(El presente Reglamento entrará en vigencia a partir del 2 de agosto del 2022)

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.

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.