COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

RESULTADOS DEL SEGUIMIENTO A LA RESOLUCIÓN CRC 5569 DE 2018

INTELIGENCIA Y ANALÍTICA DE DATOS

Junio de 2022

www.crcom.gov.co
@CRCCol /CRCCol /CRCCol CRCCOL

CONTEXTO

En 2015 la Organización para la Cooperación y el Desarrollo Económico (OCDE) identificó que, para aprovechar los beneficios asociados con el entorno digital, líderes gubernamentales y organizaciones públicas y privadas deben apartarse de abordar la seguridad digital únicamente desde una perspectiva técnica aislada y deben integrar la gestión de riesgos digitales en su proceso de toma de decisiones económicas y sociales[1].

Como iniciativa para lograr la implementación de esta recomendación, el 11 de abril de 2016 se expidió el Documento Conpes 3854 de 2016[2] que estableció la Política Nacional de Seguridad Digital, donde se establecen lineamientos y planes de acción para fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia, considerando la protección del entorno digital como un factor de importancia para preservar la seguridad de la nación y su economía.

En el marco del citado Conpes, se determinó que la Comisión de Regulación de Comunicaciones (CRC) debía realizar una revisión del marco normativo del sector de telecomunicaciones, de acuerdo con sus competencias, en materia de seguridad de las comunicaciones, para apoyar el objetivo de crear las condiciones para que las múltiples partes interesadas gestionen los riesgos de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital. A partir de esto, la CRC incluyó dentro de su Agenda Regulatoria 2017-2018 el proyecto denominado "Revisión del marco regulatorio para la gestión de riesgos de seguridad digital".

Con base en lo anterior, la CRC revisó la regulación que ha expedido en materia de seguridad de las comunicaciones, con el objetivo de crear condiciones para que las múltiples partes interesadas gestionen los riesgos de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital, para de esta manera fortalecer sus capacidades en identificación, gestión, tratamiento y mitigación de los riesgos asociados a la seguridad digital.

Como conclusión de esta revisión, la CRC identificó la necesidad de adaptar la regulación a las mejores prácticas en gestión de riesgos de seguridad de la información, por lo que modificó las disposiciones relacionadas con la seguridad de redes en el Capítulo 1 del Título V de la Resolución CRC 5050 de 2016, a través de la expedición de la Resolución CRC 5569 de 2018[3]. Por medio de esta modificación se actualizaron las previsiones en materia de seguridad digital en el sector de las telecomunicaciones y se alinearon con la visión de responsabilidad compartida y gestión del riesgo de seguridad digital entre las múltiples partes interesadas propuesta en el citado Conpes.

[1] OCDE. (2015). *Digital Security Risk Management for Economic and Social Prosperity*. Recuperado de http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf
[2] Departamento Nacional de Planeación. *Política Nacional de Seguridad Digital, CONPES 3854 de 2016.* Recuperado de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf
[3] Comisión de Regulación de Comunicaciones. *Resolución CRC 5569 de 2018*. Recuperado de: https://normograma.info/crc/docs/resolucion_crc_5569_2018.htm

Dentro de los principales cambios efectuados al marco regulatorio en la Resolución CRC 5569 de 2018, se encuentran los siguientes:

- Se añaden definiciones de acuerdo con la familia de estándares ISO/IEC 27000:2016, sobre incidentes de seguridad y Sistemas de Gestión de Seguridad de la información.

- Se adiciona la obligación para los operadores de implementar un Sistema de Gestión de Seguridad de la Información (SGSI) siguiendo para ello la familia de estándares ISO/IEC 27000.

- Se adiciona la obligación de almacenar hasta por un año información sobre los incidentes de seguridad de la información que incluya por lo menos la fecha del incidente, el servicio afectado, el número de usuarios externos afectados, la duración, la categoría y el nivel de severidad del incidente.

- Se adiciona la obligación de reporte a las autoridades (reporte a colCERT[4]). Para el caso específico de reporte de incidentes en las categorías de mayor impacto, este debe realizarse dentro de las 24 horas hábiles siguientes a la detección.

- Se adopta la clasificación de severidad de incidentes necesaria para determinar la necesidad de reporte a las autoridades según la familia de estándares ISO/IEC 27000.

- Se adiciona un periodo de recolección de información de incidentes por parte de la CRC, el cual inició en enero de 2019 y se reportó en marzo de 2020 (con datos de enero a diciembre 2019).

- Se establecieron dieciocho (18) meses a partir de la publicación como plazo de implementación para los Sistemas de Gestión de Seguridad de la Información y el reporte de incidentes a autoridades.

En particular, esta modificación establece algunas obligaciones a los operadores como la implementación de Sistemas de Gestión de Seguridad de la Información, así como el uso de un marco de autorregulación al momento de definir el alcance de dichos sistemas, de modo que los proveedores de servicios de comunicaciones desarrollen políticas de gestión de seguridad de la información, de acuerdo con su contexto específico de operación y vulnerabilidades.

OBJETIVO DE LA EVALUACIÓN

Bajo el contexto indicado previamente, en la guía de evaluación ex post de la Resolución CRC 5569 de 2019, elaborada por esta Comisión, se estableció el siguiente objetivo general a ser evaluado:

> *Determinar las capacidades de los PRST para identificar, gestionar, tratar y mitigar los riesgos de seguridad de la información.*

[4] Por medio de la Resolución Número 473 de 17 de febrero del 2022, el MinTIC adicionó al artículo 1. de la Resolución MinTIC 2108 del 2020, el Grupo Interno de Trabajo de Respuesta a Emergencias Cibernéticas de Colombia – ColCERT, bajo el Viceministerio de Transformación Digital, para con el fin de articular y coordinar a nivel nacional los aspectos de ciberseguridad a todos los sectores públicos y privados del país.

Para evaluar este objetivo general se generaron cuatro objetivos específicos mediante los cuales se plantea realizar el seguimiento a los resultados de la medida regulatoria en comento:

1. Indagar por la existencia de un marco/estructura razonablemente completa que permita la evaluación y tratamiento integral de riesgos de seguridad de la información de acuerdo con las prioridades comerciales y de seguridad de cada organización.

2. Indagar por la definición formal de los procesos y procedimientos asociados a la gestión de la seguridad de la información.

3. Determinar si se generaron mecanismos para impulsar la cooperación en materia de seguridad digital entre los prestadores de servicios de telecomunicaciones y las múltiples partes interesadas.

4. Determinar si se incentivó el fortalecimiento de los mecanismos y procedimientos para gestionar incidentes asociados a la seguridad de la información por parte de los prestadores de servicios de telecomunicaciones.

LEVANTAMIENTO DE INFORMACIÓN

Para la evaluación de los objetivos planteados respecto de la Resolución CRC 5569 de 2019, en el año 2021 se replicó parte de la encuesta sobre el estado de implementación de los modelos de seguridad digital realizada en 2017 a los Proveedores de Redes y Servicios de Telecomunicaciones (PRST) en el desarrollo del proyecto regulatorio que originó la medida regulatoria. En esta encuesta se indagó por la implementación de estándares y procesos de modelos de seguridad digital, así como en recursos y mecanismos de cooperación implementados por los PRST.

De la encuesta de 2017 se contó con la respuesta de 22 empresas[5], mientras que en la de 2021 con la respuesta de 39. Ambas encuestas fueron enviadas a los PRST partícipes en el proyecto de 2017, incluyendo en la encuesta de 2021 a PRST móviles y fijos con una participación, en el caso de los últimos, de al menos el 0,1% en la cantidad total de accesos nacionales a Internet.

En relación con el primer objetivo específico se comparó el estado de implementación del sistema de gestión de la Seguridad de la Información (SGSI) mediante el estándar ISO 27001/2.

Para el segundo objetivo específico se compararon los procesos y controles que tienen implementados los PRST en relación con aspectos de seguridad digital tales como: disponibilidad, integridad, confidencialidad, autenticación, protección, acceso y no repudio de la información.

Para el tercer objetivo específico se compararon los canales y procedimientos con los que cuentan los PRST para realizar y recibir reportes de fallas de seguridad digital.

[5] En la encuesta de 2017, dada la estructura de la misma no se cuenta con respuestas de todas las empresas para todas las preguntas de interés, por lo que para algunas preguntas solo se cuenta con información de 20 o 21 empresas en 2017.

Finalmente, para el cuarto objetivo específico se compararon los recursos asignados por los PRST y dedicación de estos recursos para gestionar los incidentes de seguridad digital.

En adición a esta encuesta, se cuenta con información de la cantidad de incidentes detectados de 17 empresas para los años 2019 y 2020, la cual ha sido reportada acorde con la estructura definida en la Resolución CRC 5569 de 2019. Esta información no se presenta en este documento al tener el carácter de reservada, pero si está disponible para el ejercicio de las funciones y el desarrollo de proyectos regulatorios de la CRC.

RESULTADOS

A continuación, se presentan los resultados en materia de seguridad y gestión del riesgo digital obtenidos a partir de las encuestas realizadas en 2017 y 2021:

Implementación de un marco para la gestión de la seguridad de la información

De acuerdo con los resultados obtenidos, el estándar ISO 27001/2 fue utilizado por al menos la mitad de las empresas encuestadas en ambos años. Mientras que en 2017 un total de 11 empresas hacían uso de este estándar, en 2021 este número aumentó a 21. De estas empresas, el 71% implementó a 2021 el estándar sin certificación, el 19% certificó ciertas áreas, y el 10% restante indicó estar certificada en todos sus procesos. En comparación con los resultados obtenidos en 2017, se observa que a dicho año la implementación del estándar sin certificación estuvo presente en la respuesta del 46% de las empresas, la certificación de algunas áreas en el 27% y la certificación general de la organización en el 27% restante de las empresas.

Es importante mencionar que aun cuando la encuesta de 2021 evidenció la falta de implementación del estándar por parte de algunos PRST (46%), de la misma no se obtuvieron respuestas con relación al desconocimiento del estándar, mientras que en 2017, 2 de las empresas encuestadas manifestaron no conocer dicho estándar (ver Gráfica 1).

Gráfica 1. Estado de la implementación del estándar ISO 27001/2

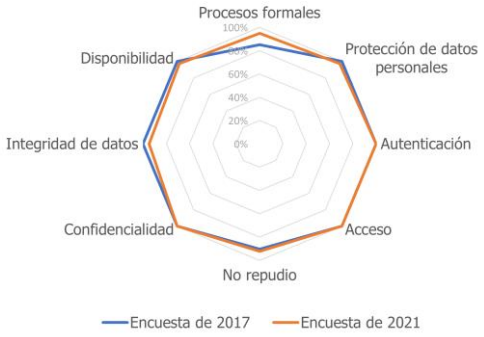
Fuente: Elaboración CRC a partir de los resultados obtenidos de las encuestas realizadas a los PRST.

Procesos asociados a la gestión de seguridad digital

En cuanto al segundo objetivo específico, se encontró que el 95% de las empresas encuestadas en 2021, lo que equivale a 37 empresas, implementaron procesos formales para el tratamiento de incidentes de seguridad. En esta misma materia, cabe anotar que el 85% de las empresas encuestadas en 2017, es decir,

17 empresas, afirmaron implementar procesos formales de este tipo.

Gráfica 2. Porcentaje de respuestas afirmativas a la implementación de procesos y controles para la seguridad de la información



Fuente: Elaboración CRC a partir de los resultados obtenidos de las encuestas realizadas a los PRST.

De otra parte, los resultados de las encuestas realizadas en 2017 y 2021 permitieron evidenciar que todas las empresas encuestadas implementan controles para la autenticación, el acceso y la confidencialidad de la información. Para el año 2021, un porcentaje superior al 92% de las empresas encuestadas implementa controles para la protección de datos personales, disponibilidad, no repudio e integridad de la información tratada por las mismas empresas.

Cabe aclarar que aun cuando se observaron disminuciones en el porcentaje de respuestas afirmativas a la implementación de controles para la protección de datos personales, integralidad y disponibilidad, estas obedecieron a una mayor participación en las respuestas obtenidas por los PRST en la encuesta de 2021 y la cantidad de empresas que no implementan procesos en estos aspectos no es superior a las que no lo hacían en 2017 (ver **¡Error! No se encuentra el origen de la referencia.**).

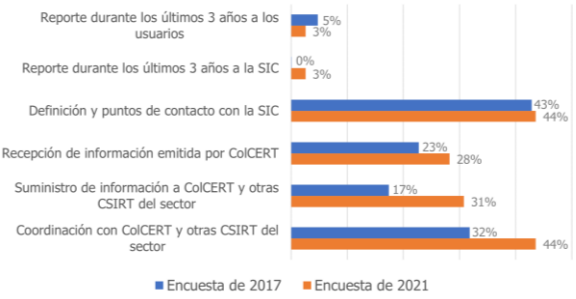
Cooperación en materia de seguridad digital

En lo relacionado con la cooperación entre los PRST y las partes involucradas en el tratamiento de incidentes de seguridad de la información, se encontró que en 2021 la coordinación con ColCERT y/o otras CSIRT[6] del sector fue realizada por el 44% de las empresas encuestadas, mientras que en 2017 dicho valor correspondía al 32% de las empresas. Lo anterior representa un cambio de 7 empresas en 2017 a 17 en 2021. El suministro de información a estas mismas entidades fue realizado por el 31% de las empresas encuestadas en 2021, mientras que en la encuesta de 2017 este porcentaje correspondía al 17% (ver Gráfica 3).

Por su parte, la definición de protocolos y puntos de contacto con la Delegatura para la Protección de Datos personales de la Superintendencia de Industria y Comercio (SIC) fue coordinado por 17 de las empresas encuestadas en 2021 (44%), mientras que el reporte de incidentes a esta misma entidad durante los tres últimos años fue realizado por solo una de estas empresas. En la encuesta realizada en 2017, el reporte de incidentes a la SIC fue nulo aun cuando el porcentaje de coordinación con esta entidad, para la definición de protocolos y puntos de atención, fue realizado por el 43% de la muestra, correspondiente a 9 empresas.

[6] Equipo de Respuesta a Incidentes de Seguridad Informática, por sus siglas en inglés.

Gráfica 3. Porcentaje de respuestas afirmativas al reporte, suministro y cooperación de información con las partes interesadas



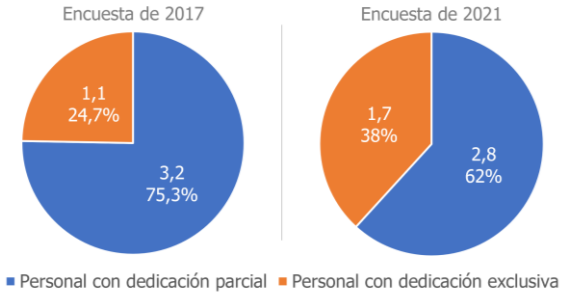
Fuente: Elaboración CRC a partir de los resultados obtenidos de las encuestas realizadas a los PRST.

Gestión de incidentes por parte de los PRST

En lo referente al cuarto objetivo específico, se identificó que el 48,7% de la muestra encuestada en 2021, lo que representa 19 empresas, contaban con un equipo dedicado de manera exclusiva a la gestión de incidentes de seguridad informática, mientras que en 2017 el 36,4% de las empresas encuestadas contaban con este recurso, equivalente a 8 empresas. De ambos grupos de empresas encuestadas, 2 manifestaron que no contaban con ningún responsable para la gestión de incidentes.

Los equipos dedicados a atender estos incidentes no presentaron un gran cambio, al pasar de tener 4,3 personas en promedio en 2017 a 4,5 personas en 2021. Como se evidencia en la gráfica 4, entre estos años se dio un cambio en la composición de estos equipos pasando de tener el 24,7% dedicado de manera exclusiva en 2017 al 38,2% en 2021. En adición al incremento de personal, el presupuesto promedio destinado a la gestión de incidentes de seguridad de la información de las empresas que aportaron información[7] paso de 374,6 millones en 2017 a 594 millones en 2021[8].

Gráfica 4. Personal responsable de la gestión de incidentes de seguridad informática



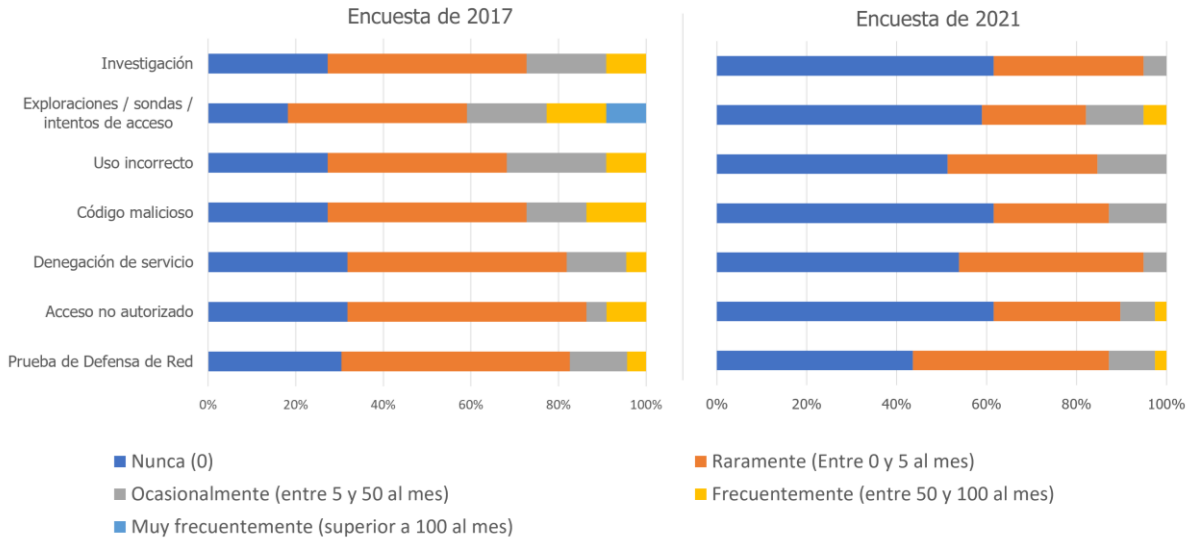
Fuente: Elaboración CRC a partir de los resultados obtenidos de las encuestas realizadas a los PRST.

Los anteriores incrementos en los recursos disponibles para la gestión de estos incidentes se ven reflejados en una disminución de la frecuencia con que se presentan y se deben atender distintos tipos de incidentes. En la Gráfica 5 se puede observar como en la mayoría de las tipologías de incidentes de seguridad informática, exceptuando las pruebas de defensa de red, más del 50% de los PRST reportaron que en 2021 nunca se presentaron ni debieron atender incidentes, mientras que en 2017 al menos el 40% de los PRST debían atender hasta 5 incidentes al mes en cada una de las tipologías señaladas.

Por otra parte, mientras que en 2017 al menos uno de los PRST debía gestionar incidentes en alguna de las tipologías establecidas en la Gráfica 5 de manera frecuente, para 2021 esto solo ocurrió para los incidentes relacionados con exploraciones, sondas o intentos de acceso, accesos no autorizados y pruebas de defensa de red.

[7] Para el año 2017 se contó con información de 12 empresas y para el 2021 fueron 27 las empresas que aportaron esta información, las demás empresas argumentaron no contar con la información desagregada.
[8] Los valores se presentan en pesos constantes de 2021 ajustados mediante el Índice de Precios al Consumidor del DANE.

Gráfica 5. Frecuencia en la gestión de incidentes de seguridad informática



Fuente: Elaboración CRC a partir de los resultados obtenidos de las encuestas realizadas a los PRST.

CONCLUSIONES

Respecto de los objetivos planteados a partir de la guía de evaluación ex post de la Resolución 5569 de 2019 y a los cuales se hizo seguimiento a partir de la encuesta realizada a los agentes interesados descrita en la sección "Levantamiento de información" y los resultados presentados en este documento, se puede concluir lo siguiente:

- Existe un mayor conocimiento e implementación del estándar ISO 27001/2 por parte de los PRST. Sin embargo, solo el 15% de los PRST que cuentan con la certificación de los estándares ISO relacionados con los sistemas de gestión de la seguridad de la información en todas o algunas áreas de su organización, y estos no han aumentado desde el 2017.
- Se evidencia la adopción de mejores prácticas en la gestión de incidentes de seguridad de la información mediante una mayor implementación de procesos formales para la gestión de estos incidentes por parte de los PRST.
- Se evidenció una mayor cooperación en materia de seguridad digital al presentarse un incremento en los mecanismos y procesos relacionados con la coordinación y compartición de información entre los PRST y las partes involucradas en el tratamiento de incidentes de seguridad de la información.
- Se evidenció un crecimiento en los recursos tanto de personal con dedicación exclusiva como financieros de los PRST para la gestión de incidentes de seguridad de la información, lo que a su vez se ve reflejado en una reducción de la frecuencia en la ocurren y que se deben gestionar estos incidentes en todas las tipologías evaluadas.

Lo anterior muestra que la Resolución CRC 5569 de 2018 alcanzó sus objetivos en la medida que se evidencia un mayor conocimiento e implementación de los estándares ISO 27001/2 por parte de los PRST, lo que se traduce en un incremento de los procesos formales para la gestión de incidentes de seguridad, una mayor cooperación entre los agentes interesados en esta materia del sector y el fortalecimiento de los mecanismos y recursos de los PRST para identificar, gestionar, tratar y mitigar los riesgos de seguridad de la información.

En adición a lo anterior, es importante mencionar que la existencia de un marco regulatorio actualizado para la gestión de riesgos de seguridad digital como el establecido en la Resolución CRC 5569 de 2019 permite contar con información estadística que aporte al desarrollo de políticas públicas y regulatorias de seguridad digital, y que contribuya a mejorar los planes generales de gestión de incidentes de seguridad de la información de los PRST.

ANEXO

Listado de operadores que participaron en las encuestas:

No.	Empresa Participante	Año Encuesta(s)
1	Cablevision S.A.S.	2017
2	Empresa de Telecomunicaciones de Bucaramanga S.A. E.S.P.	
3	Gilat Colombia S.A. E.S.P.	
4	Metrotel S.A. E.S.P.	
5	Supernet TV Telecomunicaciones S.A.S.	
6	TV Cable San Gil S.A.S.	
7	Axess Networks Solutions Colombia S.A.S.	2017 y 2021
8	Azteca Comunicaciones Colombia S.A.S.	
9	Betel Soluciones S.A.S.	
10	Colombia Telecomunicaciones S.A. E.S.P BIC	
11	Columbus Networks de Colombia S.A.S.	
12	Comunicacion Celular S.A. - Comcel S.A.	
13	Directv Colombia Ltda.	
14	Edatel S.A./Colombia Móvil S.A. E.S.P./Une Epm Telecomunicaciones S.A.	
15	Empresa de Recursos Tecnológicos S.A. E.S.P.	
16	Empresa de Telecomunicaciones de Bogotá S.A. E.S.P.	
17	Empresas Municipales de Cali E.I.C.E. E.S.P.	
18	HV televisión S.A.S.	
19	IFX Networks Colombia S.A.S.	
20	Infraestructura y Servicios de Colombia S.A.S.	
21	Skynet de Colombia S.A.S E.S.P.	
22	Sol Cable Visión S.A.S. E.S.P.	
23	Almacenes Éxito Inversiones S.A.S.	2021
24	Avantel S.A.S - En reorganización	
25	CODISERT S.A.	
26	Colombia Mas TV S.A.S.	
27	conexión Digital Express S.A.S.	
28	Conexiones tecnológicas y comunicación S.A.S.	
29	Dobleclick Software e Ingenieria S.A.S.	
30	Eme Ingenieria S.A.	
31	Energía Integral Andina S.A.	
32	Hughes de Colombia S.A.S.	
33	Kalu de Colombia S.A.S.	

No.	Empresa Participante	Año Encuesta(s)
34	Lecarvin S.A.S.	
35	Legon Telecomunicaciones S.A.S.	
36	Logística Flash Colombia S.A.S.	
37	Media Commerce Partners S.A.S.	
38	NET ISP S.A.S.	
39	Partners Telecom Colombia S.A.S.	
40	Ruralink S.A.S.	
41	SP Sistemas Palacios Ltda.	
42	Suma Móvil S.A.S.	
43	TV SANV S.A.S.	
44	Virgin Mobile Colombia S.A.S.	
45	WISP Ingenieria S.A.S.	