permite acceder a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella. También es el nombre del programa informático que implementa el cliente. Para que la conexión funcione, como en todos los servicios de internet, la máquina a la que se acceda debe tener un programa especial que reciba y gestione las conexiones. El puerto que se utiliza generalmente es el 23.

ll. **Vulnerabilidad**: es cualquier debilidad en un sistema de información, sus procedimientos de seguridad, su implementación o en sus controles internos, que podrían permitir la materialización de una amenaza.

TÍTULO II
OBLIGACIONES ESENCIALES DE PRESTADORAS DE SERVICIOS DE ACCESO A INTERNET

CAPÍTULO I
GOBERNANZA DE LA CIBERSEGURIDAD

Artículo 4.- Marco de trabajo y gobernanza. Las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa deben contar con una estructura organizacional definida y con alta competencia para desempeñar las funciones de ciberseguridad dentro de la entidad y velar por el cumplimiento de lo dispuesto en el presente Reglamento.

Párrafo I. La estructura organizacional de ciberseguridad de las prestadoras de servicio acceso a internet y prestadoras de infraestructura activa deberá tener un nivel de independencia para establecer controles y políticas de acuerdo a este reglamento en toda la organización.

Párrafo II. Las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa deben contar con un Comité de Ciberseguridad encargado de garantizar e impulsar la

gestión de ciberseguridad, y dirigir el plan de estrategia de ciberseguridad en la organización. El Comité de Ciberseguridad debe estar conformado por áreas estratégicas para el desarrollo de la ciberseguridad en la organización.

Párrafo III. La estructura organizacional de ciberseguridad de las prestadoras de servicio acceso a internet y prestadoras de infraestructura activa, debe contar con un Equipo de Respuesta ante Incidentes de Seguridad Cibernética, encargado de gestionar los reportes de incidentes y coordinar las acciones de respuesta ante los mismos.

Párrafo IV. El gerente de la estructura organizacional de ciberseguridad de las prestadoras de servicio acceso a internet y prestadoras de infraestructura activa debe mantener una comunicación continua con la Dirección de Ciberseguridad, Comercio Electrónico y Firma Digital del **INDOTEL** para el tratamiento de temas como:

a. Seguimiento a los planes de mejoras;

b. Intercambio de información e inteligencia sobre ciberseguridad;

c. Esfuerzos en conjunto orientados a la promoción de una cultura de ciberseguridad; y

d. Cumplimiento de lo dispuesto en el presente Reglamento.

CAPÍTULO II
MARCO DE GESTIÓN DE CIBERSEGURIDAD

Artículo 5.- Política de ciberseguridad. Las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa deben establecer y mantener una política de ciberseguridad, la cual aborde todos los aspectos relevantes para una efectiva gestión de los riesgos de ciberseguridad, la protección de sus redes, activos de información y servicios, en adición a la protección de las comunicaciones, informaciones y privacidad de sus usuarios.

Párrafo. La política de ciberseguridad debe ser de conocimiento general por parte de todo el personal de la organización, así como de terceras partes interesadas con incidencia en la ciberseguridad, y debe estar alineada con los objetivos de negocio, los requisitos legales y regulatorios, el entorno de las amenazas y las tendencias tecnológicas de la industria.

Artículo 6.- Gestión de Riesgo. Las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa deben establecer un proceso de gestión de riesgo que permita la identificación, tratamiento y control de los riesgos de ciberseguridad en la infraestructura tecnológica, partiendo del análisis y evaluación de las amenazas, vulnerabilidades, impacto potencial y probabilidades de ocurrencia.

Párrafo. La gestión de riesgo debe tomar en cuenta los riesgos inherentes al sector de las telecomunicaciones, el rol que juegan las plataformas críticas para la provisión del servicio por parte de la prestadora, así como los riesgos propios de la cadena de suministro de las tecnologías de información y comunicaciones.

Artículo 7.- Capacitación sobre ciberseguridad. Las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa deben establecer y mantener un programa de educación sobre ciberseguridad con el objetivo de capacitar al personal, asociados y usuarios en

la protección de los sistemas y activos de tecnología de información y comunicación de la organización, el manejo adecuado de los datos y la aplicación de salvaguardas ante las amenazas relevantes, así como el cumplimiento con las regulaciones aplicables. El programa debe contemplar, como mínimo, los siguientes aspectos:

a. Orientación para personal de nuevo ingreso, así como talleres regulares o a raíz de cambios en la organización y en el entorno que puedan afectar el grado de exposición ante las amenazas de ciberseguridad. Este proceso de orientación cotidiana también aplicará a usuarios finales, representantes de servicio al cliente y personal de nivel ejecutivo.

b. Entrenamiento especializado para grupos específicos dentro de la organización, tales como los integrantes de la estructura organizacional de ciberseguridad y el Equipo de Respuesta ante Incidentes de Seguridad Cibernética, administradores de sistemas, desarrolladores de software y operadores; que abarque tópicos de ciberseguridad relevantes a cada grupo y las medidas de protección ante diversas amenazas, tales como phishing, ingeniería social, técnicas de programación segura, gestión de vulnerabilidades técnicas, respuesta ante incidentes, protección contra software malicioso, entre otros.

c. Orientación a terceras partes interesadas (por ejemplo, prestadoras, clientes, socios), sobre las principales medidas ante amenazas relevantes tales como phishing, ingeniería social, protección de los medios de autenticación, notificación y respuesta ante los incidentes, entre otros aspectos.

Artículo 8.- Trabajo remoto colaboradores. Las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa deben establecer para sus colaboradores que estén trabajando en un ambiente remoto (locaciones fuera de las localidades formales de la organización), lo siguiente:

a. Este modelo de trabajo debe estar sujeta a autorización y debe ser en específicos lugares aprobados previamente por la organización.

b. Proteger equipos tecnológicos e información que estén manejando contra perdida, robo y amenazas e incidentes.

c. Establecer conexión segura hacia la red administrativa de la organización.

Artículo 9.- Gestión de activos. Las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa deben establecer una gestión de activos de tecnologías de la información, telecomunicaciones e infraestructuras que puedan impactar en la continuidad del servicio. Cada uno de los elementos de configuración debe cumplir con lo siguiente:

a. **Registro:** los datos relevantes y atributos del elemento de configuración deben estar debidamente registrados y disponibles para sus operadores autorizados.

b. **Identificación:** los elementos de configuración deben tener un único e irrepetible identificador y un nombre en la red que cumpla con nomenclatura coherente. En cualquier plataforma, sistema o área de la empresa, el identificador único y nombre en la red debe mantenerse, sin ningún tipo de modificación.

c. **Criticidad**: las entidades deberán realizar una evaluación de toda su infraestructura y sistemas de TI y Telecomunicaciones para así conocer y clasificar la criticidad de cada elemento de configuración que estén gestionando.

Párrafo I. Las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa deben establecer y mantener un inventario exhaustivo y actualizado de todos los activos tecnológicos de la entidad, incluyendo servidores, dispositivos de usuario final (tales como portátiles y móviles), elementos de red (incluyendo elementos core, de distribución y acceso), equipos en las premisas del cliente (CPE), dispositivos IoT, entre otros, pertenecientes a las prestadoras.

Párrafo II. El inventario debe registrar el tipo de dispositivo, el fabricante y modelo, la ubicación física, las direcciones de red, direcciones de hardware, nombres de host y/o dominio, el propietario del activo, la función del activo, la clasificación del activo, entre otros detalles. El inventario debe incluir activos conectados a la infraestructura física, virtual, remotamente, en las premisas y aquellos dentro de entornos de nube. El inventario debe ser revisado y actualizado con una frecuencia mínima de un (1) año.

Párrafo III. Se debe establecer y mantener un inventario exhaustivo y actualizado de todo el software autorizado instalado en los activos tecnológicos de la empresa, incluyendo componentes de terceros utilizados en el desarrollo (entre estos, librerías y paquetes de software). El inventario de software debe documentar el nombre, fabricante, versión, fecha de instalación/uso inicial, el propósito del software y el estado de soporte del mismo. El inventario de software debe ser revisado y actualizado con una frecuencia mínima de seis (6) meses y el estado de soporte del software debe ser validado como mínimo una (1) vez al mes.

Párrafo IV. El inventario de activos puede ser establecido mediante el uso de herramientas para la gestión de inventario de activos tecnológicos (*IMS,* por sus siglas en inglés), herramientas compatibles con el modelo de ITIL CMDB, así como herramientas de tipo MDM (Mobile Device Management) para dispositivos móviles de usuario final.

Artículo 10.- Clasificación de los datos. Las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa deben establecer y mantener un esquema de clasificación de los datos en función de su valor, sensibilidad, criticidad y requisitos legales y/o regulatorios. Se debe revisar y actualizar el esquema de clasificación anualmente, o cuando ocurran cambios significativos en la empresa que puedan afectar esta medida.

Párrafo. Por igual, se debe establecer y mantener un inventario de datos, conteniendo como mínimo un inventario de los datos sensibles, clasificado en base al esquema de clasificación establecido. Se debe revisar y actualizar el inventario anualmente, como mínimo, con prioridad en los datos confidenciales.

Artículo 11.- Cumplimiento regulatorio. Las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa deben identificar, documentar y gestionar el cumplimiento con todos los requisitos legales, regulatorios y contractuales relacionados con la ciberseguridad, incluyendo las obligaciones sobre la privacidad, así como las responsabilidades y el enfoque de la entidad para cumplir con estos requisitos.

Párrafo. Los requisitos pueden abarcar, entre otros, los siguientes:

a. Derechos de propiedad intelectual;

b. Protección de la privacidad y protección de datos carácter personal;

c. Regulación sobre el comercio electrónico y firma digital;

d. Regulación sobre el uso de controles criptográficos;

e. Legislación sobre ciberdelincuencia.

CAPÍTULO III
SISTEMAS DE ACCESO

Artículo 12.- Gestión de las identidades y el acceso. Las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa deben restringir el acceso físico y lógico a los activos e instalaciones asociadas únicamente a los usuarios, procesos y dispositivos autorizados, según las necesidades legítimas de acceso para el desempeño de las actividades y/o funciones autorizadas dentro de la entidad. Las identidades y credenciales de acceso deben ser otorgados, administrados, validados, revocados y auditados según la política de control de acceso establecida y acorde con el principio de mínimo privilegio, la segregación de funciones, la clasificación de los datos y los activos tecnológicos y los requisitos regulatorios y contractuales aplicables.

Párrafo. Los procesos de gestión de las identidades y el acceso deben incorporar medidas para asegurar cumplimiento con las políticas de control de acceso establecidas y minimizar los riesgos de acceso no autorizado a los activos y componentes de las redes de la empresa. Entre estas medidas se encuentran:

a. Deshabilitar las cuentas de acceso que se encuentren inactivas por un período de tiempo predeterminado;

b. Modificar y/o revocar los accesos que no sean requeridos a partir de los cambios en el estado de los sujetos, tanto internos como externos, así como de los sistemas y servicios de tecnología de información y comunicaciones;

c. Revisar de forma periódica las cuentas de acceso y deshabilitar o eliminar aquellas que se encuentren inactivas o sin la debida justificación;

d. Limitar el uso de las cuentas de acceso a horarios específicos, según el patrón de uso autorizado de las mismas;

e. Incorporar, en la medida de lo posible, métodos automatizados en los procesos de gestión de identidades y acceso para reducir las oportunidades de error, omisión, violación u otras amenazas que puedan comprometer la efectividad de los mismos.

Artículo 13.- Autenticación. Las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa deben autenticar todo acceso a las redes y activos de la entidad por parte de los usuarios, dispositivos y sistemas, a través de métodos que ofrezcan niveles adecuados de seguridad en proporción con el grado de riesgo y el valor de los activos objeto del acceso. Los requisitos de autenticación deben abarcar, como mínimo, los siguientes aspectos:

a. Requisitos para garantizar el uso de elementos de autenticación seguros (por ejemplo, contraseñas o claves criptográficas robustas);

b. Reemplazo de los elementos de autenticación predeterminados o establecidos por el fabricante;

c. Requisitos para evitar el uso no autorizado y/o compromiso de los elementos de autenticación (por ejemplo, su reemplazo de forma periódica o cuando exista algún indicio de compromiso);

d. Uso de autenticación multifactorial (MFA) para el acceso remoto y el acceso a sistemas críticos y/o que manejen activos de información o funcionalidades sensibles, así como a las aplicaciones y sistemas expuestos al Internet;

e. Centralización de la autenticación mediante el uso de sistemas de inicio de sesión único (*SSO,* por sus siglas en inglés), así como el uso de servidores de autenticación, autorización y auditoría (*AAA,* por sus siglas en inglés) para el control de acceso a los elementos de red críticos.

Artículo 14.- Gestión del acceso privilegiado. Las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa deben asegurar un control estricto sobre el acceso privilegiado, tales como acceso de superusuario, de forma tal que se restrinja su uso al personal mínimo que requiera este nivel de acceso, así como garantizar la trazabilidad de la actividad realizada con estos privilegios. El control sobre el acceso privilegiado debe incluir, como mínimo, las siguientes medidas:

a. Mantener un registro de asignación de acceso privilegiado indicando la justificación, aprobación y tiempo de validez del acceso privilegiado.

b. Restringir el acceso privilegiado a cuentas específicas dedicadas a la administración, distintas a las utilizadas para otros fines.

c. Reemplazar las contraseñas predeterminadas de las cuentas privilegiadas por contraseñas robustas que cumplan con requisitos de complejidad adecuados. Estas contraseñas pueden ser resguardadas mediante el uso de bóvedas de contraseñas que ofrezcan la debida protección en cuanto a autenticación, cifrado, control de integridad y otros atributos de seguridad.

d. Requerir autenticación multifactorial (MFA por sus siglas en inglés) para el uso de las cuentas de acceso privilegiado y/o el acceso a información sobre las mismas.

e. Registrar toda actividad realizada con cuentas de acceso privilegiado, según la política de gestión de eventos de seguridad establecida.

f. Revisar con periodicidad la asignación de acceso privilegiado y realizar los ajustes de lugar, así como tomar las acciones que sean requeridas para cumplir con la política y requisitos en torno a este control.

CAPÍTULO IV
GESTIÓN DE SEGURIDAD TÉCNICA

Artículo 15.- Seguridad y resiliencia de las redes. Las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa deben implantar medidas para proteger a las redes y componentes críticos de amenazas con el potencial de afectar la confidencialidad, integridad y disponibilidad de las comunicaciones y servicios críticos, incluyendo, entre otras, las siguientes medidas:

a. Segmentar la red en zonas separadas física o lógicamente, tomando en cuenta los requisitos de seguridad de los sistemas en cada zona, la sensibilidad y/o criticidad de los activos, así como los requisitos regulatorios y/o contractuales. Como mínimo, se debe segregar las zonas que alojen sistemas o activos de alta criticidad y/o sensibilidad (Ej. Elementos del core de la red o sistemas OSS/BSS críticos), zonas con sistemas utilizados para las tareas administrativas o tareas que requieran acceso privilegiado (Ej. VLAN administrativo) y las zonas directamente expuestas al Internet (Ej. DMZ);

b. Filtrar el tráfico de red para permitir únicamente los protocolos, servicios y comunicaciones autorizados, así como para bloquear el tráfico malicioso. El filtrado de tráfico puede llevarse a cabo por medio de dispositivos de seguridad tales como cortafuegos de red y de aplicaciones (WAF para aplicaciones web, SBC para tráfico VoIP), sistemas de detección y prevención de intrusiones (*IDS/IPS* por sus siglas en inglés), filtros de contenido y/o URLs, entre otros;

c. Cifrar las comunicaciones sensibles, tales como tráfico de usuario, acceso remoto administrativo, así como cualquier transmisión de datos confidenciales o de carácter personal;

d. Proteger mediante cifrado y control de integridad las comunicaciones remotas y/o por medio de redes públicas, así como las comunicaciones inalámbricas (por ejemplo, WLAN, banda ancha móvil);

e. Controlar el acceso para los activos y dispositivos que se conectan remotamente a las redes de la entidad. El acceso debe ser permitido únicamente a los dispositivos que se encuentren debidamente autenticados, que cumplan con una configuración base segura, cuenten con la debida protección contra software malicioso y cuyo firmware y software se encuentre debidamente actualizado. Este control puede ser implantado con la ayuda de soluciones de control de admisión a redes (*NAC* por sus siglas en inglés), soluciones de detección y respuesta para *endpoints* (*EDR* por sus siglas en inglés), entre otras;

f. Mantener medidas de alta disponibilidad y balanceo de carga para proteger a la red ante amenazas a la disponibilidad y estabilidad, tales como los ataques de denegación de servicio, la saturación de los recursos de ancho de banda, procesamiento y almacenamiento, entre otros aspectos que puedan degradar o causar indisponibilidad de los servicios.

Párrafo. En adición a lo anterior, las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa deben adoptar medidas orientadas a proteger las redes y servicios a los usuarios de amenazas y patrones de ataque comunes en internet, entre las que se encuentran:

a. Prevenir la suplantación o *"spoofing"* de direcciones IP;

b. Medidas orientadas a evitar alteración no autorizada de las tablas de enrutamiento (por ejemplo, mediante el filtrado de tráfico BGP);

c. Prevenir los ataques al sistema de DNS, tales como alteración no autorizada de registros, falsificación de respuestas *("hijacking"* o *"cache poisining*"), mediante el uso de protocolos de seguridad u otras medidas centradas en DNS;

d. Mitigar los ataques de denegación de servicio distribuido (DDoS), ataque de malware a gran escala (por ejemplo, botnets), campañas de SPAM malicioso o phishing y otras amenazas mediante medidas como listas negras de direcciones IP o basadas en DNS, hoyos negros de red (blackhole), DNS *"sinkhole"* y el descarte o filtrado de tráfico de comando y control vinculado a estas amenazas.

Artículo 16.- Protección contra software malicioso. Las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa deben mantener protecciones adecuadas contra el software malicioso en todos los activos tecnológicos comúnmente afectados por esta amenaza, incluyendo servidores, computadoras de escritorio, computadoras portátiles y dispositivos móviles. Las medidas de protección contra software malicioso incluyen, sin limitarse a las siguientes:

a. Instalación y mantenimiento de software antimalware en todos los activos con capacidad para detectar y proteger contra los tipos comunes de software malicioso, entre estos virus, troyanos, gusanos, ransomware, backdoor o troyano de acceso remoto (RAT), *rootkit* y *cryptominers*. El software antimalware debe estar configurado para actualizar sus firmas automáticamente y debe tener la capacidad de proteger mediante técnicas adicionales;

b. Ejecución de análisis periódico de la memoria, almacenamiento y medios extraíbles para detectar, aislar y/o remover el malware;

c. Listas blancas para permitir únicamente la ejecución de programas y aplicaciones aprobados;

d. Controles a nivel perimetral para filtrar el software malicioso, así como bloquear los vectores de ataque del mismo, entre estos filtros de Spam, phishing, IPs y URLs maliciosos;

e. Generación y monitoreo de los eventos relacionados con la detección y protección contra software malicioso.

Párrafo. Para los dispositivos con menor probabilidad de ser afectados por malware, las entidades deben evaluar periódicamente la exposición de los mismos ante malware e implantar las medidas que puedan ser requeridas para mitigar el riesgo.

Artículo 17.- Gestión de configuración segura. Las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa deben establecer y mantener un proceso de configuración segura para los componentes de las redes y los activos de tecnología de información y comunicación de la organización, tomando como referencia las guías de configuración segura recomendadas por la industria, de forma tal que se reduzca la superficie de ataque de los activos y se mitiguen las vulnerabilidades asociadas a las configuraciones predeterminadas. Los controles de configuración segura deben abordar, entre otras, las siguientes medidas:

a. Desactivar servicios y protocolos de red innecesarios y/o inseguros;

b. Habilitar el cifrado y uso de protocolos seguros (por ejemplo, SSH y HTTPS);

c. Configurar políticas robustas de autenticación;

d. Deshabilitar o reemplazar las credenciales predeterminadas;

e. Limitar el acceso privilegiado y restringir los derechos de acceso predeterminadas;

f. Aplicar restricciones en los firewalls para permitir únicamente tráfico autorizado;

g. Habilitar la auditoría de eventos relevantes a la seguridad.

Párrafo. La gestión de la configuración segura, así como otras tareas de gestión de activos, debe realizarse a través de herramientas aprobadas y controladas, basadas en protocolos estándares de la industria, tales como TR-069 o CWMP para dispositivos en premisas del cliente (CPE), SNMP, entre otros; de forma tal que se automatice el proceso en el mayor grado posible.

Artículo 18.- Gestión de cambios. Las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa deben controlar los cambios a la configuración de los sistemas y componentes de las redes de la entidad, a través de un proceso de control de cambios formal que permita minimizar los riesgos introducidos por cambios no autorizados y que tengan el potencial de aumentar el grado de exposición de los activos críticos de las redes. El proceso de control de cambios debe contemplar, como mínimo, los siguientes aspectos:

a. Identificación, registro y aprobación de todo cambio significativo, incluyendo estimación de los posibles impactos del cambio en la seguridad del activo y los servicios que apoya;

b. Planificación y prueba de los cambios;

c. Evaluación del cambio, incluyendo la validación del cumplimiento con todos los requisitos de ciberseguridad relevantes;

d. Procedimientos para revertir el cambio y recuperar el sistema a su estado anterior en caso de fallos.

Artículo 19.- Seguridad de los datos y registros. Las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa deben aplicar medidas para proteger la confidencialidad, integridad y disponibilidad de los datos en reposo y/o en tránsito por las redes, en concordancia con su nivel de sensibilidad, criticidad y/o requisitos de integridad, así como las exigencias regulatorias y contractuales que apliquen. Las medidas para proteger los datos deben incluir, sin limitarse a, lo siguiente:

a. Cifrar los datos en reposo o en tránsito por medio de protocolos y métodos criptográficos robustos y basados en estándares de la industria. Ejemplos de estos protocolos y métodos de cifrado lo constituyen aquellos desarrollados y/o recomendados por organizaciones como la Unión Internacional de las Telecomunicaciones (UIT), Instituto Nacional de Estandarización y Tecnología (NIST), 3rd Generation Partnership Project (3GPP), el Internet Enginering Task Force (IETF) y otras entidades dedicadas a los estándares tecnológicos y su aplicación en la ciberseguridad, entre estos TLS, AES y Blowfish. Adicionalmente, el cifrado de los datos debe realizarse tomando en cuenta las mejores prácticas en la selección y manejo de las claves de cifrado;

b. Ofuscar o enmascarar los datos sensibles y/o sujetos a requisitos de privacidad o protección bajo normas y/o regulaciones aplicables a la empresa;

c. Comprobar la integridad del software, firmware y los datos mediante la firma digital y funciones *"hash"* seguras, tales como SHA-2;

d. Respaldar y/o replicar los datos y registros críticos, acorde con su grado de criticidad y requisitos de recuperación, así como los requisitos contractuales y regulatorios aplicables;

e. Eliminar de forma segura los datos en reposo, a través de métodos confiables de sanitización de medios de almacenamiento, tales como la sobre escritura con ceros de forma repetida (Ej. 3 o más veces), la desmagnetización de los medios o "*degaussing"* y el cifrado de los datos con eliminado seguro de las claves para medios basados en memoria flash (Ej. Discos de estado sólido o SSD).

Artículo 20.- Gestión de Respaldo (Backups). Las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa deben establecer una política de respaldo de la información crítica y/o sensible para los servicios ofrecidos por la entidad, que permita recuperar de forma oportuna y adecuada los datos en caso de pérdida, corrupción, alteración o destrucción. El método, período de retención, frecuencia y medidas de protección de las copias de respaldo deben ser establecidos con base en la clasificación o grado de sensibilidad y/o criticidad de la información o activo, así como los requisitos regulatorios, legales y contractuales correspondientes. La política de respaldo debe contemplar, como mínimo, los siguientes aspectos:

a. Respaldo de los datos críticos y/o vinculados a sistemas críticos de las redes de la entidad (por ejemplo, configuraciones de equipos core, bases de datos de suscriptores, entre otros);

b. Protección de las copias de respaldo mediante controles equivalentes a los utilizados para proteger los datos originales, tales como el cifrado de los datos sensibles, almacenamiento en sitios remotos con la debida seguridad física y ambiental, entre otros;

c. Control de versiones de los datos respaldados para protección contra corrupción y otras amenazas;

d. Definición de un período de retención para los datos respaldados acorde con la clasificación y requisitos regulatorios, legales y contractuales aplicables;

e. Pruebas periódicas de los medios y procedimientos de recuperación de los datos respaldados, de forma tal que se asegure su fiabilidad y la capacidad de recuperación según el tiempo y las condiciones establecidas;

f. Establecer y mantener un proceso de recuperación de datos. El proceso debe abordar el alcance de las actividades de recuperación de datos, la priorización de la recuperación y la seguridad de los datos de respaldo.

Artículo 21.- Seguridad durante el ciclo de desarrollo de sistemas. Las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa deben establecer y mantener requisitos y prácticas de seguridad durante el ciclo de desarrollo de sistemas de manera que se

aborde la ciberseguridad en las etapas tempranas del desarrollo y se mitiguen de forma oportuna los riesgos asociados al desarrollo de sistemas. Los requisitos de seguridad durante el ciclo de desarrollo de sistemas deben abarcar, como mínimo, los siguientes aspectos:

a. Realizar modelamiento de amenazas para identificar vectores de ataque y posibles fallas de seguridad en el sistema durante la fase de diseño, mediante un análisis de la arquitectura, los componentes, el flujo de los datos, las funcionalidades y los casos de uso;

b. Aplicación de los principios y técnicas de diseño y programación segura, incluyendo la validación y/o sanitización de las entradas, utilización de técnicas robustas de autenticación y manejo de sesiones, uso de protocolos y algoritmos robustos para el cifrado de los datos y la firma digital, validación de la integridad de los datos, protección contra técnicas de explotación comunes (por ejemplo, desbordamiento de búfer, ataques de inyección y ejecución remota de código), entre otros aspectos;

c. Uso de librerías y componentes de terceros aprobados y actualizados, adquiridos de fuentes confiables y validados por métodos seguros (Ej. función hash robusta);

d. Separación de los entornos de desarrollo y prueba de los entornos de producción, de forma tal que se minimicen las oportunidades de acceso o cambios no autorizados a los sistemas en producción;

e. Pruebas estáticas y dinámicas de seguridad de aplicaciones (*SAST* y *DAST*, por sus siglas en inglés), incluyendo la revisión del código fuente y las pruebas de intrusión para identificar y corregir las vulnerabilidades en las etapas de pre-producción.

CAPÍTULO V
AMENAZAS Y GESTIÓN DE INCIDENTES

Artículo 22.- Gestión de vulnerabilidades. Las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa deben establecer y mantener un proceso de gestión de vulnerabilidades para los activos informáticos y de telecomunicaciones de la organización. El proceso de gestión de vulnerabilidades debe abordar, como mínimo, los siguientes aspectos:

a. Recepción y procesamiento de información oportuna y de fuentes confiables sobre las vulnerabilidades técnicas en el software y los sistemas utilizados en las redes y activos tecnológicos de la organización. Las fuentes confiables de información sobre vulnerabilidades incluyen los boletines del fabricante e información de inteligencia proveniente de grupos de interés especial y entidades especializadas en la ciberseguridad;

b. Establecer un proceso para la recepción de reportes sobre vulnerabilidades técnicas por parte de entidades y sujetos externos a la organización, tales como reguladores, organismos de seguridad del Estado, usuarios y otras terceras partes interesadas;

c. Análisis y estimación del riesgo de las vulnerabilidades y la identificación, prueba, priorización y aplicación de las medidas para remediar o mitigar las vulnerabilidades;

d. Actualización y/o aplicación oportuna de las correcciones a todo el software y firmware utilizado por los componentes de las redes y los activos de tecnología de información y comunicación de la organización, incluyendo los sistemas operativos, las aplicaciones, los

sistemas integrados, así como los componentes y librerías de terceros. Las actualizaciones deben llevarse a cabo a través de la gestión automatizada de actualizaciones y debe tomar en cuenta la severidad de las vulnerabilidades, el valor de los activos y el impacto para el negocio y sus servicios en caso de ser aprovechadas por un atacante;

e. Ejecución de escaneos automatizados de vulnerabilidades de los activos informáticos y de telecomunicaciones de la organización, tanto internos como los que se encuentran expuestos a redes externas, con una frecuencia mínima de una vez por trimestre. Los escaneos de vulnerabilidades deben ser tanto autenticados como no autenticados, utilizando herramientas confiables recomendadas por la industria. Los hallazgos de los escaneos deben ser priorizados y remediados según el nivel de riesgo que representen, los requisitos regulatorios y contractuales aplicables, así como las políticas y procedimientos de gestión de riesgos de la entidad.

Artículo 23.- Gestión de eventos. Las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa deben producir, mantener, centralizar y revisar periódicamente registros sobre los eventos relevantes a la ciberseguridad. Entre los eventos a registrar se encuentran los eventos relativos a la autenticación, el uso de privilegios especiales, ejecución de funciones críticas y/o sensibles, acceso a datos confidenciales o de carácter personal, cambios a la configuración de los sistemas, los eventos y errores críticos.

Los registros de eventos deben incluir, como mínimo, los siguientes detalles:

a. Fecha y hora de ocurrencia;

b. Identificación del usuario (por ejemplo, nombre de usuario, IMSI, entre otros);

c. Identificación del activo, y de ser posible su ubicación (por ejemplo, dirección MAC o IMEI, IP, geolocalización);

d. Descripción del evento;

e. Cualquier otro elemento relevante para investigar el evento.

Párrafo I. Los registros de eventos deben ser centralizados en la medida de lo posible, y deben ser resguardados contra acceso ilícito, alteración, eliminación y otras amenazas. Las entidades deben retener los registros de eventos de seguridad por un mínimo de un (1) año.

Párrafo II. Las alertas de seguridad deben estar bajo un proceso de monitoreo continuo y la totalidad de los eventos de seguridad deben ser revisados con una frecuencia mínima de (1) una vez a la semana.

Párrafo III. Se debe sincronizar los relojes de los activos y componentes de la red con fuentes de tiempo confiables, de forma tal que se asegure consistencia en los registros de eventos.

Artículo 24.- Gestión de amenazas de ciberseguridad. Las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa deben establecer mecanismos y procesos para el monitoreo y detección de amenazas de ciberseguridad que comprenda, como mínimo, las siguientes capacidades:

a. Detección de anomalías con base en los umbrales y flujos de las comunicaciones autorizadas parte de las operaciones y servicios legítimos de la entidad;

b. Generación de alertas tempranas a partir de la detección de indicadores de amenazas e inteligencia confiable sobre las tácticas, técnicas y procedimientos de los atacantes;

c. Correlación de eventos provenientes de diversas fuentes de eventos relevantes a la ciberseguridad, tales como registros de actividad en servidores, elementos de red, dispositivos de usuarios finales, aplicaciones y sistemas OSS/BSS críticos, firewalls, sistemas de detección y prevención de intrusiones, sistemas antimalware, servidores AAA, entre otros;

d. Clasificación de las alertas en cuanto a su relevancia, severidad y/o potencial impacto adverso en las operaciones y servicio de la entidad;

e. Capacidad para reportar y compartir, tanto a nivel interno como externo, información técnica y codificada e inteligencia sobre las amenazas e incidentes de ciberseguridad detectados.

Párrafo. Las alertas generadas por los sistemas de detección de amenazas y anomalías deben ser monitoreadas de forma continua por personal de operaciones de ciberseguridad, debidamente capacitado en la detección, triaje, análisis y respuesta ante amenazas e incidentes de ciberseguridad.

Artículo 25.- Inteligencia sobre amenazas de ciberseguridad. Las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa deben consumir inteligencia sobre amenazas cibernéticas proveniente de fuentes confiables, tales como foros sobre intercambio de inteligencia y otros grupos de expertos en la materia, que permitan perfilar las amenazas en base a sus tácticas, técnicas y procedimientos, así como obtener información oportuna sobre indicadores de compromiso que permitan apoyar la gestión de los riesgos y la respuesta efectiva a las amenazas de ciberseguridad.

Párrafo I. Entre las fuentes de inteligencia sobre amenazas cibernéticas se puede considerar el marco MITRE ATT&CK, así como otros recursos reconocidos.

Párrafo II. Las entidades deben considerar apoyarse en métodos automatizados y basados en estándares de la industria para el consumo e intercambio de información de inteligencia, tales como STIX y TAXII del comité OASIS, entre otros.

Artículo 26.- Gestión de incidentes. Las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa deben establecer y mantener un proceso de gestión de incidentes de ciberseguridad de forma tal que se minimice el impacto de los incidentes y permita tomar medidas para evitar su reincidencia. El proceso de gestión de incidentes de ciberseguridad debe contemplar el ciclo completo de manejo de incidentes, incluyendo el establecimiento de roles y responsabilidades, el reporte y comunicación sobre los incidentes, así como las acciones a ejecutar antes, durante y después del incidente, orientadas a detectar, priorizar, contener y erradicar las amenazas, así como recuperar los activos y/o servicios afectados por el incidente.

Párrafo. En adición, se deben establecer y mantener procedimientos detallados de manejo de incidentes para las principales amenazas de ciberseguridad, así como para amenazas relevantes para el sector de las telecomunicaciones y los servicios de acceso a internet, entre estas:

a. Hacking y/o acceso ilícito en la red;

b. Ataque de código malicioso;

c. Denegación de servicio (DoS) y Denegación de servicio distribuido (DDoS);

d. SPAM malicioso, phishing y otras formas de ingeniería social;

e. Brechas de datos, incluyendo brechas de datos de clientes y/o datos de carácter personal;

f. Ataques a la infraestructura y servicios críticos de la red, tales como BGP Hijacking y DNS poisoning;

g. Spoofing y/o suplantación de identidad, incluyendo IP spoofing, SIM Swap, apropiación de cuenta (account takeover) y robo de servicios.

Párrafo I. Los procedimientos de manejo de incidentes deben contemplar la comunicación sobre los incidentes a las partes interesadas, incluyendo las partes externas tales como prestadoras, socios, clientes, grupos de interés especial, reguladores y organismos judiciales, tomando en cuenta las políticas y planes de respuesta establecidos, los acuerdos contractuales y la legislación y normativa aplicable.

Párrafo II. Los procedimientos de manejo de incidentes deben incluir procedimientos de investigación forense y cumplimiento con el debido proceso de ley, para una debida adquisición, preservación, análisis y documentación de la evidencia digital que sirva de apoyo a las acciones de remediación, disciplinarias y/o legales en torno al incidente.

Artículo 27.- Gestión de Problemas. Las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa deben implementar la gestión de problemas, que será el principal apoyo para la causa raíz de los incidentes, que ayudará a determinar una solución definitiva o temporal del problema luego de un incidente regular de alto impacto a la disponibilidad de los servicios o incidente de ciberseguridad.

Párrafo. Luego de un incidente de alto impacto o un incidente de ciberseguridad, se debe poner en ejecución el proceso de gestión de problemas, para obtener el análisis de la causa raíz y una propuesta de una solución definitiva o temporal.

CAPÍTULO VI
GESTION DE SEGURIDAD

Artículo 28.- Seguridad física y ambiental. Las instalaciones críticas, incluyendo centros de datos, oficinas centrales, sitios de celdas y cualquier recinto que aloje sistemas y/o informaciones críticas, debe contar con medidas de seguridad física y ambiental que provean protección contra acceso no autorizado, así como daños producidos por actos intencionales, accidentales y desastres naturales. Las medidas de seguridad física y ambiental deben incluir un perímetro físico seguro, controles de entrada adecuados, vigilancia humana y por medio de video, alarma contra intrusiones, controles de humedad y temperatura, sistemas de detección y supresión de incendio, entre otros.

Artículo 29.- Seguridad de la cadena de suministro. Las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa deben establecer y mantener una política de gestión de proveedores externos. Esta política debe abordar todas las fases del ciclo de gestión de proveedores externos, incluyendo la identificación y clasificación de los proveedores, así como la evaluación, el seguimiento y la terminación de la relación con los proveedores de servicios.

Párrafo I. La política de gestión de proveedores externos debe incluir el establecimiento de los requisitos de ciberseguridad para abordar los riesgos asociados con los servicios de tecnología de la información y comunicación y la cadena de suministro de productos.

Párrafo II. Dentro de los requisitos de ciberseguridad en el contexto de la cadena de suministro, se debe prestar especial atención al establecimiento de controles para comprobar la integridad de los componentes críticos de la red, tales como equipos core, de distribución y acceso (por ejemplo enrutadores, conmutadores, multiplexores), servidores en las premisas y entorno de nube, entre otros; de forma tal que se asegure ausencia de canales ocultos u otras vulnerabilidades que permitan interceptación ilícita de las comunicaciones, acceso no autorizado al sistema y/o los datos, denegación de servicio u otras amenazas. Esta medida puede ser establecida por medio de requisitos contractuales con las prestadoras que compongan la cadena de suministro o mediante inspecciones físicas especializadas.

Párrafo III. Se debe evaluar de forma regular a las prestadoras de servicios externos para asegurar el cumplimiento con los acuerdos contractuales y los requisitos de ciberseguridad establecidos. El alcance de la evaluación puede variar según la clasificación del proveedor y puede incluir la revisión de informes de evaluación estandarizados, como los informes de auditoría de los Controles de Organización de Servicio 2 (*SOC 2* por sus siglas en inglés), el Reporte de Cumplimiento con el estándar de seguridad de datos de tarjetas de pago (PCI-DSS por sus siglas en inglés), informes de auditoría de la Alianza de Seguridad de Nube STAR (*CSA STAR* por sus siglas en inglés), cuestionarios personalizados u otros procesos rigurosos. Se debe reevaluar a las prestadoras de servicios anualmente, como mínimo, o al suscribir o renovar los contratos.

Artículo 30.- Seguridad en ambientes de nube. Las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa que provean servicios en nube deben asegurar que la infraestructura dedicada a habilitar estos servicios cuente con las debidas medidas de ciberseguridad, resiliencia y privacidad para proteger adecuadamente los sistemas, aplicaciones, datos, servicios y demás activos alojados y/o gestionados por o para los clientes. Las prestadoras de servicios de nube deben incorporar, entre otras, las siguientes medidas:

a. Definir y asignar las responsabilidades para la protección de los activos y para llevar a cabo procesos específicos de ciberseguridad en el ambiente de nube, así como establecer y acordar claramente las responsabilidades de ciberseguridad que sean compartidas entre el proveedor de servicios de nube (*Cloud Service Provider* o CSP por sus siglas en inglés) y el cliente de servicios de nube (*Cloud Service Client*, por sus siglas en inglés), considerando el modelo de entrega de servicios de nube para cada caso, ya sea este Infraestructura como Servicio (IaaS), Plataforma como Servicio (PaaS), Software como Servicio (SaaS) u otros modelos que puedan ser adoptados;

b. Establecer y mantener políticas y procedimientos para la seguridad de la infraestructura y la virtualización del ambiente de nube. Se debe revisar y actualizar las políticas y procedimientos por lo menos una (1) vez al año;

c. Restringir, cifrar y monitorear las comunicaciones entre entornos únicamente a conexiones autenticadas, autorizadas y justificadas;

d. Fortalecer las plataformas, sistemas operativos, hipervisores y plano de control de las infraestructuras de acuerdo con los estándares y mejores prácticas de la industria y las guías de configuración segura establecidas para los activos de la entidad;

e. Diseñar, desarrollar, implantar y configurar las aplicaciones, plataformas y componentes de infraestructura de forma tal que el acceso, las operaciones y los recursos de los clientes de servicios de nube o "tenants" se encuentren debidamente aislados, segregados, restringidos y monitoreados;

f. Utilizar canales de comunicación seguros y cifrados para la migración de servidores, servicios, aplicaciones o datos a entornos de nube. Dichos canales deben incluir solo protocolos estándares aprobados y actualizados;

g. Proveer interfaces de programación de aplicaciones (*API,* por sus siglas en inglés) seguras, para permitir a los clientes de servicios de nube recuperar sus datos de manera programática y habilitar la interoperabilidad y la portabilidad de los datos;

h. Implantar protocolos de red estandarizados y criptográficamente seguros para la gestión, importación y exportación de los datos;

i. Planificar y monitorear la disponibilidad, calidad y capacidad adecuada de los recursos para ofrecer el desempeño requerido según los requisitos establecidos.

Artículo 31. Gestión de la privacidad. Las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa deben establecer, aplicar y mantener políticas y procedimientos para identificar y tratar los riesgos asociados a la adquisición, procesamiento y manejo de datos de carácter personal. Estas políticas y procedimientos deben abordar, como mínimo, lo siguiente:

a. Evaluar el riesgo de procesamiento de datos personales, de acuerdo con las leyes, regulaciones y mejores prácticas aplicables;

b. Desarrollar sistemas, productos y prácticas de negocio basados en las mejores prácticas de la industria y el principio de "privacidad desde el diseño", asegurando que la configuración de privacidad predeterminada de los sistemas se encuentre en conformidad con todas las leyes y regulaciones de privacidad aplicables;

c. Definir, implantar y evaluar procedimientos y medidas técnicas para asegurar que cualquier transferencia de datos personales o sensibles esté protegida del acceso no autorizado y solo sea procesada dentro del alcance permitido por las leyes y regulaciones aplicables;

d. Definir e implantar procedimientos y medidas técnicas que permitan a los titulares de los datos solicitar el acceso, rectificación o supresión de sus datos personales, de acuerdo con las leyes y regulaciones aplicables.

e. Definir, implantar y evaluar procedimientos y medidas técnicas para asegurar que los datos personales sean procesados de acuerdo con las leyes y regulaciones aplicables y para los fines declarados al titular de los datos;

f. Definir, implantar y evaluar procedimientos y medidas técnicas para la transferencia y subprocesamiento de datos personales dentro de la cadena de suministro del servicio, de acuerdo con las leyes y regulaciones aplicables;

g. Definir, implantar y evaluar procedimientos y medidas técnicas para revelar al titular de los datos los detalles de cualquier acceso a datos personales por parte de los subprocesadores y otras terceras partes autorizadas, previo al inicio de dicho acceso;

h. Establecer, describir y publicar el procedimiento para administrar y responder a las solicitudes de divulgación de datos personales por parte de los órganos de investigación del Estado de acuerdo con las leyes y regulaciones aplicables.

CAPÍTULO VII
GESTIÓN DE CONTINUIDAD DEL NEGOCIO

Artículo 32. Continuidad del Servicio. Las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa deben implementar y mantener una Gestión de continuidad de servicio que esté presente en las fases de diseño, transición y operación de los servicios ofrecidos.

Párrafo I. Dichas prestadoras deben contar con un plan robusto de acción frente a incidentes de alto impacto o desastres que pongan en riesgo la continuidad de servicios esenciales de telecomunicaciones.

Párrafo II. Los servicios y funciones identificados como altamente críticos para el negocio, bajo la gestión de riesgo, deben estar sujetos a medidas que garanticen su continuidad y recuperación ante incidencias y/o desastres con el potencial de provocar interrupciones, fallas y/o indisponibilidad. Estas medidas de continuidad y recuperación deben incluir, sin limitarse a, lo siguiente:

a. Definición de los objetivos de continuidad y recuperación para los servicios, funciones y activos críticos, con base en el análisis de impacto al negocio (*BIA* por sus siglas en inglés), el análisis de riesgo u otros ejercicios de gestión de riesgo aplicables.

b. Establecimiento y mantenimiento de los planes y procedimientos de continuidad del servicio y recuperación ante desastres, así como su evaluación periódica, monitoreo y mejoramiento continuo.

c. Definición y establecimiento de los requisitos, estrategias y acciones para abordar los riesgos identificados, incluyendo el establecimiento de medidas de redundancia y alta disponibilidad para activos críticos, el establecimiento de sitios de recuperación ante desastres para recuperar los servicios y/o funciones esenciales, la replicación continua de los datos críticos, la planificación y aprovisionamiento de los recursos humanos y servicios de terceros críticos, entre otras medidas.

CAPÍTULO VIII

SEGUIMIENTO Y MEJORA DE LA SEGURIDAD

Artículo 33.- Revisión independiente de ciberseguridad. Las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa deben establecer y mantener un programa de auditoría y pruebas de intrusión que permita identificar, evaluar y corregir de manera continua las debilidades e implantar mejoras en la ciberseguridad de las redes y servicios de la entidad. El programa de auditoría y prueba de intrusión debe incorporar, como mínimo, los siguientes requisitos:

a. Contemplar auditorías de ciberseguridad y pruebas de intrusión por lo menos cada dos años y cuando ocurran cambios significativos que tengan el potencial de alterar el grado de exposición de los sistemas y redes de la empresa. Entre estos cambios se encuentran la migración de plataformas críticas y la implantación de nuevos sistemas *OSS/BSS*;

b. Las auditorías evaluaciones y pruebas de intrusión deben ser llevadas a cabo por firmas o expertos calificados independientes, con habilidades y experiencia avaladas por certificaciones relevantes de la industria. Estas auditorías y pruebas de intrusión deben ser ejecutadas siguiendo metodologías reconocidas tales como las guías de pruebas de seguridad OWASP, NIST 800-115, entre otras;

c. Debe abarcar todos los activos críticos para los servicios ofrecidos al cliente, tales como los componentes de red, las aplicaciones, los microservicios, las interfaces de programación de aplicaciones (*API,* por sus siglas en inglés), los servicios en infraestructura de nube y demás activos críticos de la empresa;

d. Planificar, monitorear y validar las remediaciones que surjan producto de las auditorías y pruebas de intrusión, e incorporar las mismas como parte de los procesos de gestión de los riesgos de ciberseguridad de la empresa.

Párrafo I. Los resultados de las auditorías internas deben contener la documentación y notificación a las partes interesadas de sus conclusiones y recomendaciones. El proceso de realización de las auditorias deberá ser repetible y consistente.

Artículo 34.- Auditorías. En virtud de lo dispuesto por el literal g) del artículo 30 y literal r) del artículo 78 de la Ley General de Telecomunicaciones núm. 153-98 el INDOTEL tendrá la potestad de realizar evaluaciones o auditorías a las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa, que podrán llevarla a cabo colaboradores de INDOTEL o también firmas externas autorizadas previamente por INDOTEL.

Párrafo I. Cuando el INDOTEL comprenda que el informe resultante de una auditoría indique que cualquier aspecto de la auditoría no se llevó a cabo de manera satisfactoria, podrá ordenar a que repita ese aspecto de la auditoría.

CAPITULO IX
DE LOS REPORTES

Artículo 35. Reporte de incidentes de ciberseguridad. Las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa están obligadas a reportar oportunamente según se establece en el Párrafo III del presente artículo, al INDOTEL los incidentes de ciberseguridad que presente su infraestructura, redes o sistemas de información. INDOTEL tendrá la potestad

de compartir dicha información con cualquier Equipo de Respuesta de Incidente Seguridad Cibernética que entienda prudente.

Párrafo I. En tal virtud, las prestadoras tienen que reportar detalladamente sobre los incidentes de ciberseguridad que detecten en sus redes y aplicaciones, que alcance los umbrales de gravedad establecidos en las instrucciones pertinentes emitidas por INDOTEL. Los detalles específicos de la información sobre los incidentes de ciberseguridad son establecidos por el INDOTEL a través de su Dirección de Ciberseguridad, Comercio Electrónico y Firma Digital.

Párrafo II. El reporte de los incidentes de ciberseguridad debe contener las siguientes informaciones:

a. ID del incidente (número único asignado al registro del incidente en la plataforma de la prestadora);

b. Título y descripción del incidente que explique la situación actual y la magnitud del impacto del incidente con respecto a la empresa y los clientes finales;

c. Categoría del incidente, según el siguiente catalogo:

Categoría	Sub-categoría
Código malicioso	Virus
	Malware
	Rootkit
	Ransomware
	Herramientas de Acceso Remoto (RAT)
Disponibilidad	Denegación de Servicios (DoS) Denegación Distribuida de Servicios (DDoS)
	Sabotaje
	Error Humano
Robo de información	Sniffing
	Ingeniería Social (Phishing/Spear Phishing)
	Escaneo de vulnerabilidades
Intrusión	Alteración sitio web(Defacement)
	Inyección SQL
	Ataque de Fuerza bruta
	Explotación de vulnerabilidades (Hardware/Software)
Compromiso de Información	Acceso no autorizado
	Modificación/Publicación/Eliminación de información no autorizado
Fraude	Suplantación/Spoofing
Contenido abusivo	Correo No deseado (Spam)
	Publicación/almacenamiento de contenido de abuso sexual infantil en línea

d. Dispositivo, aplicativo o plataforma afectada (nombre del equipo e identificador asignado en el gestor de incidentes);

e. Criticidad;

f. Fecha y hora de inicio del incidente. Si existe alguna alerta o evento que indique el inicio o fin de la incidencia, deben de suministrar estas fechas y horas;

g. Cantidad de clientes afectados;

h. Si existe afección de algún servicio.

Párrafo III. Los reportes deben ser formulados por los encargados de ciberseguridad de las prestadoras y enviados a través de los mecanismos establecidos para ello por el INDOTEL. Con todo, el tiempo que medie entre la detección del incidente y la emisión del reporte, no podrán exceder del que se indica a continuación de conformidad a la naturaleza y alcance de cada evento:

Criticidad	**Descripción**	**Tiempo para reportar**
Severa	Las redes o sistemas no están disponible; datos de clientes y/o de carácter personal están siendo extraídos o expuestos; o procesos críticos están siendo alterados o manipulados.	2 horas
Alta	Las redes o sistemas están parcialmente fuera de operación; datos de clientes y/o de carácter personal están en riesgo de ser extraídos o expuestos; o los procesos críticos están en riesgo de ser alterados o manipulados.	3 horas
Media	Redes y sistemas en operación con fallas o incidentes de ciberseguridad reducidos y limitados.	4 horas

Párrafo IV. Las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa están obligadas a notificar a las personas posiblemente afectadas por estos incidentes, o al público en general, si las personas afectadas no pueden ser notificadas individualmente, en un plazo no mayor a las setenta y dos (72) horas, contadas a partir de tener conocimiento sobre los mismos. En caso de incumplimiento, esta notificación podrá ser realizada al público en general por el INDOTEL.

Párrafo V. Las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa están obligadas a enviar al INDOTEL, un informe sobre la respuesta y resolución del incidente. Este informe incluirá información sobre las causas del incidente de ciberseguridad, indicadores de compromiso, el tiempo dedicado a su resolución, las medidas aplicadas, el impacto

del mismo y toda otra información que sea pertinente sobre el incidente. Las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa tienen un plazo de 48 horas luego de la solución del incidente de ciberseguridad para enviar este informe.

Artículo 36. Reporte de métricas. Las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa están obligados a reportar métricas sobre incidentes de ciberseguridad al INDOTEL, con una frecuencia trimestral y conforme se indica a continuación:

a) Incidentes de ciberseguridad:
– Incidentes de ciberseguridad: bajo un formato implementado por la Dirección de Ciberseguridad, Comercio Electrónico y Firma Digital.
- Tiempo promedio de recuperación de incidentes de ciberseguridad: bajo un formato implementado por la Dirección de Ciberseguridad, Comercio Electrónico y Firma Digital.

Párrafo I. Las prestadoras de servicios de acceso a internet y prestadoras de infraestructura activa están obligadas a reportar métricas sobre disponibilidad de las redes al INDOTEL, con una frecuencia trimestral y conforme se indica a continuación:

b) Disponibilidad:
- Disponibilidad red core datos.
- Disponibilidad red acceso datos.
- Disponibilidad red core móvil.
- Disponibilidad red acceso móvil.

Formula de disponibilidad:

%Disponibilidad= $\mathbf{100} * \frac{TTS-TIS}{TTS}$

TTS: Tiempo Total del Servicio (segundos)
TIS: Tiempo Interrupción del Servicio (Segundos)

Párrafo II. Aunque la exigencia de entrega de las métricas de incidentes y disponibilidad es trimestral, dichas métricas deben compilarse y calcularse de manera mensual, y para el caso de disponibilidad se medirá las veinticuatro (24) horas. No se contemplará tiempo de indisponibilidad aquellos momentos que el servicio se vea afectado por mantenimientos planificados.

Párrafo III. Se llevará las métricas de disponibilidad segmentadas para los elementos de red core y los elementos de la red de acceso, manteniendo la misma fórmula de cálculo. Para los elementos de la red core el valor de la disponibilidad deberá ser mayor a 99.99% medido en un periodo mensual y los elementos de accesos deberá ser mayor de 99.50% medido en un periodo mensual.

a. **Elementos red core:** Media Gateway, Packet Data Media Gateway, Service Gateway, Home Location Register, Home Suscriber Server, Broadband Access Server (BAS)/MultiService Broadband Networg Gateway (MSBNG), y Mobility Management Entity (MME), Serving GPRS Support Node (SGSN), Gateway GPRS Support Node (GGSN), Packet Gateway (PGW), Serving Gateway (SGW), Mobile Switching Center (MSC), Radio Network Controller (RNC), Base Station Controller (BSC), y otros nodos de la red core.

b. **Elementos red de acceso:** Nodos B, Evolved Node B (ENodoB), Base Station Subsystem (BTS), All Purpose EDGE QAM (Apex), Digital Subscriber Line Access Multiplexer (DSLAM) y Cable Modem Termination System (CMTS), Optical Line Termination (OLT).

TÍTULO III
RÉGIMEN SANCIONADOR

CAPÍTULO I
SANCIONES

Artículo 37.- Sanciones. Las prestadoras de servicios de acceso a Internet y prestadoras de infraestructura activa que infrinjan cualquiera de las disposiciones contenidas en el Título II sobre obligaciones esenciales de prestadoras de servicios de acceso a internet de este reglamento serán pasibles de la aplicación de las sanciones establecidas en la Ley General de Telecomunicaciones, núm. 153-98.

TÍTULO IV
DISPOSICIONES FINALES

CAPÍTULO I
DISPOSICIONES FINALES

Artículo 38.- Disposiciones derogatorias. El presente Reglamento deroga expresamente la Resolución del Consejo Directivo del INDOTEL, núm. 129-06, que aprueba la Norma de Calidad de Servicio y Seguridad de la Red.

Artículo 39.- Entrada en vigencia. El presente Reglamento entrará en vigencia a los ochos (8) meses a partir de su publicación en un periódico de circulación nacional y una vez vencido este plazo, el mismo será de obligado cumplimiento y deberá ser aplicado y observado por todas las Prestadoras de servicios públicos de acceso a Internet y prestadoras de infraestructura activa que operan en la República Dominicana, de conformidad con lo dispuesto por el artículo 99 de la Ley General de Telecomunicaciones núm. 153-98.