



Ciberseguridad y/o Seguridad Digital

TÉRMINOS DE REFERENCIA 2026



TÉRMINOS DE REFERENCIA - GRUPOS DE TRABAJO 2026

1. Introducción

Nombre del Grupo de Trabajo: [Ciberseguridad]

Año: 2026

Coordinador: [Instituto Dominicano de las Telecomunicaciones de la Republica Dominicana (INDOTEL) y Agencia Nacional de Telecomunicaciones (ANATEL)]

Miembros: [Amparo Arango, aarango@indotel.gob.do, +1 809 696 7008 y Salerme Oliveira, salerm@anatel.gov.br, 55 61981456822]

2. Objetivo General

[Los proveedores de servicios de Internet (ISPs) tienen un rol clave: no solo entregan conectividad, sino que pueden ofrecer una primera línea de defensa ante amenazas cibernéticas (malware, phishing, ataques DDoS, entre otros). Una red de internet "limpia y segura" contribuye a la protección de usuarios, empresas e infraestructura crítica en cada país, lo que tiene un valor estratégico para la seguridad nacional, la estabilidad económica, la protección de datos, y la confianza ciudadana.

Si los entes reguladores adoptan estándares comunes de ciberseguridad para ISPs, se puede lograr un nivel uniforme de protección en toda la región, reduciendo riesgos transfronterizos y promoviendo un entorno digital más seguro.

En este contexto, un Grupo de Trabajo especializado fortalecer la ciberseguridad del ecosistema regional de telecomunicaciones mediante la definición, armonización y promoción de medidas regulatorias y buenas prácticas aplicables a los ISPs, con el fin de salvaguardar la seguridad nacional, la infraestructura crítica, los usuarios y la economía digital de los países miembros de REGULATEL.]

3. Actividades Principales

[Listar las actividades principales que el grupo llevará a cabo para alcanzar su objetivo.]

1. [Actividad 1: Encuesta de Diagnóstico sobre la Regulación de Ciberseguridad para el Mercado de Acceso a Internet: Esta actividad consiste en el diseño, aplicación y análisis de una encuesta regional de diagnóstico dirigida a los organismos reguladores miembros de REGULATEL, con el objetivo de identificar el estado actual de los marcos regulatorios, políticas públicas y medidas de supervisión relacionadas con la ciberseguridad aplicable a los proveedores de servicios de Internet (ISPs)]

2. [Actividad 2: Seminario Virtual: Mejores Prácticas en Ciberseguridad para Proveedores de Servicios de Internet: Este seminario tiene como objetivo generar un espacio regional de diálogo técnico y estratégico entre reguladores, expertos y actores relevantes, para intercambiar experiencias y mejores prácticas sobre la implementación de medidas de ciberseguridad por parte de los proveedores de servicios de Internet.

4. Descripción de las Actividades

4.1. [Encuesta de Diagnóstico sobre la Regulación de Ciberseguridad para el Mercado de Acceso a Internet]

Descripción: [Esta actividad consiste en el diseño, aplicación y análisis de una encuesta regional de diagnóstico dirigida a los organismos reguladores miembros de REGULATEL, con el objetivo de identificar el estado actual de los marcos regulatorios, políticas públicas y medidas de supervisión relacionadas con la ciberseguridad aplicable a los proveedores de servicios de Internet (ISPs).

La encuesta permitirá mapear el nivel de madurez regulatoria en la región, identificar convergencias y divergencias normativas, así como detectar brechas, desafíos comunes y oportunidades para la armonización regional, siempre desde una perspectiva de protección del interés público y la seguridad nacional.]

Metodología: [Elaboración de un cuestionario estructurado (en formato digital) con preguntas cerradas y semiabiertas, organizado en ejes temáticos:

- Existencia de obligaciones de ciberseguridad para ISPs
- Enfoque regulatorio (voluntario, obligatorio, basado en riesgos)
- Relación con CIIP e infraestructura crítica
- Supervisión, sanciones e incentivos
- Coordinación con CSIRTs u otras autoridades nacionales]

Resultados Esperados:

1. Mapa regional del estado de la regulación de ciberseguridad para ISPs, identificando niveles de madurez, enfoques regulatorios y buenas prácticas existentes.
2. Identificación de brechas y prioridades comunes, que sirvan de base para futuras recomendaciones, guías o líneas de acción del Grupo de Trabajo.]

4.2. [Seminario Virtual: Mejores Prácticas en Ciberseguridad para Proveedores de Servicios de Internet]

Descripción: [El conversatorio virtual tiene como objetivo generar un espacio regional de diálogo técnico y estratégico entre reguladores, expertos y actores relevantes, para intercambiar experiencias y mejores prácticas sobre la implementación de medidas de ciberseguridad por parte de los proveedores de servicios de Internet. La actividad permitirá analizar enfoques exitosos,

lecciones aprendidas y desafíos regulatorios, reforzando el rol de los ISPs como actores clave en la protección del ecosistema digital, la infraestructura crítica y los intereses nacionales.

Metodología: [Organización de un evento virtual de 90–120 minutos.

- Formato mixto:
 - Presentaciones breves de expertos invitados
 - Casos prácticos o experiencias nacionales
 - Espacio de diálogo abierto con preguntas y respuestas
- Participación de:
 - Reguladores miembros de REGULATTEL
 - Expertos en ciberseguridad y regulación
 - Representantes de ISPs (cuando sea pertinente)]

Resultados Esperados:

1. Identificación de un conjunto inicial de mejores prácticas regionales en ciberseguridad para ISPs, desde la perspectiva regulatoria.
2. Fortalecimiento del intercambio de conocimiento y cooperación técnica entre los reguladores miembros.

5. Cronograma de Actividades

Actividad	Fecha de Inicio	Fecha de Finalización	Responsable(s)	Resultados Esperados
Encuesta de Diagnóstico sobre la Regulación de Ciberseguridad para el Mercado de Acceso a Internet	[01/06/2026]	[03/09/2026]	[INDOTEL]	[Resultado 1]
Seminario Virtual: Mejores Prácticas en Ciberseguridad para Proveedores de Servicios de Internet:	[01/04/2026]	[07/04/2026]	[INDOTEL]	[Resultado 2]

6. Indicadores de Éxito

1. [Indicador 1: Número de países y reguladores participantes.]
2. [Indicador 2: Nivel de interacción durante el conversatorio (preguntas, comentarios, casos compartidos).]
3. [Indicador 3: Producción de un resumen ejecutivo o nota técnica con las conclusiones del evento.]

7. Recursos Necesarios

[Listar los recursos humanos, financieros o materiales necesarios para llevar a cabo las actividades.]

1. [Recurso 1: Plataforma de videoconferencia.]
2. [Recurso 2: Moderador con experiencia en regulación y ciberseguridad.]
3. [Recurso 3: Apoyo del secretariado para logística y documentación.]
3. [Recurso 4: Expertos invitados (reguladores, CSIRTs, especialistas técnicos).]

8. Contacto

Responsable Principal: [Amparo Arango]

Correo Electrónico: [aarango@indotel.gob.do]

Teléfono: [+1 809 696 7008]

Nota: Por favor, asegúrense de diligenciar todos los apartados de la plantilla y remitirla antes del 31 de enero de 2026 a aarango@indotel.gob.do