SOLICITUD PARA EL SEGURO CONTRA RIESGOS CIBERNÉTICOS

I. Información del Entidad

Nombre del Entidad: COMISIÓN DE REGULACIÓN DE COMUNICACIONES

Dirección del Entidad: CALLE 59ª BIS # 5-53 PISOS 8, 9 Y 10

Ciudad: BOGOTÁ Departamento: CUNDINAMARCA Código Postal: 11011

Teléfono: 601 3198300 Sitio Web del Entidad: www.crcom.gov.co

Nombre del Grupo Económico al que pertenece (De ser aplicable): NA

Descripción de las actividades de la entidad: Regulador único de los servicios de Comunicaciones, televisión y postal en Colombia.

Información de Contacto

Nombre y Cargo de la persona encargada de los seguros: DIANA GISSELA WILCHES TORRES

Teléfono: 601 3198300 Correo electrónico: diana.wilches@crcom.gov.co

Nombre y Cargo de la persona de contacto ante un Evento de Seguridad de la Información: JUAN NICOLÁS AYALA RODRÍGUEZ

Teléfono: 601 3198300 Correo electrónico: juan.ayala@crcom.gov.co

II. Información General

Por favor complete el siguiente cuadro con la información del **Entidad**:

	Año Anterior 31-12-2025	**Año Actual 31-03-2026**
Número de empleados	**150**	**150**
Ingresos brutos percibidos en Colombia.	$ 51.513.081.695,91	$ 24.925.654.526,47
Ingresos brutos percibidos fuera de Colombia.	$ 0,00	$ 0,00
Total Activos	$ 33.521.663.791,88	$ 40.810.334.058,33

Por favor estime el número de expedientes de información personal bajo el cuidado, custodia o control del **Entidad,** sus subsidiarias y todas las entidades presentadas en la solicitud. En caso de no tener registro alguno, por favor marque esta casilla. ☐

Tipo de información personal	**Número de expedientes**
Información Personal Reservada (IPR) excluyendo información financiera e Información Clínica de Carácter Confidencial (ICC)	Menos de 500K ☐ 1M – 5M ☒ 500K-999K ☐ Más de 5M ☐
Información Clínica de Carácter Confidencial (ICC)	Menos de 500K ☒ 1M – 5M ☐ 500K-999K ☐ Más de 5M ☐
Información Financiera	Menos de 500K ☒ 1M – 5M ☐ 500K-999K ☐ Más de 5M ☐
Información Corporativa de terceros	Menos de 500K ☐ 1M – 5M ☒ 500K-999K ☐ Más de 5M ☐
Información Personal de residentes en Estados Unidos	Menos de 500K ☐ 1M – 5M ☐ 500K-999K ☐ Más de 5M ☐

Políticas de Seguridad de Redes e Información

1. ¿El **Entidad** tiene una política de seguridad de la información que registre y exhiba la manera como la información está protegida por la entidad? SI ■ NO ☐	
2. ¿El **Entidad** implementa políticas de seguridad de redes e información que sean revisadas anualmente? SI ■ NO ☐	
3. ¿El **Entidad** cumple con las normas nacionales e internacionales en materia de protección y seguridad de información aplicables a sus actividades? SI ■ NO ☐ En caso afirmativo, por favor describir la periodicidad con la que se revisa el cumplimiento normativo. Anual	
4. ¿El **Entidad** ha implementado políticas y procedimientos con base en las revisiones periódicas para verificar el cumplimiento de la normatividad en materia de protección y seguridad de la información. SI ■ NO ☐ En caso contrario, por favor explique los motivos.	
5. ¿El **Entidad** contrata con terceros para verificar alguna de sus políticas y/o procedimientos en materia de protección y seguridad de la información? SI ☐ NO ■ En caso afirmativo, por favor indicar cuales políticas y procedimientos.	
6. ¿El **Entidad** cuenta con un programa para poner a prueba y auditar los controles de seguridad adoptados? SI ■ NO ☐	

En caso afirmativo, con que periodicidad el **Entidad** prueba los controles. Anual

Capacitación de empleados y cumplimiento de normas

1. ¿Con qué periodicidad el **Entidad** ofrece capacitación sobre seguridad de la información para sus empleados? SI ■ NO ☐	**Mensual**
2. ¿El **Entidad** evalúa a todos los empleados y consultores independientes? SI ■ NO ☐	
3. ¿El **Entidad** ofrece capacitación sobre suplantación de identidad para todos sus empleados? SI ■ NO ☐	
4. ¿El **Entidad** impide el acceso al computador de los empleados, cuando éstos terminan su vínculo con la compañía? SI ■ NO ☐	

Seguridad de las Contraseñas

1. ¿El **Entidad** exige que las contraseñas de sus empleados tengan al menos 8 caracteres, un número y carácter especial? SI ■ NO ☐	
2. ¿Las contraseñas de los empleados del **Entidad** expiran y requieren su modificación por los menos cada 90 días? SI ■ ☐	
3. ¿El **Entidad** requiere que los usuarios remotos sean autenticados y encriptados antes de acceder a redes internas y sistemas informáticos? SI ■ NO ☐	
4. ¿El **Entidad** requiere que sus empleados utilicen la autenticación de doble factor o multifactores en todos los dispositivos móviles que tengan acceso a redes internas o sistemas informáticos? SI ■ NO ☐	

Cumplimiento de normas sobre pagos con tarjetas de crédito:

1. ¿El Entidad procesa, almacena o transmite información relacionada con tarjetas de crédito. SI ☐ NO ■ En caso afirmativo, por favor responder las preguntas 2-4.	La CRC no cuenta con tarjetas de crédito
2. ¿Cuál es número total estimado de transacciones anuales que se realizan con tarjetas de crédito? SI ☐ NO ☐	No aplica
3. ¿El **Entidad** cumple con los estándares de seguridad requeridos para pagos con tarjetas de crédito de acuerdo con su volumen y nivel de negocios? SI ☐ NO ☐	No aplica

En caso contrario, explique los motivos.	
4. ¿En qué fecha se presentó la última asesoría recibida por parte de terceros sobre pagos con tarjetas de crédito para el personal del **Entidad** (Si es aplicable)? SI ☐ NO ☐	No aplica

Cumplimiento de las normas sobre información clínica:

1. ¿El **Entidad** procesa, almacena o transmite Información Clínica de Carácter Confidencial (ICC)? SI ☐ NO ■ En caso afirmativo, por favor responder las preguntas 2 y 3.	
2. ¿El **Entidad** ha evaluado su cumplimiento con las reglas de privacidad, seguridad y violación de las normas sobre información clínica y su correspondiente notificación en el último año? SI ☐ NO ☐ En caso afirmativo, por favor indique si se trató de una autoevaluación o la efectuó un tercero independiente:	
3. ¿El **Entidad** cumple con las reglas de privacidad, seguridad y violación de las normas sobre información clínica y su correspondiente notificación? SI ☐ NO ☐	

Actividades Tercerizadas

1. ¿El Entidad contrata a proveedores externos para alguna de las siguientes actividades?:

Actividad	SI	NO	**Nombre del proveedor**
Gestión de Seguridad de la Información	x		Wexler S.A.S.
Alquiler de espacios físicos para alojamiento de equipos y recuperación de desastres		x	
Almacenamiento y recuperación de información	x		Svait
Proveedor de servicios de aplicativos o aplicaciones	x		Microsoft
Hosting de sitios web		x	
Procesamiento de tarjetas de crédito		x	
La administración de recursos humanos/ servicios extralegales a trabajadores			
Servicios de almacenamiento en “la nube”	x		Microsoft

2. ¿El **Entidad** exige a sus proveedores que demuestren el cumplimiento de políticas de protección de seguridad de la información que concuerden con las de la **Entidad**? 3. SI ■ NO ☐	En las minutas de los contratos se incluye una cláusula en la que los diferentes proveedores se comprometen a respetar la política de seguridad y privacidad de la información de la CRC, y demás normas y lineamientos

	internos en lo que respecta a la gestión de la seguridad de la información que le sean aplicables. A este compromiso le hace seguimiento el supervisor del contrato cuando autoriza cada pago.
4. ¿El **Entidad** realiza la Debida Diligencia o "Due Diligence" sobre cada proveedor para asegurar que sus medidas cumplen con las normas de seguridad de datos del **Entidad**? SI ■ NO ☐	
5. ¿El **Entidad** realiza auditorías sobre todos sus proveedores para asegurarse que éstos cumplan con los estándares aceptados por el **Entidad**? SI ☐ NO ■	
6. ¿El **Entidad** exige a sus proveedores que lo defiendan e indemnicen en caso de que los proveedores contribuyan a una violación de confidencialidad o privacidad? SI ■ NO ☐	
7. ¿El **Entidad** requiere que sus proveedores mantengan un seguro de responsabilidad civil vigente? SI NO	Depende de la naturaleza del contrato

Medidas de seguridad y procedimientos de protección

1. ¿El **Entidad** cuenta con una persona encargada de la administración de su sitio web y la seguridad de su red? SI ■ NO ☐

   En caso afirmativo, indique el nombre del funcionario y describa sus responsabilidades.

2. ¿El **Entidad** encripta esta información?
   A. Aquella almacenada en dispositivos móviles y soportes portátiles. SI ☐ NO ■
   B. Aquella que está inactiva o "en reposo" dentro de las bases de datos y computadores. SI ■ NO ☐
   C. Aquella que está almacenada en copias de seguridad (discos externos, redes de almacenamiento externo) SI ■ NO ☐

3. ¿El **Entidad** ha establecido y consignado por escrito políticas sobre?

   A. Encriptación de comunicaciones internas y externas. SI ■ NO ☐
   B. Eliminación constante de los dispositivos informáticos en des uso SI ■ NO ☐
   C. Controles de seguridad para prevenir accesos no autorizados a dispositivos móviles SI ■ NO ☐

4. ¿El Entidad cuenta con controles físicos para el acceso a sus instalaciones?

SI ■ NO ☐

5. ¿La red del **Entidad** cuenta con "firewalls" o cortafuegos entre los lugares de acceso restringido y los de acceso público? SI ■ NO ☐
6. ¿La red del Entidad cuenta con "firewalls" o cortafuegos para acceder a información sensible? SI ☐ NO ☐
7. ¿El Entidad utiliza antivirus/anti-malwares en todos sus computadores? SI ■ NO ☐
8. ¿El Entidad ha implementado un sistema de detección de intrusos a las redes?

   SI ■ NO ☐
9. ¿El Entidad tiene un proceso centralizado para el mantenimiento, monitoreo y análisis de los registros de las auditorías? SI ■ NO ☐
10. ¿El Entidad realiza pruebas sobre la vulnerabilidad a la exploración/penetración de?
    A. Sistemas internos y externos SI ■ NO ☐
    B. Aplicaciones web SI ■ NO ☐
11. ¿Con qué periodicidad el Entidad realiza actualizaciones, modificaciones o reparaciones (Patches/Hot-Fixes/Service Packs) a sus softwares/firmwares? SI ■ NO ☐

    Por favor descríbalo: Mensual
12. ¿El Entidad aplica el principio "least privilege" (acceso restringido a los lugares o información estrictamente necesario para el adecuado desempeño de las labores asignadas) para el acceso a información sensible? SI ■ NO ☐
13. ¿El Entidad aplica la segmentación o segregación de la red para proteger información sensible? SI ■ NO ☐

Procedimientos de respuesta y Continuidad del negocio

1. ¿El Entidad cuenta con un procedimiento escrito sobre el plan de respuesta ante las siguientes situaciones?
   En caso contrario, por favor explique.

   A. Acceso no autorizado a la red SI ■ NO ☐
   B. Violación de la Privacidad/Confidencialidad SI ■ NO ☐
   C. Ataques que impidan disponer de los servicios de su sistema SI ■ NO ☐
   D. Interrupción del funcionamiento de la red SI ■ NO ☐
   E. Amenaza extorsiva SI ☐ NO ■
2. ¿Con qué periodicidad el Entidad pone a prueba sus procedimientos de respuesta? **Anual**

3. ¿El Entidad cuenta con un plan de continuidad del negocio y de recuperación ante desastres? SI ■ NO ☐
4. ¿El Entidad ha puesto a prueba su plan de continuidad del negocio y de recuperación ante desastres durante el último año? SI ■ NO ☐
5. ¿Cuánto tiempo toma restablecer las operaciones del Entidad después de recibir un ataque que impida disponer de los servicios de su sistema o una interrupción del funcionamiento de su red? **4 horas**_ Por favor explique. **Tiempo establecido por el BIA**
6. ¿Con qué periodicidad el Entidad realiza copias de seguridad de la información relevante? **Diario** Por favor explique. **Tiempo establecido en el plan de copias de respaldo**
7. ¿El **Entidad** cuenta con un procedimiento para administrar y controlar la vida útil de los equipos que soportan el funcionamiento de los sistemas y la red? SI ■ ☐
8. ¿El Entidad implementa una política de control para el cambio de sus sistemas tecnológicos? SI ■ NO ☐
9. ¿El plan de continuidad del negocio y de recuperación ante desastres del **Entidad** contempla fallos en la nube? SI ■ NO ☐
10. ¿Cuánto tiempo toma restablecer las operaciones del Entidad que dependen del proveedor de servicios que implican el uso de la nube? SI ■ NO ☐ 4 horas

Cobertura de Medios Cibernéticos

1. ¿El Entidad pública en sus sitios web o cuentas de redes sociales?
   A. Contenidos licenciados por terceros SI ☐ NO ■
   B. Contenidos generados por los usuarios (videos, fotografías, salas de chats, etc.) SI ☐ NO ■
   C. Transmisión de música o video SI ■ NO ☐
2. ¿El Entidad cuenta con procedimiento para identificar alguna de las siguientes circunstancias previo a la publicación de los contenidos mencionados anteriormente?
   A. Infracción de derechos de autor SI ■ NO ☐
   B. Infracción de marca SI ■ NO ☐
   C. Difamación (incluyendo la difamación comercial) SI ■ NO ☐
   D. Invasión de privacidad SI ■ NO ☐
3. ¿El Entidad cuenta con un procedimiento formal para responder las quejas recibidas en relación con contenido difamatorio, infracciones, controversias o violaciones sobre la privacidad de terceros? SI ■ NO ☐
4. ¿El Entidad cuenta y hace cumplir un procedimiento para retirar contenidos de acuerdo con las normas sobre derecho de autor? SI ■ NO ☐

Coberturas de Delito Cibernético e Ingeniería Social

1. ¿El **Entidad** cuenta con un plan de acción ante fraudes relacionados con pagos electrónicos? SI ☐ NO ■

2. Por favor marque todos los controles contra fraudes implementados por el Entidad:
   A. Software anti-spam SI ■ NO ☐
   B. Tecnologías diseñadas para la autenticación/validación de correos electrónicos tales como SPF, DKIM, firmas digitales, Identificador del remitente, etc. SI NO ☐
   C. Controles automáticos con las respectivas instituciones financieras requiriendo autenticación para cualquier pago en línea que exceda criterios predeterminados? SI ■ NO ☐
   D. Procedimientos independientes de verificación para todas las solicitudes por correo electrónico para hacer pagos por transferencia o pagos electrónicos SI ☐ NO ■
   E. Personas autorizadas para hacer pagos electrónicos o por transferencia SI ■ NO ☐
   F. Personas autorizadas para llevar a cabo las operaciones descritas con un límite determinado SI ■ NO ☐
   G. Controles en donde se requieran más de una persona autorizada para aprobar pagos electrónicos o por transferencia SI ■ NO ☐

Historial de reclamaciones e información sobre pérdidas

1. ¿El Entidad ha recibido o conoce sobre eventuales reclamaciones, litigios o pérdidas durante los 3 últimos años derivadas de seguridad de la información, seguridad de la red o medios de comunicación? SI ☐ NO ■

2. ¿El Entidad ha sido objeto de investigación, requerimientos o acciones por parte de autoridades competentes con motivo de una supuesta violación a la normatividad sobre seguridad y privacidad de la información dentro de los últimos 3 años? SI ☐ NO ■

   En caso afirmativo en las preguntas 1-2 anteriores, por favor haga una descripción completa de los hechos en un anexo a esta Solicitud de Seguro, incluyendo costos, pérdidas incurridas y cualquier medida correctiva adoptada como respuesta al incidente.

3. ¿El **Entidad** o cualquiera de las personas que se presenten para este seguro, tienen conocimiento de cualquier hecho, circunstancia, situación, evento o transacción que razonablemente podría dar lugar a una reclamación o pérdida que estaría dentro del ámbito de la cobertura ofrecida? SI ☐ NO ■

   En caso afirmativo, por favor explique:

El Entidad entiende y acepta que si existe algún hecho, circunstancia, situación, evento o transacción previa, divulgado o no, las reclamaciones o pérdidas derivadas de tales supuestos no gozarán de cobertura bajo el seguro ofrecido, salvo las excepciones expresamente consagradas en él.

Representación del Entidad, Advertencias sobre fraudes y Firmas

LA FIRMA DE ESTA **SOLICITUD DE SEGURO** NO IMPLICA QUE EL ASEGURADOR DEBA ACEPTAR EMITIR LA PÓLIZA, NI EL ENTIDAD DEBA PAGAR LAS PRIMAS O PRECIO DEL SEGURO. SE ACUERDA QUE LA PRESENTE **SOLICITUD DE SEGURO**, INCLUYENDO CUALQUIER MATERIAL PRESENTADO COMO ANEXO A LA MISMA, SERÁ LA BASE DEL CONSENTIMIENTO DEL ASEGURADOR PARA EL PERFECCIONAMIENTO DEL CONTRATO Y SERÁ PARTE INTEGRANTE DE LA PÓLIZA EN CASO DE EMISIÓN. EL ASEGURADOR TOMARÁ COMO CIERTA LA INFORMACIÓN CONSIGNADA EN ESTA SOLICITUD, INCLUYENDO CUALQUIER MATERIAL PRESENTADO ANEXO A LA PRESENTE PARA LA EMISIÓN DE LA PÓLIZA.

EL REPRESENTANTE AUTORIZADO DEL ENTIDAD DECLARA QUE, EN VIRTUD DE SU CONOCIMIENTO Y DESPUÉS DE UNA INVESTIGACIÓN RAZONABLE, LAS DECLARACIONES CONSIGNADAS EN ESTA SOLICITUD DE SEGURO Y EN CUALQUIER MATERIAL SUMINISTRADO COMO ADJUNTO SON CIERTAS Y COMPLETAS Y SERÁN TENIDAS COMO TAL POR EL ASEGURADOR. SI LA INFORMACIÓN CONSIGNADA EN LA SOLICITUD VARÍA ANTES DE LA FECHA DEL INICIO DE LA VIGENCIA DE LA PÓLIZA, EL ENTIDAD NOTIFICARÁ AL ASEGURADOR DE TALES CAMBIOS, Y EL ASEGURADOR PODRÁ MODIFICAR O RETIRAR CUALQUIER COTIZACIÓN PRESENTADA. EL ASEGURADOR ESTÁ AUTORIZADO PARA HACER INVESTIGACIONES EN RELACIÓN CON ESTA SOLICITUD.

LA INFORMACIÓN SOLICITADA EN ESTA SOLICITUD ES CON FINES DE SUSCRIPCIÓN Y NO CONSTITUYEN AVISO AL ASEGURADOR DENTRO DEL MARCO DE NINGUNA PÓLIZA SOBRE CUALQUIER RECLAMACIÓN O PÉRDIDA ACTUAL O FUTURA.

Firma del Representante o la persona autorizada	
Nombre	**FELIPE AUGUSTO DÍAZ SUAZA**
Date	**22 DE MAYO DE 2026**
Cargo	**DIRECTOR EJECUTIVO**

Si la persona que firma la Solicitud no es el Presidente, Director General, Director Operativo, Director Financiero, el Secretario General, Director de Tecnología e Información, Jefe de Seguridad, Jefe de Privacidad, por favor marque con una X que la persona ha sido designada como directivo del **Entidad** por su Junta Directa o Consejo de Administración.

Firma del Intermediario Representante del Asegurado	
Nombre	
Nombre del intermediario y teléfono	
Fecha	