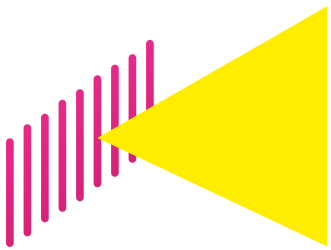
IMPACTO DE LOS INCIDENTES DE SEGURIDAD DIGITAL

EN COLOMBIA 2017

BID Mejorando vidas

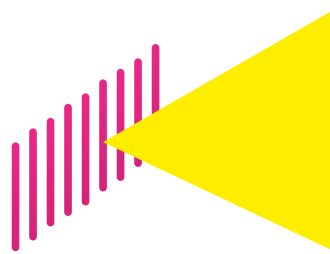
MINTIC

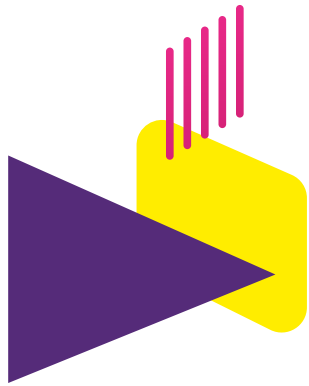
OEA Más derechos para más gente



IMPACTO DE LOS INCIDENTES DE SEGURIDAD DIGITAL

EN COLOMBIA 2017





Este estudio cuenta con el apoyo financiero del gobierno de Canada

CRÉDITOS

DAVID LUNA
Ministro de Tecnologías de la Información y las Comunicaciones de Colombia (MINTIC)

LUIS ALMAGRO
Secretario General de la Organización de los Estados Americanos (OEA)

EQUIPO TÉCNICO MINTIC
Juanita Rodríguez
Orlando Garcés
Antonio Carrillo

EQUIPO TÉCNICO OEA
Claudia Paz y Paz
Alison August Treppel
Belisario Contreras
Bárbara Marchiori de Assis
Kerry-Ann Barrett
Jorge Bejarano
Harold Coronado

EQUIPO TÉCNICO BID
Ana María Rodríguez-Ortiz
Carlos Santiso
Javier León
Miguel Porrúa
Florencia Cabral

COLABORADORES
Danil Kerimi
Lara Pace
Andres Galindo
Gonzalo Romero

ENTIDADES COLABORADORAS

Asociación Bancaria y de Entidades Financieras de Colombia
-ASOBANCARIA-
Asociación Colombiana de las Micro, Pequeñas y Medianas Empresas
-ACOPI-
Asociación Nacional de Empresarios de Colombia -ANDI-
Asociación Nacional de Empresas de Servicios Públicos y Comunicaciones
-ANDESCO-
Cámara Colombiana de Comercio Electrónico -CCCE-
Cámara Colombiana de Informática y Telecomunicaciones -CCIT-
Centro Cibernético Policial de la Policía Nacional -CCP-
Comando Conjunto Cibernético del Comando General de las Fuerzas
Militares -CCOC-
Comisión de Regulación de Comunicaciones -CRC-
Confederación Colombiana de Cámaras de Comercio -CONFECAMARAS-
Consejo Nacional Gremial -CNG-
CSIRT de la Policía Nacional -CSIRT PONAL-
Departamento Administrativo Dirección Nacional de Inteligencia -DNI-
Departamento Nacional de Planeación
Federación Colombiana de la Industria de Software y Tecnologías de la
Información -FEDESOFT-
Federación Nacional de Comerciantes -FENALCO-
Grupo de Respuesta a Emergencias Cibernéticas -colCERT-
Ministerio de Defensa Nacional
Ministerio de Justicia y del Derecho
Ministerio de Relaciones Exteriores
Ministerio de Tecnologías de la Información
y las Comunicaciones
Presidencia de la República

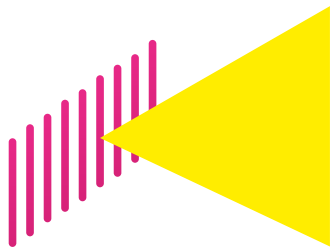
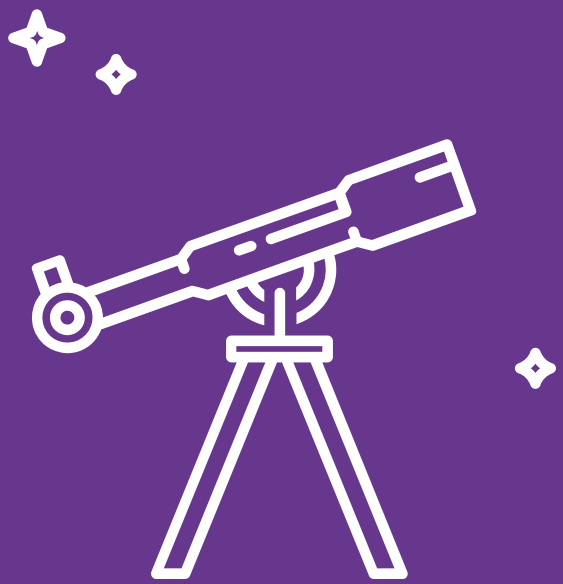


TABLA DE CONTENIDO

TABLA DE CUADROS

TABLA DE GRÁFICOS

TABLA DE GRÁFICOS



PRINCIPALES CONCLUSIONES Y OBSERVACIONES

PRINCIPALES CONCLUSIONES Y OBSERVACIONES

Este estudio fruto de la colaboración entre el MINTIC, la OEA y el BID representa una iniciativa pionera en la región y poco frecuente a nivel mundial, ya que releva información sobre las amenazas para la seguridad digital de un país y su capacidad de defenderse ante las mismas que resulta difícil de recolectar. El gobierno de Colombia se sitúa así en la vanguardia de la generación de conocimiento en el área de la seguridad digital que facilite el diseño y la implementación de políticas que atiendan los aspectos más débiles del escenario que muestra este estudio.

La información recogida permite tener una visión completa de los ataques que sufren tanto el sector público como el privado, así como su nivel de preparación para defenderse de dichos ataques. El estudio hace un esfuerzo por presentar la información en función de los diferentes perfiles de las instituciones tanto públicas como privadas y se han utilizado numerosas herramientas estadísticas para facilitar al lector la extracción de sus propias conclusiones.

Las organizaciones colombianas que participaron en este estudio presentan, en su mayoría, un alto nivel de conectividad. De las empresas entrevistadas, 65% indicaron que entre el 81% y el 100% de su fuerza laboral contaba con acceso a Internet. En el sector público, 69% de las entidades participantes indicaron que entre el 81% y el 100% de sus empleados tenían acceso a Internet en el trabajo.

Cuando se pregunta a las organizaciones colombianas si creen que están preparadas para hacer frente a un incidente digital, un promedio simple del 37% de las empresas que participaron del estudio (empresas de los sectores Servicios, Industria y Comercio) creen que estaban preparadas para manejar un incidente digital. En cuanto al tamaño de estas empresas, el 70% de las grandes empresas se sienten muy preparadas o preparadas para gestionar un incidente digital, frente al 45% de las microempresas. Cuando se realiza la misma pregunta a las entidades públicas, uno de los resultados encontrados es que la mayoría de las entidades a nivel nacional se sienten preparadas. Los participantes del estudio en el nivel nacional indicaron que

el 13% y el 48%, se sentían muy preparados o preparados, respectivamente. No obstante, cuando se compara con las entidades territoriales de orden municipal y departamental, los datos muestran que tan solo el 28%, a nivel municipal, y el 38%, a nivel departamental, se sintieron muy preparados o preparados para manejar un incidente. Se observa que existe un nivel más alto de confianza en la preparación a nivel nacional, y que sería interesante desarrollar iniciativas de política pública enfocadas al nivel departamental y municipal.

El Estudio también incluyó preguntas específicas sobre las medidas de seguridad digital adoptadas por la organización, esto con el objetivo de poder hacer una comparación con su nivel de percepción de seguridad. **Se observó que, de manera general, las organizaciones colombianas que contestaron que se sienten preparadas, de hecho, adoptan más medidas de seguridad que las demás organizaciones**. Por ejemplo, **las grandes empresas tienden a adoptar más medidas de seguridad que una microempresa, así como las entidades públicas nacionales tienen una preocupación más grande con la seguridad digital que las entidades de orden territorial**. Sin embargo, las organizaciones que se sienten más preparadas aún necesitan incrementar sus medidas de seguridad digital, lo que debe incluir una asignación presupuestal más grande para asuntos en materia de seguridad digital.

Entre las medidas más importantes que se pudieron identificar para asegurar a una organización colombiana contra los incidentes digitales es la identificación de un cargo con dedicación exclusiva para el manejo de incidentes digitales. Este cargo es importante ya que les ayudará a las entidades a detectar, aislar y resolver incidentes rápidamente cuando ocurran.

Entre todos los que respondieron a la pregunta ¿Tiene su entidad/empresa un área, cargo (s) o rol(es) dedicado(s) a la seguridad digital (seguridad digital y/o de seguridad de la información)?, 70% de las grandes empresas respondieron que sí comparado con poco más del 20% de las microempresas. Entre sectores económicos, la mayoría de empresas del sector Industria dijo tener un equipo con dedicación exclusiva, con un poco más del 54% respondiendo positivamente a la pregunta, frente a solo el 45% y el 42% de las empresas de los sectores de Servicios y Comercio, respectivamente. Entre las entidades públicas, solo el 33% a nivel nacional y el 10% y 17% a nivel municipal y departamental, respectivamente, tienen un área dedicada a la seguridad digital dentro de su organización. Se observó que existe una tendencia general a transferir la responsabilidad de la respuesta a incidentes y la seguridad digital bajo las

funciones generales de los departamentos de tecnología de la información.

Cuando se pregunta, en una escala de 1-5, lo que los entrevistados creen que son los principales factores que afectarían su capacidad de abordar la seguridad digital, **la falta de personal con dedicación exclusiva al área y la falta de presupuesto fueron clasificados como más altos, con la falta de conciencia de los empleados inmediatamente después**. De hecho, los análisis de la asignación presupuestal a asuntos de seguridad digital confirmaron esta preocupación de los entrevistados, como se observa más abajo.

Tener la capacidad de identificar incidentes es importante para las entidades, ya que es el primer paso para poder contener un ataque malicioso y poder responder. Cuando se pregunta si se han identificado incidentes digitales contra su organización en el año 2016, **más del 70% de las microempresas contestaron que no han identificado incidentes digitales**. Entre las pequeñas empresas, aproximadamente el 60% tampoco identificaron incidentes digitales. Sin embargo, entre las medianas y grandes empresas, la mayoría de las empresas contestaran que sí identificaron incidentes digitales: 51% y 63%, respectivamente. Al analizar los distintos sectores económicos, solamente en el sector Industria la mayoría de las empresas identificaron los incidentes digitales: 52% de las empresas. Con respecto a las entidades estatales, el 59% de las entidades de orden nacional identificaron incidentes digitales, mientras que un 56% de las entidades de orden territorial departamental respondieron de la misma forma. Por otro lado, 42% de las entidades de orden territorial municipal contestaron que han identificado los incidentes digitales.

Se identificó una relación estadísticamente significativa positiva entre la implementación de medidas técnicas como pruebas de vulnerabilidad y mantenimiento de la infraestructura de Tecnologías de la Información y la identificación de incidentes digitales por las organizaciones públicas y privadas. Así también se aprecia con la variable explicativa relativa a la práctica de evaluación de riesgo cibernético. Es decir, organizaciones que implementan más medidas de seguridad digital tienden a identificar un número más grande de incidentes digitales. Esto significa que muchas organizaciones que no implementan estas medidas no tienen el conocimiento de que son blancos de ataques cibernéticos. Asimismo, se observó una relación estadísticamente positiva al conocer de la Política Nacional de Seguridad Digital (Documento CONPES 3854 de 2016), aprobado el 11 de abril de 2016, y la identificación de incidentes digitales por las entidades estatales.

En cuanto a los tipos de incidentes que se están experimentando, los participantes del estudio indicaron en su respuesta a la pregunta, ¿Qué tipos de incidentes digitales, amenazas cibernéticas o ataques cibernéticos ha identificado su entidad/ empresa durante el año 2016?, que el malware y el phishing se encontraban entre los tipos de incidentes más comunes. Se observó que, dentro del sector de Servicios, el 50% de los que respondieron notaron un aumento en los ataques de malware, 47% de phishing, 39% de ataques basados en web y 18% de ataques de denegación de servicio. En el sector Comercio, se hicieron observaciones similares con un 53% reportando un incremento en el malware, un 41% reportó un aumento en el phishing y un 21% notó un incremento tanto en ataques basados en web como en ataques de denegación de servicio. Curiosamente, sin embargo, hubo algunas variaciones dentro del sector Industria en esta observación, ya que el 67% reportó un incremento en la gravedad de los ataques basados en web y el malware y el 59% reportó un aumento en los ataques de phishing. En términos de entidades que identifican realmente no solo el aumento en gravedad sino el tipo de ataques, los participantes del estudio indicaron que han visto un mayor aumento en ataques de phishing y malware.

Al analizar los valores de las empresas que asignaron algún presupuesto a la seguridad digital, **se observó que la mediana del presupuesto de la seguridad digital en relación a las ventas de las empresas fue aproximadamente 0,3% de las ventas en 2016**. Las microempresas tienen presupuestos para la seguridad digital más pequeños en términos absolutos. Por otro lado, las empresas del sector de Servicios (principalmente del sector financiero) tienden a asignar un presupuesto más grande a la seguridad digital.

En las entidades públicas, la estimación de la mediana del presupuesto asignado a la seguridad digital en relación al presupuesto de inversión fue aproximadamente 0,05% del total de las inversiones en 2016.

Es decir, cuando se asignó presupuesto a la seguridad digital, este presupuesto no llegó a 1% de las ventas o inversiones de las organizaciones en 2016. Además, se verificó que, en promedio simple, la mayor parte del presupuesto fue asignado para plataformas y medios tecnológicos, mientras la generación de capacidades recibió la menor cantidad de recursos tanto en las organizaciones públicas como en las privadas. Cabe recalcar que la generación de capacidades incluye temas como capacitación y concientización de los empleados y funcionarios. Como se mencionó, la falta de personal con dedicación exclusiva al área y la falta de presupuesto fueron clasificados como los principales factores que afectaron la

seguridad digital en las organizaciones, siedo la falta de conciencia de los empleados inmediatamente después.

Es importante señalar que muchas de las organizaciones no estiman el costo de los incidentes digitales: 79% de las empresas afirmaron que no contaban con ningún costo estimado, mientras el 85% de las entidades públicas afirmaron que no hacen ningún tipo de estimación. En este contexto, se realizaron estimaciones en base a las organizaciones que sí estimaron el costo de los incidentes digitales.

Se logra observar que el costo relativo con incidentes digitales disminuyó a medida que las empresas aumentan de tamaño. Aunque las grandes empresas tuvieron un costo absoluto con incidentes digitales muy superiores que los costos incurridos por una microempresa, por ejemplo, el costo relativo con incidentes digitales de una gran empresa fue significativamente más pequeño. **Es muy importante notar que hay un número más grande de empresas con costos relativos a la pérdida de propiedad intelectual por encima de los $325 millones de pesos colombianos: cerca de 10% de las empresas, siendo que 3% presentaron pérdidas a la propiedad intelectual de más de COP $4.000.000.000.** En este último grupo, la mayoría consistió en grandes empresas, incluyendo empresas del sector Comercio, y del sector financiero.

Los resultados indican que existe una relación significativa y positiva entre el costo y el número de incidentes. **Según el modelo, se estima que el incremento de una unidad en el número de incidentes aumenta en aproximadamente COP $500 mil pesos colombianos el costo incurrido por las empresas en Colombia como resultado de incidentes digitales. Es importante tener en cuenta que este valor es una estimación a partir de la información reportada y que algunos incidentes pueden tener valores más bajos, mientras otros más altos.**

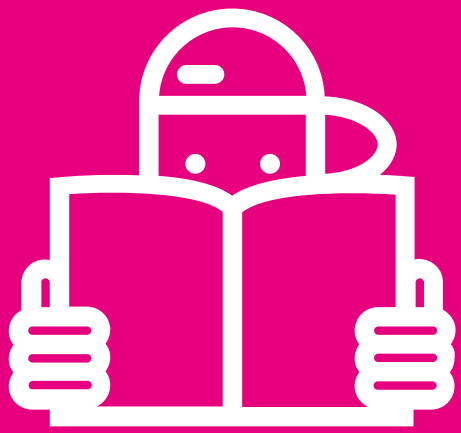
En relación a las entidades estatales nacionales, el costo representó aproximadamente 0,5% de la inversión de las entidades públicas. No obstante, estos datos se refieren a las entidades estatales de orden nacional de la rama ejecutiva o a entes autónomos nacionales. No hubo un número significativo de entidades territoriales que respondieran la información acerca del costo.

En resumen, se puede concluir que las adopciones de medidas de seguridad digital son esenciales no sólo para protegerse, sino también para tener una mejor comprensión acerca del impacto de los incidentes digitales en las organizaciones colombianas. **Aunque muchas organizaciones afirmaron estar preparadas para los incidentes digitales, muchas organizaciones no tienen personal dedicado a la seguridad digital**, con la tendencia general a transferir la responsabilidad de la respuesta a incidentes y la seguridad digital bajo las funciones generales de los departamentos de TI.

La asignación presupuestal a la seguridad digital es menos de 1% de las ventas/inversiones de las organizaciones y, cerca de 10% de este 1% es asignado a temas de capacitación y concientización. Esto es preocupante, principalmente cuando se observa que la mayoría de las organizaciones que participan del estudio tienen cerca de 81% a 100% de sus empleados y funcionarios conectados al Internet, y con el aumento de la gravedad de los ataques de phishing y malware, que pueden tener como blanco cualquier persona dentro de la organización.

Los datos recabados muestran que los ataques cibernéticos aumentan en sofisticación e impacto mientras que la actualización de los recursos humanos y tecnológicos para defenderse y las dotaciones presupuestarias enfocadas en la seguridad digital son aún pequeñas y crecen con lentitud. La gravedad de las amenazas y el daño que generan demandan acciones urgentes en las cuales el sector público y el privado colaboren estrechamente.

A partir del análisis de las distintas organizaciones colombianas, se pudo observar que las grandes empresas están más preparadas y, aunque los costos absolutos de los incidentes digitales son más altos, sus costos relativos son más pequeños que los costos de las microempresas. Es decir, se estima que los costos de los incidentes digitales tienen un impacto más grande en las microempresas. Con respecto a las entidades estatales, se nota la relación estadísticamente positiva en conocer la Política Nacional de Seguridad Digital (Documento CONPES 3854 de 2016) e identificar incidentes digitales, principalmente entre las entidades nacionales. Sería interesante desarrollar acciones de política de seguridad digital con un enfoque particular en las entidades de orden territorial.



GUÍA DEL LECTOR

GUÍA DEL LECTOR

El propósito de este instrumento elaborado por el Gobierno de Colombia, a través del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), la Organización de los Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID), es obtener información sobre las amenazas de seguridad digital (seguridad cibernética y/o seguridad de la información) y su impacto en el país.

La Política Nacional de Seguridad Digital, aprobada el pasado 11 de abril de 2016 por el Consejo Nacional de Seguridad Digital, mediante la expedición del Documento CONPES 3854 de 2016, informó sobre la necesidad de ***"Crear las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital***". En este contexto, este estudio servirá de insumo del gobierno nacional para generar instrumentos pertinentes en relación al cumplimiento de la política definida y la priorización del desarrollo de los planes futuros en la materia. Más específicamente, este estudio permitirá identificar cuáles son los principales incidentes, amenazas y ataques contra la seguridad digital (seguridad cibernética y/o seguridad de la información) que están afectando al país, reconocer sus principales blancos u objetivos y conocer los costos económicos que estos representan para los diferentes sectores de la economía del país y del Gobierno, entre otros. Por lo tanto, este estudio pretende identificar cómo están afectando los incidentes de seguridad digital a las organizaciones colombianas tanto del sector privado, como del sector público y ha tomado como base cifras del año 2016.

El estudio se divide en dos partes de la siguiente manera:

PARTE 1) Análisis del Sector Privado: este análisis se divide en cinco secciones. La primera sección del análisis ofrece información acerca del perfil de las empresas colombianas, tal como el tamaño, el número de empleados, el sector económico y el porcentaje aproximado del personal de la empresa que tiene acceso a Internet para desarrollar sus actividades profesionales. Con estos datos, se pudo analizar la seguridad digital de las empresas teniendo en cuenta sus distintos perfiles. La segunda sección del análisis presenta información sobre las medidas de seguridad digital adoptadas por las

empresas, tal como medidas técnicas, políticas organizacionales y gestión del riesgo de la seguridad digital. La tercera sección describe los incidentes digitales enfrentados por la empresa durante el período de tiempo analizado. La cuarta sección estima el presupuesto asignado por la empresa a asuntos de seguridad digital y, finalmente, la última sección busca identificar los costos generados por las consecuencias de los incidentes digitales.

PARTE 2) Análisis de Entidades del Sector Público: de manera similar al análisis del sector privado, este análisis se divide en cinco secciones. La primera proporciona un resumen del perfil las entidades públicas colombianas entrevistadas, e incluye información acerca del orden a que pertenece la entidad, número de personal, y porcentaje del personal de la entidad con acceso a Internet. La segunda sección describe las medidas de seguridad digital adoptadas por las distintas entidades, mientras la tercera ofrece una descripción de los tipos de incidentes vividos durante el periodo de tiempo analizado por las entidades entrevistadas. La cuarta sección describe la asignación presupuestal, y la última parte analiza los costos generados debido a los incidentes digitales.

ANEXO 1) Análisis Situacional: ofrece una visión general del panorama de seguridad digital de Colombia e incluye un análisis de la situación de la capacidad de seguridad digital en Colombia, tomando como base los resultados del Informe elaborado por la OEA, el BID, y el Centro de Capacidad Global sobre Seguridad Cibernética de la Universidad de Oxford, titulado ***Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?*** Los niveles de madurez descritos en ese Informe cubren cinco dimensiones: (1) Política y Estrategia; (2) Cultura y Sociedad; (3) Educación; (4) Marcos Legales; y (5) Tecnologías. El análisis situacional también proporciona información sobre los avances realizados en relación con la seguridad digital y otras actividades relacionadas con el campo de la seguridad digital.

ANEXO 2) Metodología: describe la metodología adoptada para este Estudio. Incluye la lógica para el desarrollo de las preguntas planteadas en el instrumento de recolección de información utilizado, así como la metodología de distribución adoptada.

ANEXO 3) Análisis estadístico complementario: presenta los resultados de las regresiones lineales conducidas en este Estudio, así como las estimaciones de los modelos LOGIT adoptados.

PRÓLOGO

DAVID LUNA

MINISTRO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA (MINTIC)

IMPACTO DE LOS INCIDENTES, AMENAZAS Y ATAQUES CIBERNÉTICOS EN COLOMBIA

El desarrollo de economías digitales sólidas que contribuyan a la generación de prosperidad económica y social en América Latina y el Caribe requiere de la construcción de un entorno digital abierto y, al mismo tiempo, seguro y confiable, acorde con el aumento y dinamismo de las actividades digitales de sus ciudadanos. Para ello, los países de nuestra región deben contar con una visión estratégica respecto a la seguridad digital y a la gestión de los riesgos asociados a los incidentes y amenazas que puedan atentar contra la integridad de los miembros de la sociedad, el Estado Social de Derecho, el ejercicio de los derechos fundamentales, la seguridad nacional, la defensa nacional y la soberanía.

En el caso de Colombia, el creciente uso de Tecnologías de la Información y las Comunicaciones (TIC); el aumento de conexiones a Internet ; la masificación de las redes de telecomunicaciones como base para cualquier actividad socioeconómica, y el incremento en la oferta de servicios disponibles en línea , evidencian un incremento significativo en la participación de los colombianos a través de canales electrónicos.

No obstante, el exponencial uso del entorno digital acarrea incertidumbres y riesgos inherentes de seguridad digital que, de no ser gestionados adecuada y oportunamente, pueden derivar en incidentes, amenazas y ataques cibernéticos, con graves consecuencias de tipo económico o social para el país.

Dado lo anterior, y mediante la identificación de una clara problemática por resolver, Colombia expidió su Política Nacional de Seguridad Digital (documento CONPES 3854 de 2016), liderada por los ministerios de Defensa Nacional y de Tecnologías de la Información y las Comunicaciones de Colombia y con el concurso de todas las partes interesadas. Esta es una de las primeras políticas nacionales en el mundo y la primera en la región en acoger las recomendaciones en gestión de riesgos de seguridad digital emitidas en septiembre de 2015 por la Organización para la Cooperación y el Desarrollo Económicos (OECD). Asimismo, este documento incorporó las recomendaciones de otros organismos internacionales como la

Organización de Estados Americanos (OEA), la Unión Internacional de Telecomunicaciones (UIT) y la Organización del Tratado del Atlántico Norte (OTAN).

La Política articula una visión estratégica que busca que el gobierno nacional y los territoriales, las organizaciones públicas y privadas, la Fuerza Pública, los propietarios u operadores de las infraestructuras críticas cibernéticas nacionales, la academia y la sociedad civil hagan un uso responsable del entorno digital y fortalezcan sus capacidades 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.

Con el fin de contar con insumos fundamentales para generar documentos estratégicos y priorizar las acciones por parte del gobierno nacional, el Ministerio TIC de Colombia, la OEA y el Banco Interamericano de Desarrollo, en conjunto con expertos nacionales e internacionales en la materia, han adelantado este estudio titulado Impacto de los incidentes, amenazas y ataques cibernéticos en Colombia, el cual presenta un panorama actual de la seguridad digital (seguridad cibernética y/o seguridad de la información) en Colombia; identifica los principales tipos de incidentes, amenazas y ataques contra la misma que afectan a entidades del sector público y a empresas; reconoce sus principales blancos u objetivos, y estima, de manera general, algunos costos económicos que estos representan para los diferentes sectores de la economía del país.

El gobierno nacional de Colombia está convencido de que la gestión de riesgos de seguridad digital es requisito fundamental para los procesos de digitalización sectorial y transformación digital del país, y se constituye en una valiosa herramienta para el afianzamiento de la paz, el fortalecimiento de la confianza, la masificación del Internet, la reducción de la pobreza y la consolidación de la economía digital.

Por esta razón, y a partir de los resultados presentados en este estudio, es necesario que los líderes de las organizaciones públicas y privadas de Colombia y de la región revisen en detalle las medidas de seguridad digital implementadas hasta hoy y su nivel de inversión, con el fin de adaptar sus modelos de administración y negocio para maximizar las oportunidades en el desarrollo de las actividades socioeconómicas en el entorno digital.

1 En Colombia se multiplicó por 11 el número de conexiones a Internet, pasando de 2,6 millones en 2010 a 28,7 millones en 2017. Con 15,6 millones de conexiones de Internet de Banda Ancha en 2017, el país logró un incremento del 609 % frente al 2010, acercándose a niveles de acceso similares a países que pertenecen a la OCDE, como Portugal, Turquía e Israel, y muy por encima del promedio de crecimiento de los países de América Latina y el Caribe.

2 El país cuenta con una red nacional de fibra óptica y se avanza en la conexión de zonas apartadas del territorio nacional, a través de la red de alta velocidad. Actualmente, más de 160 mil hogares cuentan con Internet a tarifas sociales y se han instalado más de 1.300 nuevos Kioscos Vive Digital en zonas rurales, 37 laboratorios para desarrollar videojuegos, aplicaciones y contenidos digitales y más de 750 zonas WiFi gratis.

3 Se estima que el 26 % de las micro, medianas y pequeñas empresas (MiPyme) colombianas compran en línea y el 8 % venden por Internet.

CLAUDIA PAZ Y PAZ

SECRETARIA DE SEGURIDAD MULTIDIMENSIONAL DE LA OEA

Las amenazas de ciberseguridad son ahora una parte de nuestra realidad cotidiana. Las naciones soberanas deben considerar ahora su desarrollo y sus inversiones económicas en el marco de un mundo digital.

Según cálculos del sector, el gasto mundial en productos y servicios de seguridad de la información llegará a USD $86.400 millones en 2017, un incremento del 7 por ciento desde 2016, con un gasto esperado de USD $93.000millones en 2018. Más alarmante es el hecho de que se prevé que el gasto mundial en productos y servicios de seguridad digital exceda USD $1 billón en los próximos cinco años, 2017-2021.

Con más de una década de experiencia en el campo de la ciber seguridad, la Organización de los Estados Americanos (OEA) proporciona a los Estados Miembros investigaciones y estudios exhaustivos sobre la ciber seguridad en América Latina y el Caribe.

Es en esta línea, que presentamos este reporte sobre las prácticas de seguridad digital y el impacto de los incidentes cibernéticos en las organizaciones colombianas.

Desde el año 2016, la OEA y el Ministerio de Tecnologías de la Información y Comunicaciones de Colombia (MINTIC) han estado cooperando con el propósito de brindar asistencia técnica en la realización de un estudio como éste.

La OEA, a través del Comité Interamericano contra el Terrorismo (CICTE), trabajó en estrecha colaboración con el Gobierno colombiano para obtener aportes de los actores nacionales a lo largo del proceso de desarrollo del informe.

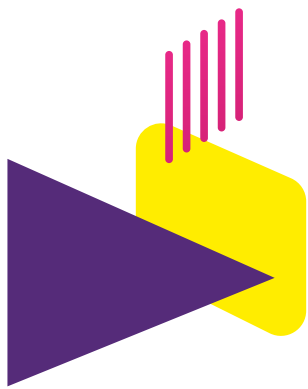
Los resultados del informe evidencian que la gran mayoría de las empresas y entidades estatales no realizan una evaluación de riesgo de la seguridad digital, y cuando se les preguntó bajo qué departamento se manejaba la seguridad digital, la gran mayoría respondió que era manejada por el departamento de tecnología y no por un departamento específico de seguridad.

Esto indica la necesidad de que las empresas asignen mayores recursos para la gestión de la seguridad digital a todos los niveles.

El estudio también evidencia la existencia de una significativa correlación entre el costo y el número de incidentes, ya que aun cuando las organizaciones afirman estar preparadas para afrontar incidentes digitales, muchas de ellas no cuentan con el personal dedicado a la seguridad digital, y menos del 1% del presupuesto de las ventas/inversiones de las organizaciones es asignado a la seguridad digital, con alrededor del 10% del mismo asignado a los temas de capacitación y concientización.

Colombia ha demostrado su compromiso de hacer de la seguridad digital una prioridad y un fuerte componente de su desarrollo socioeconómico, por esto confiamos en que este estudio no sólo será beneficioso para el Gobierno de Colombia, sino que también aportará una visión sobre la importancia de las buenas prácticas en seguridad digital y la realidad del costo de los incidentes cibernéticos en nuestra región.

Esperamos poder continuar apoyando al Gobierno de Colombia en sus esfuerzos y seguir trabajando conjuntamente con el Banco Interamericano de Desarrollo (BID) para extender iniciativas de cooperación en el tema de seguridad cibernética como ésta, a otros países de la región.



ANA MARÍA RODRÍGUEZ

GERENTE DE INSTITUCIONES PARA EL DESARROLLO DEL BID

El año pasado, el Informe Ciberseguridad 2016 ¿Estamos preparados en América Latina y el Caribe?, mostró que la región aún no está lista para enfrentar los desafíos de esta nueva sociedad digital.

La región continúa la marcha para subirse el tren de la cuarta revolución industrial, más de la mitad de los países cuentan con una estrategia de gobierno digital, Latinoamérica y el Caribe es la región del mundo más activa en las redes sociales, y en la región, más de la mitad de la población se conecta a internet regularmente. Sin embargo, no estamos llevando a cabo las políticas de seguridad digital que garanticen que nuestros ciudadanos y nuestras empresas pueden operar en el ciberespacio sin correr el peligro de que su identidad sea robada, su patrimonio dañado o su integridad física puesta en peligro.

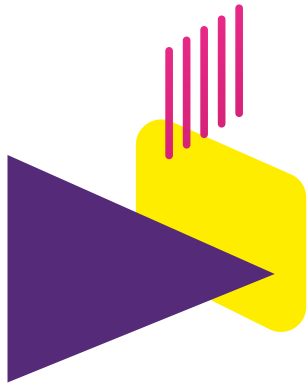
Al igual que internet, la seguridad digital tiene naturaleza global y urgencia de apropiación local. Las políticas de ciberseguridad efectivas precisan mecanismos de intercambio de información, colaboración y coordinación que reúnan los esfuerzos de los diferentes países tanto en el sector público como en el privado. La cadena que defiende a los ciudadanos de la era digital de los ataques cibernéticos es tan fuerte como su eslabón más débil y, por tanto, debe ser interés de todos que ningún país se quede atrás en la implementación de políticas de ciberseguridad.

Con base en datos compartidos por las empresas y las instituciones públicas, este informe, Impacto de los Incidentes de Seguridad Digital en Colombia, desvela las principales áreas de debilidad digital en Colombia y sus efectos, dejando mensajes que reclaman la atención de todos los actores en el ecosistema digital del país. La mayor parte de las organizaciones colombianas no están adecuadamente preparadas y están siendo atacadas, los ataques son cada vez más severos y tienen un impacto económico importante. También son eslabones débiles el ciudadano común y

la microempresa, para los cuales es necesario llevar a cabo acciones de sensibilización y capacitación que disminuyan el riesgo de que sean víctimas de un ataque cibernético.

La profundidad de este estudio y la información relevada, sitúan a Colombia como un referente en el levantamiento de información completa sobre un sector en el que resulta difícil que las instituciones compartan información. Ello ha sido posible gracias a la colaboración entre MINTIC, la OEA y el BID, con los aportes técnicos del Foro Económico Mundial y de la Universidad de Oxford.

Estoy segura de que esta publicación será una herramienta útil para orientar la implementación de la Política Nacional de Seguridad Digital recientemente lanzada en Colombia y confío en que otros países sigan el ejemplo de este país estudiando en profundidad el impacto de los incidentes de ciberseguridad y diseñen las políticas necesarias para disminuirlo. El BID es y seguirá siendo socio activo de la transformación digital en Latinoamérica y el Caribe, para maximizar sus beneficios y controlar sus riesgos. Los datos muestran que la inversión en prevenir los ciberataques es menor que la necesaria para recuperarse.



PARTE 1

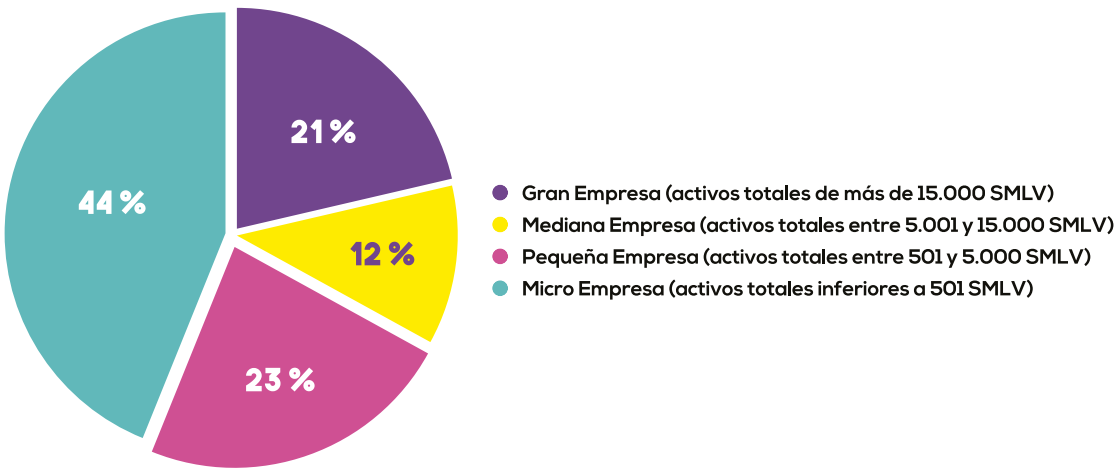
ANÁLISIS DEL SECTOR PRIVADO

PERFIL DE LAS EMPRESAS

A los efectos de este estudio, una ***empresa*** es empresa colombiana: i) del sector privado o ii) de economía mixta en la que el Estado tenga participación inferior al 50%. En respuesta a la pregunta:

¿Cuál es el tamaño de su empresa?, el 44% de los entrevistados indicó que correspondían a microempresas, el 23% a pequeñas empresas y el 12% y el 21% informaron que eran medianas y grandes empresas, respectivamente, como se demuestra en el siguiente diagrama:

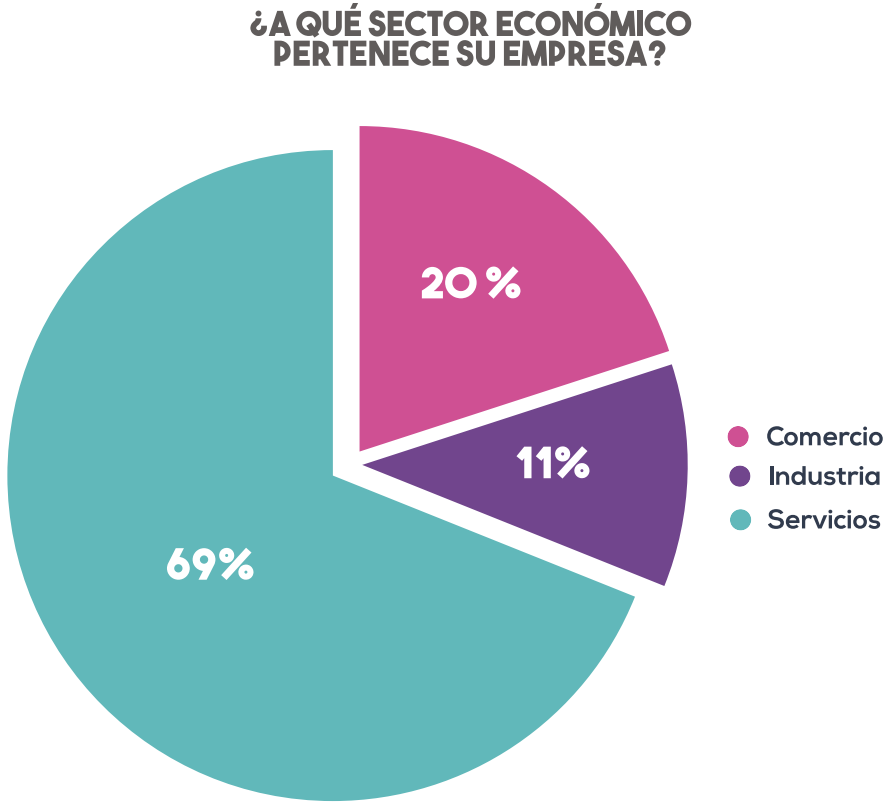
GRÁFICO 1: TAMAÑO DE LAS EMPRESAS



Número de observaciones: 515
Nota: SMLV es Salario Mínimo Legal Mensual Vigente de Colombia

Entre las Empresas entrevistadas, el 84% informó que el 100% era de propiedad privada, mientras que el 16% era i) de propiedad pública o ii) de propiedad pública y privada (mixta). De las Empresas entrevistadas, el 69% pertenece al sector de Servicios, o que incluye, por ejemplo, el sector financiero, el 20% al sector Comercio y el 11% al sector Industria.

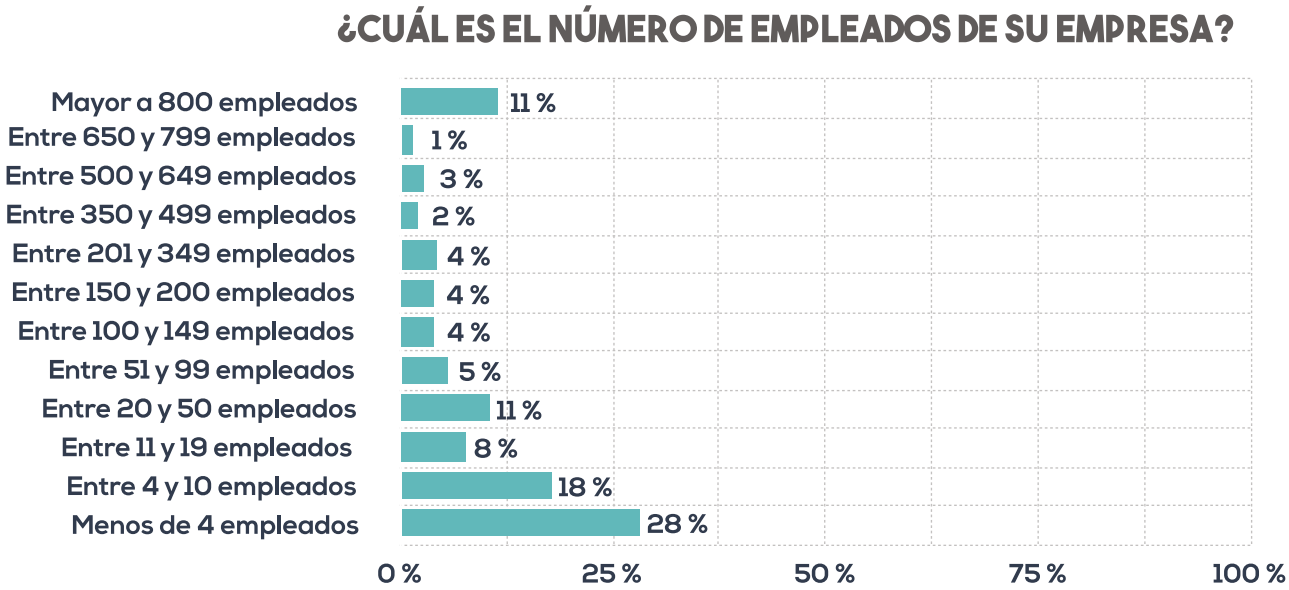
GRÁFICO 2: SECTOR ECONÓMICO DE LOS ENTREVISTADOS



Número de observaciones: 515

En cuanto al número de las Empresas entrevistadas en función del tamaño, el 28% tenían menos de 4 empleados, 60% entre 4 y 799 empleados, y 11% de las empresas tienen mayor a 800 empleados.

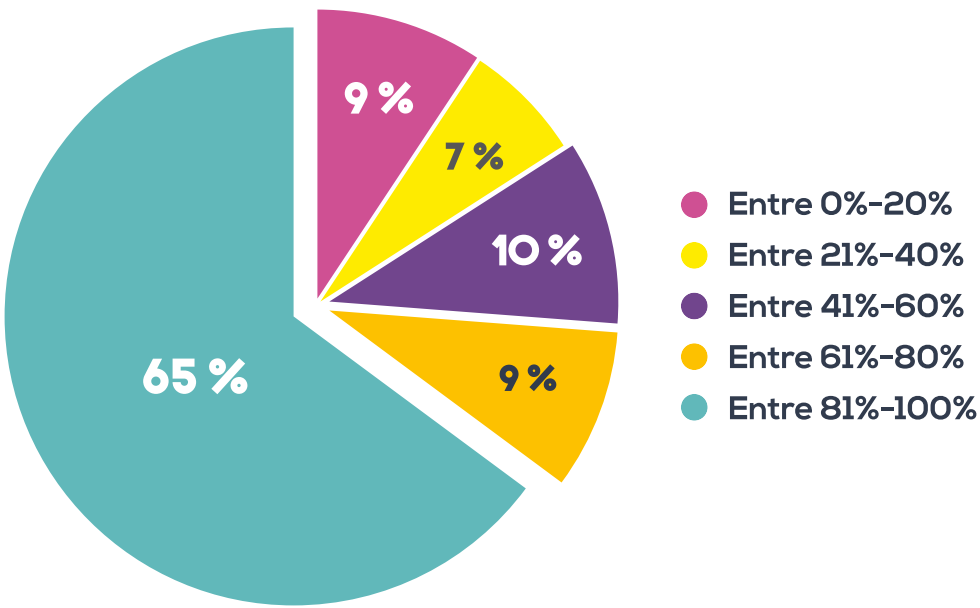
GRÁFICO 3: NÚMERO DE EMPLEADOS DE LAS EMPRESAS



Número de observaciones: 515

En relación con las Empresas que participaron de este estudio, el 65% indicaron que entre el 81% y el 100% de su fuerza laboral contaba con acceso a Internet, el 9% respondió que le daban acceso al 61%-80% de sus empleados y un 26% le daba entre 0 y 60% de sus empleados.

GRÁFICO 4: PORCENTAJE APROXIMADO DEL PERSONAL DE SU EMPRESA QUE TIENE ACCESO A INTERNET



Número de observaciones: 515

Cuando se formuló la pregunta ¿La Empresa APLICA una Política de "Trae tu propio Dispositivo" (en inglés, "bring your own device -BYOD-")?, el 40% de los entrevistados indicaron que tenían una política BYOD frente al 60% que indicaron que no la tenían.

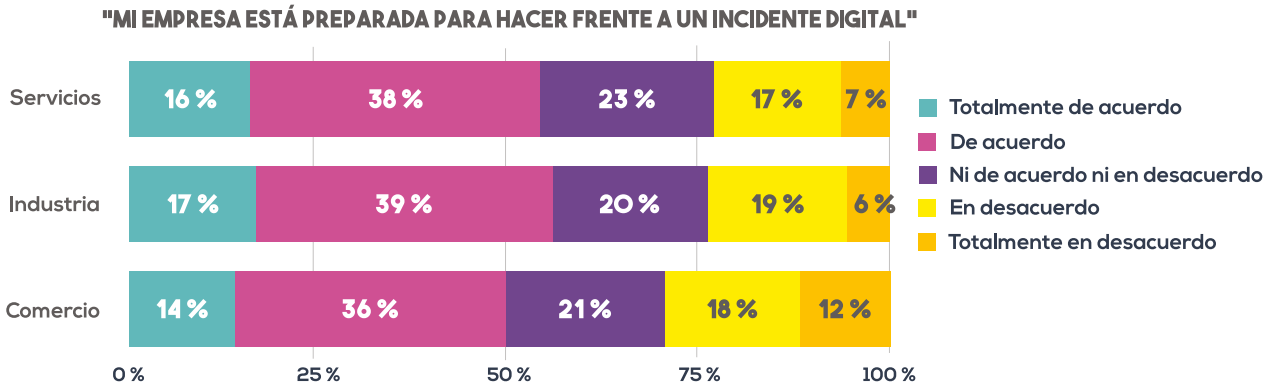
En general, se podría concluir que el perfil general de quienes participan de este estudio son Microempresas, siendo la mayoría del sector de Servicios. Sin embargo, es importante tener en cuenta que el 21% de los entrevistados pertenecen a grandes empresas y el 34% de los entrevistados contaban con un mínimo de 99 empleados o más.

PRÁCTICAS DE SEGURIDAD DIGITAL EN LAS EMPRESAS

Como parte del estudio, se realizaron una serie de preguntas con respecto a las prácticas de seguridad digital. Estas preguntas se formularon con el propósito de evaluar cómo sus prácticas impactaron el nivel de ataques experimentados y el impacto final que estas prácticas pueden tener en los costos reales incurridos como resultado de un ataque.

En respuesta a la pregunta "Mi entidad/ empresa está preparada para hacer frente a un incidente digital", los datos fueron analizados teniendo en cuenta tanto al sector como el tamaño de las mismas. Entre los sectores: Servicios, Industria y Comercio, un promedio simple del 37% de los entrevistados de los tres sectores creen que estaban preparados para manejar un incidente cibernético. Aproximadamente el 30% de los entrevistados del sector Comercio consideraron que no estaban preparados o no estaban totalmente preparados para un incidente cibernético.

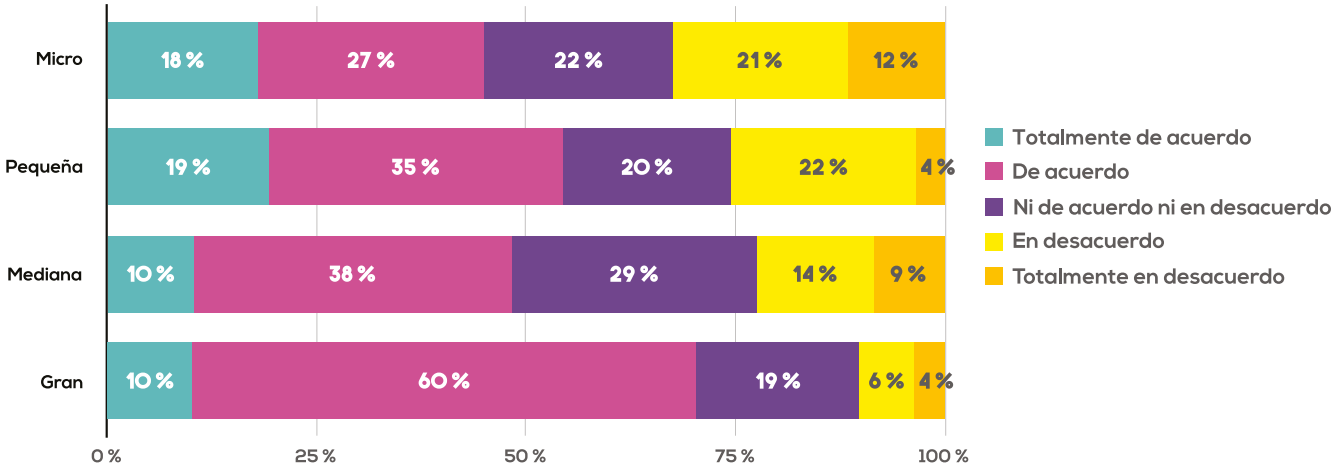
GRÁFICO 5: NIVEL DE PREPARACIÓN PARA HACER FRENTE A UN INCIDENTE DIGITAL (SECTOR ECONÓMICO)



Número de observaciones: 486

En cuanto al tamaño de estas empresas, el 70% de las grandes empresas se sienten muy preparadas o preparadas para un incidente digital, frente al 45% de las microempresas. De los resultados se desprende que un promedio simple de alrededor del 22% de las empresas de todos los tamaños contestaron que estaban "ni de acuerdo ni en desacuerdo" con la afirmación "Mi empresa está preparada para hacer frente a un incidente digital".

GRÁFICO 6: NIVEL DE PREPARACIÓN PARA HACER FRENTE A UN INCIDENTE DIGITAL (TAMAÑO DE LA EMPRESA)



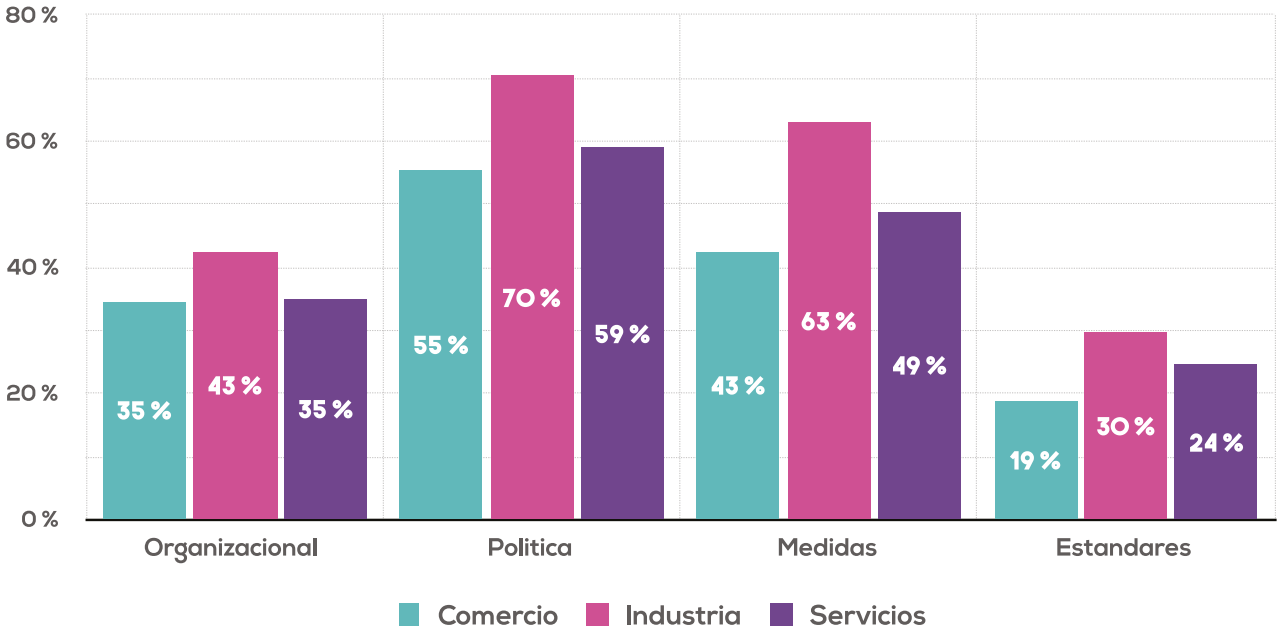
Número de observaciones: 486

Un aspecto importante de la preparación cibernética son las medidas implementadas, ya sea que se trate de políticas, medidas técnicas o normas. Con el fin de entender estos ejemplos, se enumeran a continuación:

1. Organizacional (ej. área, departamento dedicado a la seguridad digital, jefe de seguridad de la información, roles asociados a la seguridad de la información, funciones en torno a la seguridad de la información)
2. Política (ej. política de acceso al sistema, política de actualización de contraseñas, concientización)
3. Medidas técnicas (ej. pruebas de vulnerabilidad, mantenimiento de la infraestructura de TI)
4. Estándares (ej. ISO 27001, otros estándares internacionales)

En relación a esto, se les preguntó a los entrevistados, ¿Cuáles de las siguientes prácticas en seguridad digital (seguridad digital y/o seguridad de la información) son implementadas por su entidad/empresa? Entre los entrevistados de los tres sectores económicos, una mayoría respondió que había implementado medidas de políticas (55% del sector Comercio, 70% del sector Industria y 59% del sector de Servicios), con la implementación de estándares técnicos (ej. ISO 27001, otros estándares internacionales), siendo la siguiente medida más alta implementada (Comercio 43%, Industria 63% y Servicios 49%).

GRÁFICO 7: PRÁCTICAS EN SEGURIDAD DIGITAL (SECTOR ECONÓMICO)

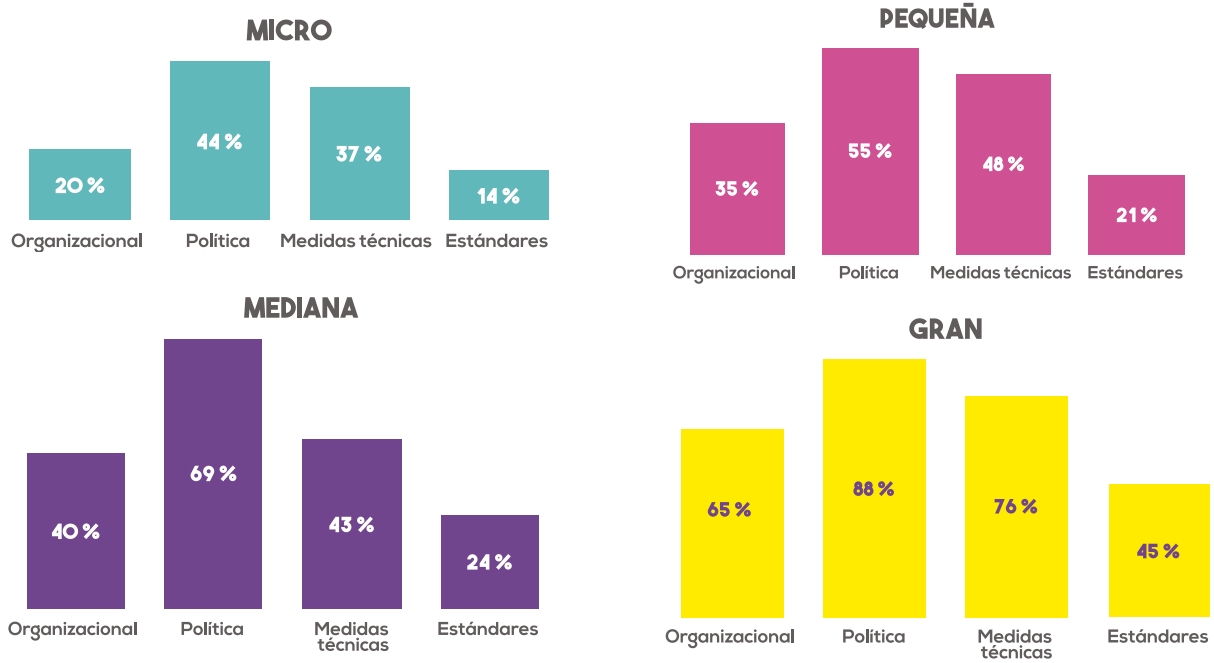


Número de observaciones: 554

Si se compara por tamaño, resulta evidente que la mayoría de los entrevistados también dieron un mayor peso a la aplicación de las políticas como una medida de seguridad digital. Entre las microempresas, 44% de ellas han implementado políticas, 37% medidas técnicas y 34% normas y medidas organizativas.

Entre las empresas más grandes, una observación de interés fue que el 88% implementó medidas de políticas, pero solo el 45% de las empresas que participan de este estudio mencionan que adoptaron estándares. Entre todos los entrevistados, la implementación de medidas y estándares organizacionales fue identificada como la práctica de más baja prioridad. Véase los gráficos a continuación.

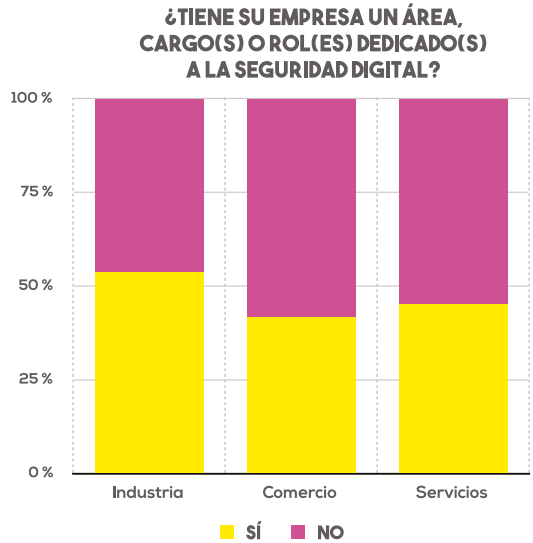
GRÁFICO 8: PRÁCTICAS EN SEGURIDAD DIGITAL (TAMAÑO DE LA EMPRESA)

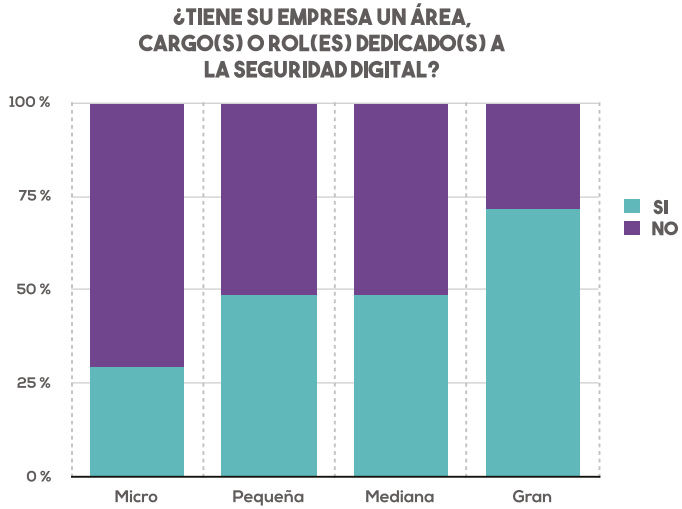


Número de observaciones: 486

Una de las medidas más importantes para asegurar a una organización contra los incidentes cibernéticos es la identificación de un cargo con dedicación exclusiva para el manejo de incidentes digitales. Este cargo es importante ya que les ayudará a las empresas a detectar, aislar y resolver incidentes rápidamente cuando ocurran y si ocurren. Si no existe este cargo, se les podría permitir a los atacantes permanecer en el sistema de las organizaciones más tiempo de lo necesario, haciendo que la detección sea un proceso más largo también. Entre todos los que respondieron a la pregunta ***¿Tiene su entidad/empresa un área, cargo (s) o rol(es) dedicado (s) a la seguridad digital (seguridad digital y/o de seguridad de la información)?***, 70% de las grandes empresas respondieron que "sí" comparado con poco más del 20% de las microempresas. Entre los sectores económicos, la mayoría del sector Industria dijo tener un equipo con dedicación exclusiva, con un poco más del 54% respondiendo positivamente a la pregunta, frente a solo el 45% y el 42% de los sectores de Servicios y Comercio, respectivamente. Véase los gráficos por tamaño y sector a continuación:

GRÁFICO 9: CARGO(S) O ROL(ES) DEDICADO(S) A LA SEGURIDAD DIGITAL (TAMAÑO Y SECTOR ECONÓMICO DE LAS EMPRESAS)





Número de observaciones = 486

La pregunta anterior se puede comparar con la siguiente pregunta, es decir, ***¿Su entidad/empresa gestiona la seguridad bajo cuál de los siguientes esquemas?*** Entre los entrevistados, el 37% de las micro, el 58% de las pequeñas, el 64% de las medianas y el 58% de las grandes empresas respondieron que la seguridad digital se manejaba bajo el departamento de TI. Solo el 22% de las micro, 18% de las pequeñas, 7% de las medianas y 21% de las grandes empresas indicaron que se manejaba bajo un área de seguridad digital.

En cuanto a los sectores, aproximadamente el 83% del sector Comercio indicó que se encontraba bajo el departamento de TI, en comparación con el 55% del sector Industria y el 47% del sector de Servicios que respondieron de manera similar. Lo que las respuestas podrían indicar es que la mayoría de los entrevistados ven la necesidad de abordar los temas de seguridad digital y lo han colocado bajo el departamento que más estrechamente se asocia con la seguridad digital (es decir, Tecnología de la Información). Sin

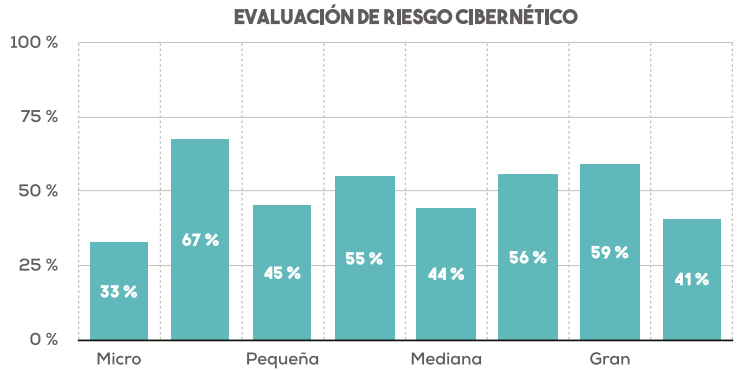
embargo, esta tendencia de reorientar los departamentos de tecnología de la información para manejar la seguridad digital y la respuesta a incidentes, a largo plazo, puede conducir a tener un equipo de personas que no poseen las habilidades necesarias para responder a incidentes más sofisticados[1].

Cuando se les preguntó a los entrevistados, ***¿Cuántas personas conforman el equipo o área que tiene a cargo la seguridad digital (seguridad digital y/o seguridad de la información) en su empresa?,*** el 55% respondió que tenían 1-2 personas dedicadas, el 27% respondió 3-5 personas y solo el 18% indicó más de 5 personas.

Esto demuestra aún más la conclusión de que si bien las empresas han reconocido la importancia de abordar los incidentes cibernéticos, no han invertido en las áreas de organización de sus empresas para hacer frente a esto.

Por último, en relación con las prácticas organizacionales, cuando se les preguntó si su organización emprendía o no la evaluación del riesgo de la seguridad digital, la mayoría de los entrevistados indicaron que no lo hicieron. Esto, en términos de tamaño de las empresas, se desglosó como sigue:

GRÁFICO 10: EVALUACIÓN DEL RIESGO CIBERNÉTICO (TAMAÑO DE LAS EMPRESAS)

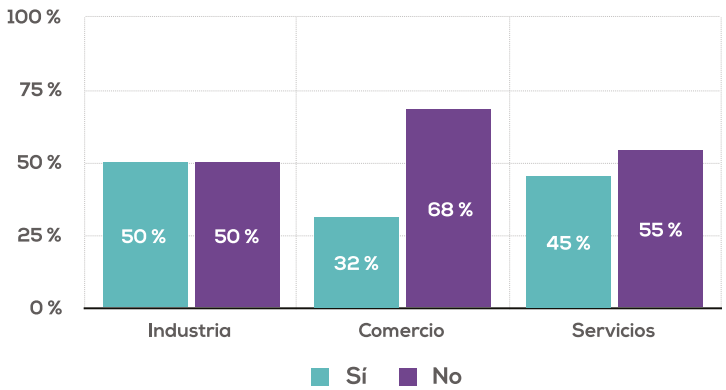


Número de observaciones 439

1 Observaciones similares se hicieron en las Capacidades de Respuesta a Incidentes en 2016: La Encuesta de Respuesta a Incidentes SANS 2016, pág. 5 Consultado en: https://www.sans.org/reading-room/whitepapers/incident/incident-response-capabilities-2016-2016-incident-response-survey-37047 Última consulta el 28 de agosto de 2018

En relación a los sectores económicos, el 50% de los entrevistados del sector Industria indicaron que no lo hicieron, en comparación con solo el 32% y el 45% de los sectores Comercio y de Servicios que sí realizaron una evaluación del riesgo de seguridad digital.

GRÁFICO 11: EVALUACIÓN DEL RIESGO CIBERNÉTICO (SECTOR ECONÓMICO)



Número de observaciones: 439

Este resultado lleva a hacer unas observaciones significativas ya que el propósito para la realización de una evaluación de riesgos para cualquier organización es ayudarle a la misma a desarrollar recomendaciones ejecutables para mejorar la seguridad e implementar las mejores prácticas de la industria. Una de las mejores prácticas de la industria es el Marco de Seguridad Digital del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés)[2], que pone de relieve que el objetivo de una evaluación de riesgos es que una organización entienda "el riesgo de seguridad digital para las operaciones organizacionales (incluyendo misión, funciones, imagen o reputación), activos de la organización y los individuos". Según lo establecido por el NIST, la realización de una evaluación de riesgos típicamente incluye los siguientes seis pasos:

1. Identificar y documentar vulnerabilidades de los Activos.
2. Identificar y documentar las amenazas internas y externas.
3. Adquirir información sobre amenazas y vulnerabilidades de fuentes externas.
4. Identificar posibles impactos comerciales y probabilidades.
5. Determinar el riesgo empresarial revisando amenazas, vulnerabilidades, probabilidades e impactos.
6. Identificar y priorizar las respuestas de riesgo.

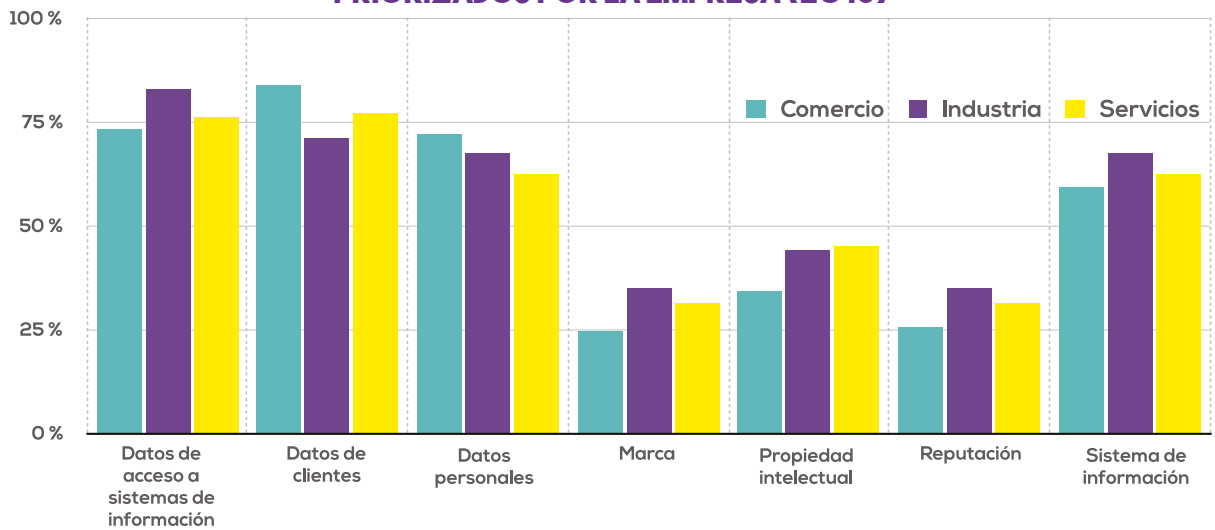
En este sentido, se puede inferir que muchos de los entrevistados no aprecian plenamente el valor que las mejores

2 Marco de Seguridad Cibernética NIST, Accedido en: https://www.nist.gov/cyberframework; Último acceso: 29 de agosto de 2017

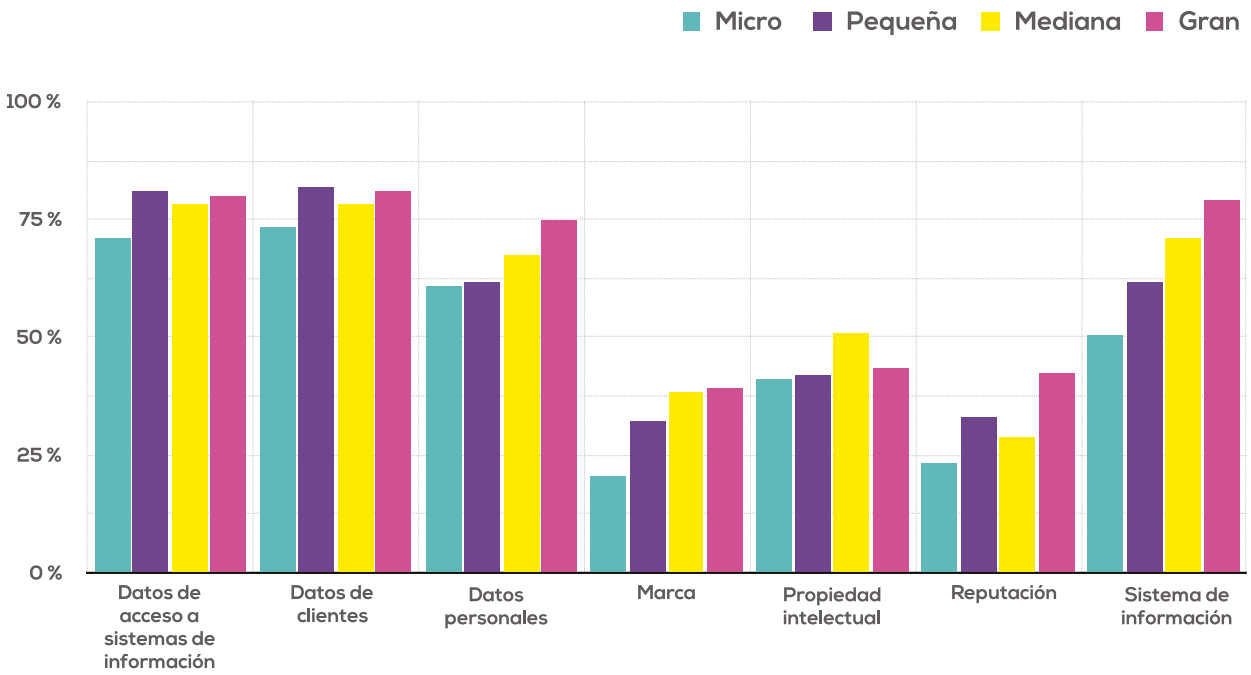
prácticas les podrían dar a sus operaciones comerciales. Por ejemplo, cuando se les preguntó: ***¿A la hora de protegerse frente a incidentes digitales, amenazas cibernéticas y/o ataques cibernéticos, cuáles de estos datos y/o activos de información son priorizados por su entidad/empresa? Por favor marque las opciones que apliquen,*** casi todos los entrevistados a través de sectores y tamaños indicaron que les darían prioridad a ***Datos de acceso a sistemas de información (p. ej.: contraseñas, tokens, credenciales)*** y ***Datos de clientes.*** En cuanto a los sectores económicos, las empresas de los tres (Comercio, Industria y Servicios) colocaron la menor prioridad en ***Marca, Propiedad intelectual/secretos industriales y Reputación***.

Curiosamente, cuando se compararon los datos por tamaño de las organizaciones, los resultados fueron casi exactamente los mismos en términos de niveles de prioridades. Esto es significativo, ya que una de las mejores prácticas para la gestión del riesgo cibernético es que las entidades sean proactivas en lugar de reactivas y, como tal, es importante revisar las amenazas, identificar vulnerabilidades y consecuencias y es evidente que la mayoría de las organizaciones vean los datos como un activo significativo por proteger. Los siguientes gráficos muestran el resumen de los resultados por sector:

GRÁFICO 12: DATOS Y ACTIVOS PRIORIZADOS POR LA EMPRESA (2016)



En términos del análisis por tamaño:



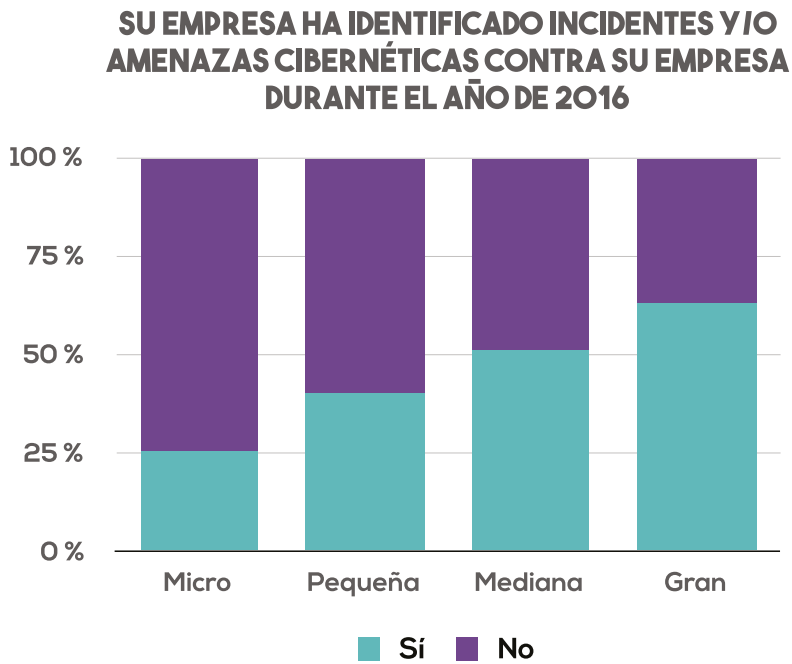
Número de observaciones: 450

Por lo tanto, cuando se pregunta, en una escala de 1-5, lo que los entrevistados creen que son los principales factores que afectarían su capacidad de abordar la seguridad digital, la falta de personal con dedicación exclusiva al área y la falta de presupuesto fueron clasificados como más altos, con la falta de conciencia de los empleados inmediatamente después. A este respecto, se puede inferir que, si bien la mayoría de las empresas ven la necesidad de abordar la seguridad digital, los recursos humanos y financieros con dedicación exclusiva todavía no están siendo priorizados.

INCIDENTES DIGITALES EN LAS EMPRESAS

Cuando se pregunta si se han identificado incidentes digitales contra su organización, más del 70% de las microempresas contestaron que no han identificado incidentes digitales. Entre las pequeñas empresas, aproximadamente 60% tampoco identificaron incidentes digitales. Sin embargo, entre las medianas y grandes empresas, la mayoría de las empresas contestaran que sí identificaron incidentes digitales: 51% y 63%, respectivamente.

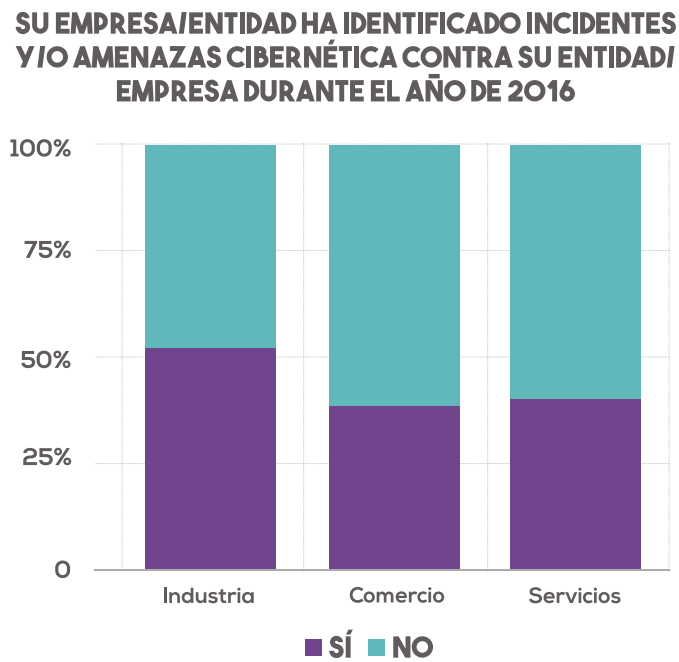
GRÁFICO 13: PORCENTAJE DE EMPRESAS QUE IDENTIFICARON INCIDENTES DIGITALES, SEGÚN EL TAMAÑO DE LA EMPRESA (2016)



Número de observaciones: 451

Al analizar los distintos sectores económicos, solamente en el sector Industria la mayoría de las empresas identificaron los incidentes digitales: 52% de las empresas. Es importante señalar que la mayoría de las empresas del sector Industria analizadas en este estudio consisten en grandes empresas.

GRÁFICO 14: PORCENTAJE DE EMPRESAS QUE IDENTIFICARON INCIDENTES DIGITALES, SEGÚN EL SECTOR ECONÓMICO (2016)



Número de observaciones: 451

Con el objetivo de comprender el por qué algunas empresas identificaron incidentes digitales, y otras no, se estimó una ecuación de determinantes de la probabilidad que una empresa del sector privado identifique incidentes digitales contra su empresa, donde la variable dependiente[3] toma el valor de "1" si la empresa identifica incidentes digitales y "0" si no los identifica.

3 La variable dependiente es aquella cuyos valores dependen de los que tomen otra variable.

Dentro de las variables explicativas[4], se incluyó un conjunto de variables dicotómicas[5] que capturaron factores específicos de las empresas, tal como el tamaño de la empresa y el sector económico. Es decir, grande, mediana, pequeña o micro, así como si la empresa pertenece al sector Industria, Comercio o de Servicios. Otras variables dicotómicas incluyeron: (i) si la empresa implementa políticas de seguridad digital (por ejemplo, política de acceso al sistema, política de actualización de contraseñas, concientización); (ii) si la empresa implementa medidas técnicas (por ejemplo, pruebas de vulnerabilidad, mantenimiento de la infraestructura de TI); (iii) si la empresa implementa estándares (por ejemplo, ISO 27001, otros estándares internacionales); (iv) si la empresa tiene un área, cargo(s) o rol(es) dedicado(s) a la seguridad digital; (vi) si la empresa conoce alguna reglamentación y/o legislación nacional o territorial que requiera las empresas de su sector implementen prácticas de gestión de riesgo cibernético; y (vii) si la empresa hace alguna evaluación de riesgo cibernético.

También se incluyeron otras variables explicativas, como el número de empleados de la empresa, el porcentaje aproximado del personal de la empresa que tiene acceso a Internet para desarrollar sus actividades profesionales, el porcentaje del capital social de la empresa que es extranjero, el valor aproximado (en pesos colombianos) de las ventas de la empresa durante el año de 2016, así como el valor aproximado de presupuesto designado por la empresa para asuntos de seguridad digital.

Dada la naturaleza binaria de la variable dependiente, se utiliza un modelo de estimación ***logit***[6] (Anexo 3***).*** Los resultados indican que hay una relación estadísticamente significativa positiva entre la implementación de medidas técnicas - como pruebas de vulnerabilidad y mantenimiento de la infraestructura de TI - y la identificación de incidentes digitales. Así también se aprecia con la variable explicativa relativa a la práctica de evaluación de riesgo cibernético. Más específicamente, los resultados indican que la probabilidad que una empresa en Colombia identifique incidentes digitales aumenta para aquellas empresas que implementan medidas técnicas de

4 La variable explicativa, o independiente, es aquella que explica los cambios en la variable dependiente.

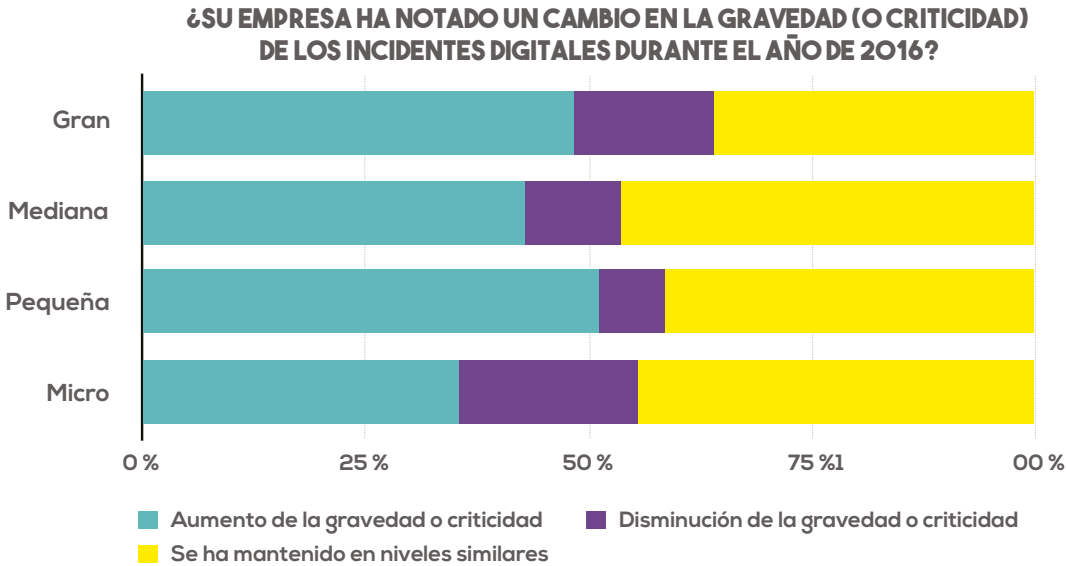
5 La variable dicotómica o binaria es aquella que tiene solo dos formas de presentarse. Es decir, una variable que puede asumir solo dos valores posibles, como "sí" o "no".

6 Este modelo asume que los efectos individuales han sido promediados, lo que facilita el cálculo y la interpretación de los efectos marginales que, a su vez, miden el efecto de un cambio en uno de los regresores sobre la variable dependiente.

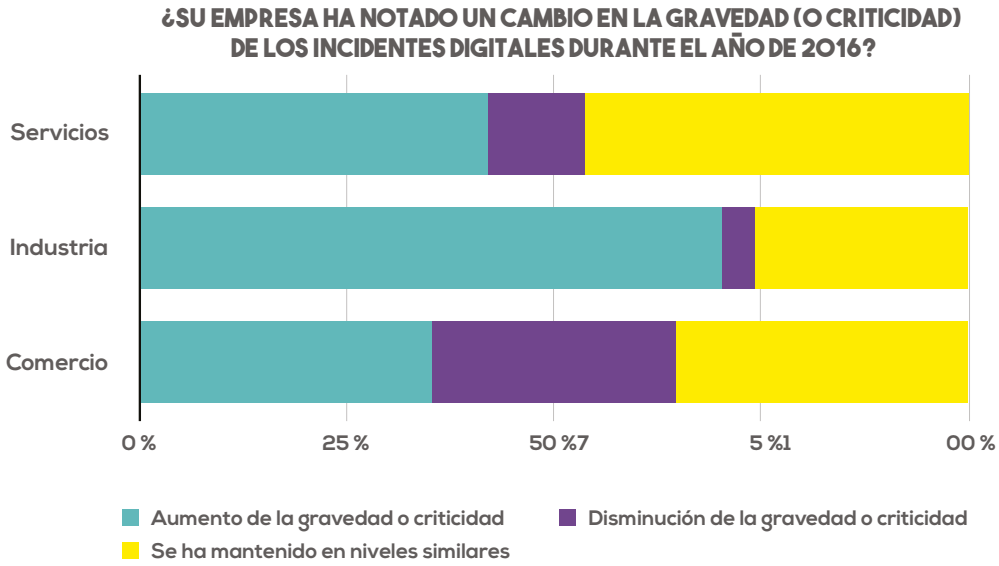
seguridad y que hacen evaluación de riesgo. Igualmente existe una relación estadísticamente significativa positiva entre la identificación de incidentes y el número de empleados de una empresa. Por otro lado, los resultados indican una relación estadísticamente significativa negativa entre la identificación de incidentes y las microempresas.

Tener la capacidad de identificar incidentes es importante para las entidades, ya que es el primer paso para poder contener un ataque malicioso y poder responder. Cuando se pregunta, ¿Su entidad/empresa ha notado un cambio en la gravedad (o criticidad) de los ataques cibernéticos durante el año 2016?, el 70% del sector Industria respondió que había notado un cambio en la gravedad de los ataques en comparación con el resto de la población. El 35% del sector Comercio y el 46% del sector de Servicios indicaron que los niveles de ataques seguían siendo los mismos. En términos de tamaño de la empresa, se observó entre las respuestas que un mayor número de pequeñas empresas respondieron haber visto un aumento en la gravedad. Véase los gráficos comparativos a continuación:

GRÁFICO 15: CAMBIO EN LA GRAVEDAD DE LOS INCIDENTES DIGITALES (2016)



Número de observaciones: 178

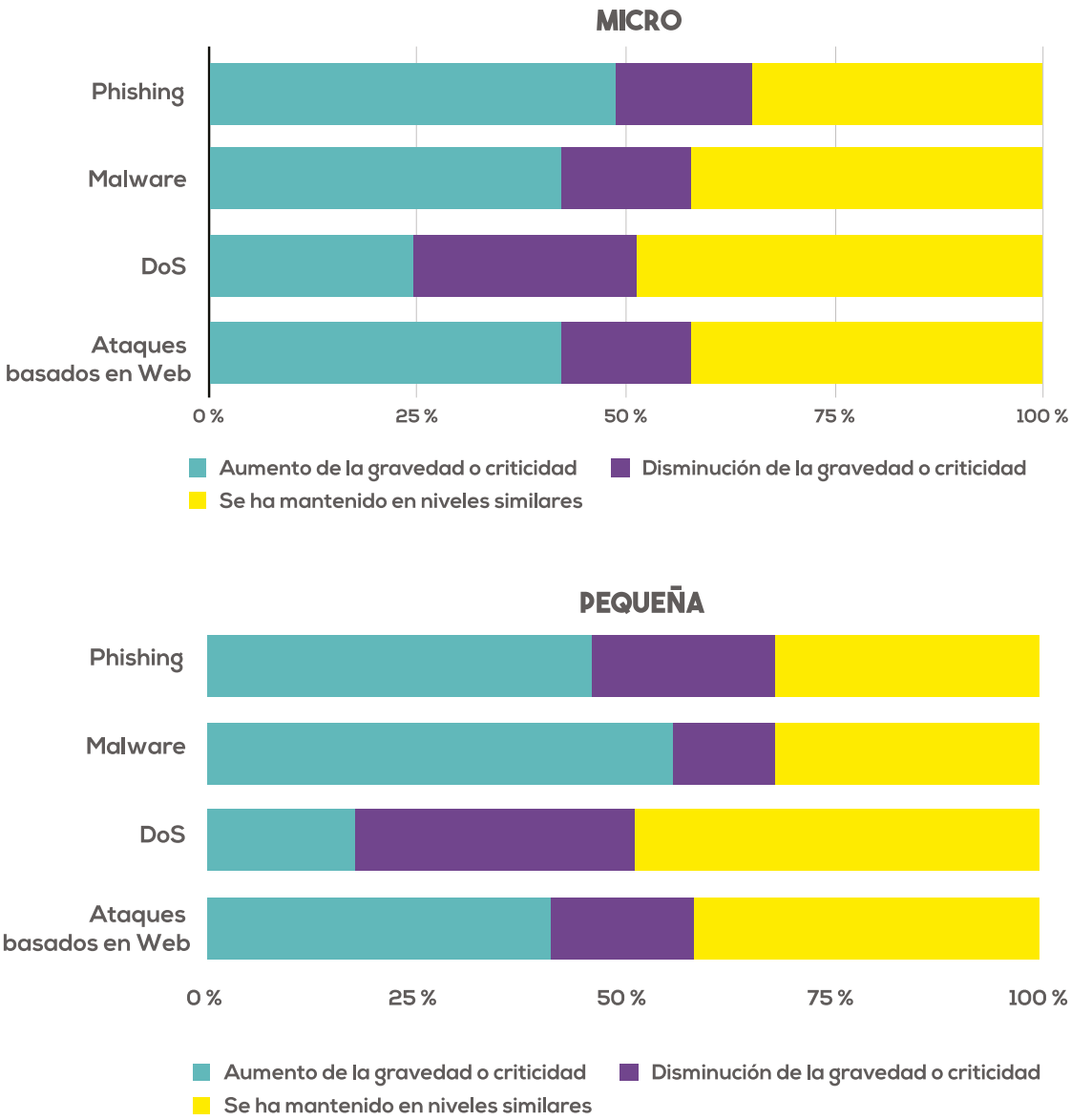


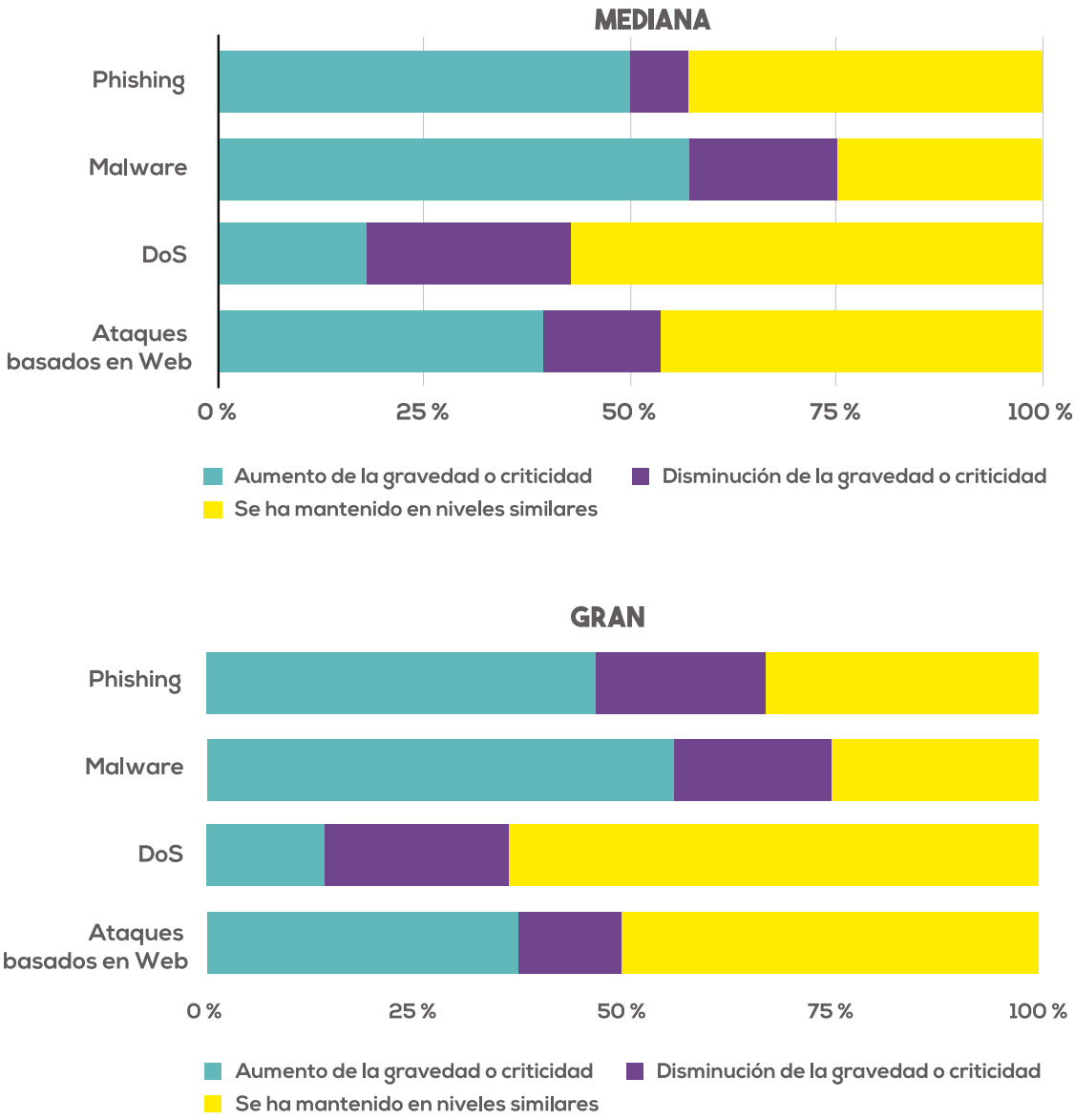
Número de observaciones: 178

En cuanto a los tipos de incidentes que se están experimentando, los participantes del estudio indicaron en su respuesta a la pregunta, ***¿Qué tipos de incidentes digitales, amenazas cibernéticas o ataques cibernéticos ha identificado su entidad/empresa durante el año 2016?,*** que el malware y el phishing se encontraban entre los tipos de incidentes más comunes. Se observó que, dentro del sector de Servicios, el 50% de los que respondieron notaron un aumento en los ataques de malware, 47% de phishing, 39% de ataques basados en web y 18% de ataques de denegación de servicio. En el sector Comercio, se hicieron observaciones similares con un 53% reportando un incremento en el malware, un 41% reportó un aumento en el phishing y un 21% notó un incremento tanto en ataques basados en web como en ataques de denegación de servicio. Curiosamente, sin embargo, hubo algunas variaciones dentro del sector Industria en esta observación, ya que el 67% reportó un incremento en la gravedad de los ataques basados en web y el malware y el 59% reportó un aumento en los ataques de phishing.

En relación con el tamaño de las empresas informantes, los resultados también fueron similares en la respuesta de las micro, pequeñas, medianas y grandes empresas. Véase gráficos comparativos a continuación:

GRÁFICO 16: GRAVEDAD DE LOS INCIDENTES DIGITALES (2016)





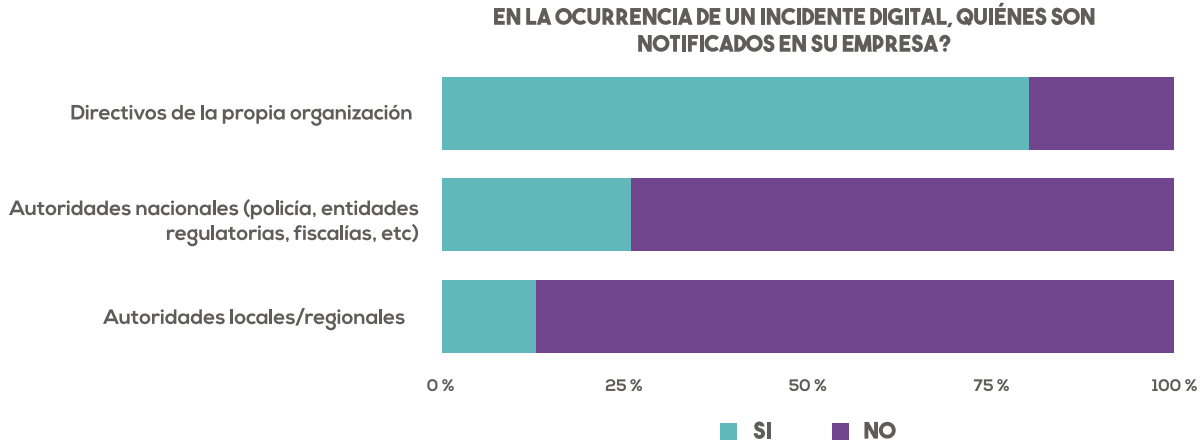
Número de observaciones: 178

Al comparar estos datos con el Informe del mes de agosto de 2017 del Centro Cibernético Policial (CCP) de Colombia, también se ha producido un incremento anual de denuncias cibernéticas bajo ***Denuncias Ley 1273-Delitos Informáticos en Colombia,*** para estos propósitos especialmente en relación al ***Articulo 269E: Uso de software malicioso y Articulo 269G: Suplantación de sitos web para capturar datos personales.*** Por su parte, el informe de marzo de 2017, ***Informe: Amenazas del Cibercrimen en Colombia 2016-2017[7],*** concluyó que el nivel de información del sector empresarial aumentó del 5% al 28% en el número de informes recibidos. El informe reveló algunos hechos interesantes como que ***durante el 2016 hubo un incremento del 114.4% en ataques de malware en el país, en relación al 2015 (153 incidentes reportados en el 2015, 328 incidentes reportados en el 2016).***

Sin embargo, sigue siendo necesario aumentar el nivel de denuncias de los incidentes digitales, como cuando se les pidió a los entrevistados que respondieran a este instrumento, ***En la ocurrencia de un incidente digital, amenaza cibernética y/o un ataque cibernético, quiénes son notificados en su entidad/empresa? Por favor marque las opciones que apliquen,*** el 87% informó que no notificó sobre incidentes digitales a una Autoridad Nacional, comparado con el 80% que respondió que lo reportaron a los directores de la organización.

7 Informe Amenazas del Cibercrimen en Colombia 2016 – 2017, Accedido en https://caivirtual.policia.gov.co/contenido/informe-amenazas-del-cibercrimen-en-colombia-2016-2017, Última entrada: 28 de agosto de 2017

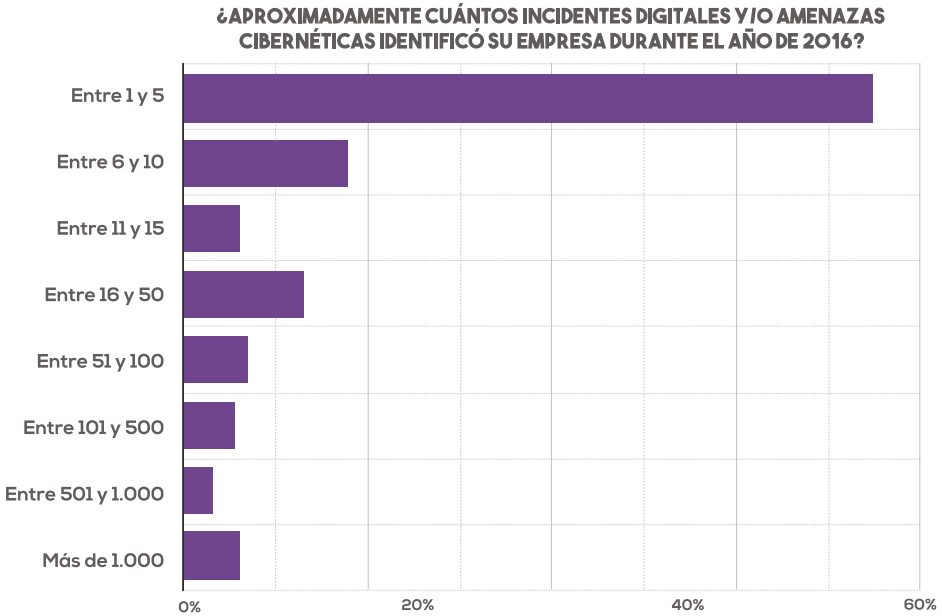
GRÁFICO 17: NOTIFICACIÓN DE INCIDENTES DIGITALES (2016)



Número de observaciones: 439

Con respecto al número de incidentes digitales, se observó en 2016 que más de 50% de las empresas colombianas entrevistadas registraron entre 1 y 5 incidentes digitales, y que aproximadamente 30% entre 6 y 100 incidentes digitales. Aunque la gran mayoría de las empresas se encuentran en los intervalos indicados, cabe resaltar que 5% de las empresas entrevistadas registraron valores anómalos de más de 1.000 incidentes digitales. De hecho, en este grupo, hay empresas que registraron más de 100 mil incidentes digitales en 2016

GRÁFICO 18: NÚMERO DE INCIDENTES DIGITALES IDENTIFICADOS POR LAS EMPRESAS (2016)



Número de observaciones: 173

Finalmente, se realizó una regresión lineal en la cual el logaritmo del número de incidentes digitales fue la variable dependiente (Anexo 3). Se optó por el logaritmo del número de incidentes, a fin de normalizar la distribución de la variable. En el modelo se incluyeron las siguientes variables explicativas: (i) las ventas de la empresa en 2016; (ii) el valor aproximado de presupuesto designado por la empresa para la seguridad digital; (iii) el número de empleados; (iv) el porcentaje aproximado de personal que tiene acceso a Internet para desarrollar sus actividades profesionales; así como (v) el porcentaje del capital social de la empresa que es extranjero.

El modelo también cuenta con las siguientes variables dicotómicas: (i) si la empresa tiene un área, cargo(s) o rol(es) dedicado(s) a la seguridad digital; (ii) si la empresa implementa medidas técnicas de seguridad (por ejemplo, pruebas de vulnerabilidad, mantenimiento de la infraestructura de TI); (iii) si la empresa adopta políticas de seguridad digital

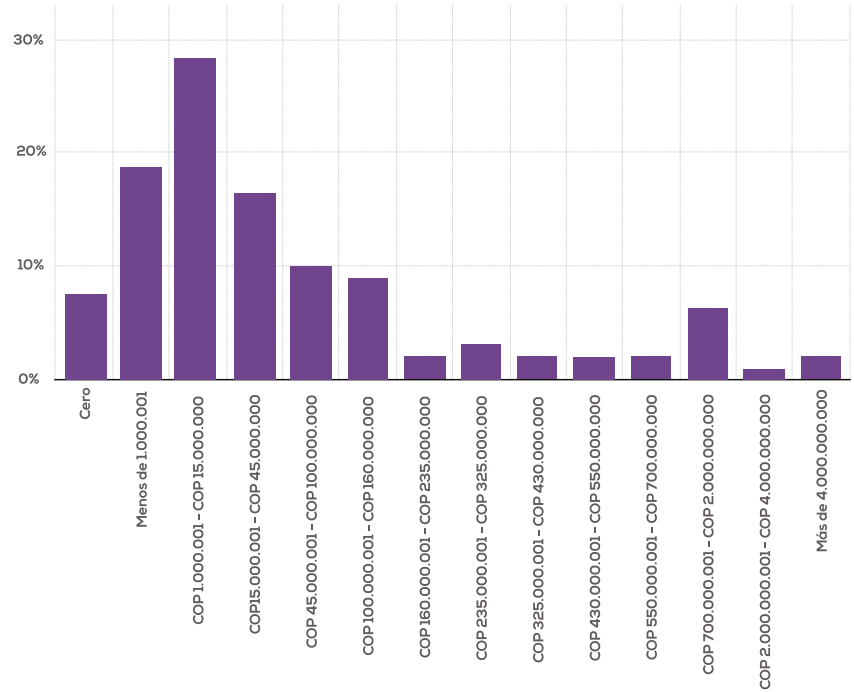
(por ejemplo, política de acceso al sistema, política de actualización de contraseñas, concientización); (iv) si la empresa implementa estándares (por ejemplo, ISO 27001, otros estándares internacionales); (v) si la empresa hace alguna evaluación de riesgo cibernético; y (vi) si la empresa conoce alguna reglamentación y/o legislación nacional o territorial que requiera las empresas de su sector implementen prácticas de gestión de riesgo cibernético. Además, el modelo cuenta con variables dicotómicas que identifican el sector económico a lo cual pertenece la empresa, tal como Industria, Comercio y Servicios, y el tamaño de la empresa.

Los resultados indican que hay una relación positiva y estadísticamente significativa entre el presupuesto designado por la empresa para seguridad digital con el número de incidentes. Con respecto a prácticas de seguridad digital, igualmente se verificó una relación significativa y positiva entre las empresas que implementan medidas técnicas de seguridad, que hacen evaluación de riesgo y que adoptan estándares. Es decir, empresas que implementan más medidas de seguridad digital tienden a identificar un número más grande de incidentes digitales. Esto significa que muchas empresas que no implementan estas medidas ni tienen el conocimiento que son blancos de ataques cibernéticos.

PRESUPUESTO PARA LA SEGURIDAD DIGITAL EN LAS EMPRESAS

Es interesante señalar que la gran mayoría de las empresas que sí asignaron presupuesto para TI, también asignaron presupuesto para asuntos de seguridad digital: cerca del 92% de las empresas que asignan presupuesto a TI también asignan a la seguridad digital. Teniendo en cuenta las empresas que asignan presupuesto para TI, se verificó cuanto fue asignado en 2016 por las empresas a la seguridad digital, como indicado en el Gráfico 19:

GRÁFICO 19: PRESUPUESTO ANUAL PARA LA SEGURIDAD DIGITAL DE LAS EMPRESAS QUE ASIGNAN RECURSOS PARA TI (2016)



Número de observaciones: 250

Se aprecia que la distribución del presupuesto es sesgada hacia la derecha, así que se prefirió trabajar con mediana del presupuesto para la seguridad digital en 2016 considerando el tamaño de la empresa, así como su sector económico. Es importante observar que el Cuadro 1 presenta el presupuesto para la seguridad digital que se encuentra en el medio de los valores proporcionados por las empresas. Asimismo, cabe señalar que 8% de estas empresas no asignaron presupuesto alguno a la seguridad digital, mientras empresas de algunos sectores, en particular del sector financiero, llegaron a invertir más de COP $6.000.000.000 en seguridad digital en 2016.

CUADRO 1: MEDIANA DEL PRESUPUESTO ANUAL PARA LA SEGURIDAD DIGITAL POR EMPRESA QUE ASIGNA RECURSOS PARA TI (2016)

TAMAÑO DE LA EMPRESA	COP ($)	SECTOR ECONÓMICO	COP ($)
Micro	500 mil – 1 millón	**Comercio**	5 – 10 millones
Pequeña	5 – 10 millones	**Industria**	45 – 60 millones
Mediana	15 – 25 millones	**Servicios**	5 millones – 10 millones
Gran	120 – 140 millones		

Número de observaciones: 250

Al analizar los valores de las empresas colombianas que asignaron algún presupuesto a la seguridad digital, se observó que la mediana del presupuesto de la seguridad digital en relación a las ventas de las empresas fue aproximadamente 0,3% del as ventas en 2016. Es decir, cuando se asignó presupuesto a la seguridad digital, este presupuesto no llegó al 1% de las ventas de la empresa en 2016.

Además, se verificó que, en promedio simple, la mayor parte del presupuesto fue asignado para plataformas y medios tecnológicos, mientras la generación de capacidades recibió la menor cantidad de recursos. Aproximadamente 47% del presupuesto de seguridad digital fue asignado a plataformas y medios electrónicos, y 11% a generación de capacidades que,

a su vez, incluye temas como capacitación y concientización. Es interesante observar que, en el capítulo sobre prácticas de seguridad digital en las empresas, se observó que la falta de conciencia y conocimiento por parte de los empleados estuvo entre las fallas que más afectaron la capacidad de las empresas en materia de seguridad digital en 2016.

CUADRO 2: ASIGNACIÓN DEL PRESUPUESTO PARA ASUNTOS DE SEGURIDAD DIGITAL (2016)

CATEGORÍAS	PORCENTAJE
Recursos Humanos (ej. empleados, contratistas)	25 %
Plataformas y Medios Tecnológicos (ej. hardware, software)	47 %
Generación de Capacidades (ej. capacitación, concientización, investigación)	11 %
Servicios Especializados (ej. gestión de seguridad, externalización, soporte)	17 %

Número de observaciones: 230

Finalmente, se realizó una regresión lineal con el objetivo de identificar los factores que llevan una empresa a invertir más en seguridad digital. En esta regresión, se utilizó el logaritmo del presupuesto asignado por las empresas para asuntos de seguridad digital durante el año de 2016 como la variable dependiente (Anexo 3). Se optó por el logaritmo del presupuesto para la seguridad digital, con vistas a normalizar la distribución de la variable. Además, se incluyeron las siguientes variables independientes: (i) el número de empleados de la empresa; (ii) el porcentaje aproximado de personal de la empresa que tiene acceso a Internet para desarrollar sus actividades profesionales; (iii) el logaritmo de las ventas de la empresa; (v) el porcentaje del capital social de la empresa que es extranjero; y (iv) el logaritmo del número de incidentes digitales sufridos por la empresa en 2016.

El modelo también cuenta con variables dicotómicas que identifican el sector económico al cual pertenece la empresa, tal como Industria, Comercio y Servicios, y el tamaño de la empresa. Igualmente se incluyen las siguientes variables dicotómicas: (i) si la empresa tiene un área, cargo(s) o rol(es) dedicado(s) a la seguridad digital; (ii) si la empresa implementa medidas técnicas de seguridad (por ejemplo, pruebas de vulnerabilidad, mantenimiento de la infraestructura de TI); (iii) si la empresa adopta políticas de seguridad digital (por ejemplo, política de acceso al sistema, política de actualización de contraseñas, concientización); (iv) si la empresa implementa estándares (por ejemplo, ISO 27001, otros estándares internacionales); (v) si la empresa hace alguna evaluación de riesgo cibernético; y (vi) si la empresa conoce alguna reglamentación y/o legislación nacional o territorial que requiera las empresas de su sector implementen prácticas de gestión de riesgo cibernético.

Los resultados indican que hay una relación positiva y estadísticamente significativa entre el número de empleados, las ventas de la empresa y el presupuesto para la seguridad digital. En otras palabras, a **mayor sea el número de empleados y las ventas de las empresas, más grande será el presupuesto asignado a la seguridad digital.**

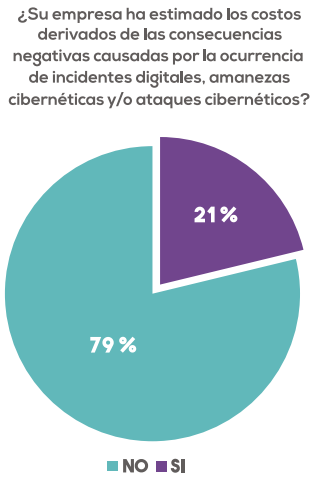
Con respecto a prácticas de seguridad digital, igualmente se verificó una relación significativa y positiva entre el presupuesto para la seguridad digital y las siguientes variables dicotómicas: existencia de un cargo o rol dedicado a la seguridad digital, medidas técnicas, políticas de seguridad digital, estándares, y evaluación de riesgo. En otras palabras, las empresas que implementan estas prácticas de seguridad digital asignan un presupuesto más grande para la seguridad digital que las empresas que no adoptan estas prácticas. Finalmente, cabe destacar la relación negativamente significativa entre las microempresas y el presupuesto para la seguridad digital. En otras palabras, **las microempresas tienen presupuestos para la seguridad digital más pequeños en términos absolutos**. Por otro lado, **las empresas del sector de Servicios (principalmente del sector financiero) tienden a asignar un presupuesto más grande a la seguridad digital.**

Es importante tener en cuenta que el presupuesto para la seguridad digital es un costo de prevención de incidentes digitales. Es decir, son los recursos utilizados para cubrir los costos incurridos con las prácticas de seguridad digital. En la próxima sección, serán analizados los costos incurridos como consecuencia de un incidente digital.

COSTO DE LOS INCIDENTES DIGITALES PARA LAS EMPRESAS

Cuando las empresas fueron preguntadas sobre la estimación de los costos derivados de las consecuencias negativas causadas por la ocurrencia de incidentes digitales, 79% de las empresas afirmaron que no contaban con ningún estimativo, como se observa en el Gráfico 20 a continuación:

GRÁFICO 20: EMPRESAS QUE ESTIMARON LAS CONSECUENCIAS NEGATIVAS DE LOS INCIDENTES DIGITALES (2016)

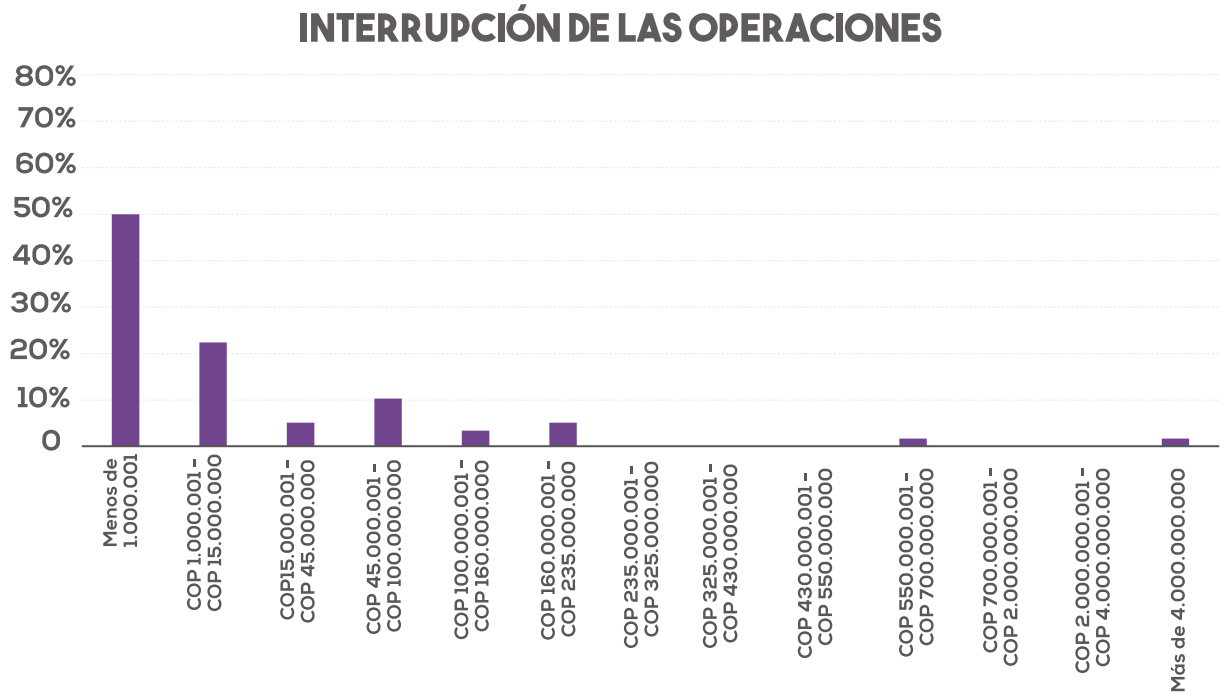


Número de observaciones: 429

Teniendo en cuenta las empresas que estimaron los costos incurridos como resultado de los incidentes digitales, los gráficos a continuación presentan la distribución de los costos con el número de incidentes digitales incurridos por las empresas según cinco categorías de costos: (i) interrupción de las operaciones normales de la empresa; (ii) daño a activos e infraestructura; (iii) sanciones, multas y gastos legales; (iv) daño a la reputación y la imagen del mercado; y (v) pérdida de la propiedad intelectual o de otra información empresarial sensible comercialmente.

En contraste con los costos de prevención de incidentes digitales, descritos en la sección sobre presupuesto a la seguridad digital, estas cinco categorías se refieren a la estimación del costo como una consecuencia de un incidente digital. Por ejemplo, un incidente digital puede llevar a la interrupción de la producción de los productos o de la prestación del servicio de la empresa, afectando sus actividades regulares. Un incidente digital también puede resultar en el robo de datos de la empresa, tal como datos sensibles comercialmente y de su propiedad intelectual. Algunos incidentes buscan atacar la infraestructura tecnológica de las empresas y causar daños a su red y sistemas. Igualmente, un incidente digital puede generar gastos legales, tal como multas reglamentarias y compensaciones a clientes. Asimismo, se buscó incluir los costos a la reputación de la empresa, que puede resultar en la pérdida de confianza de los clientes y, como consecuencia, afectar sus ventas.

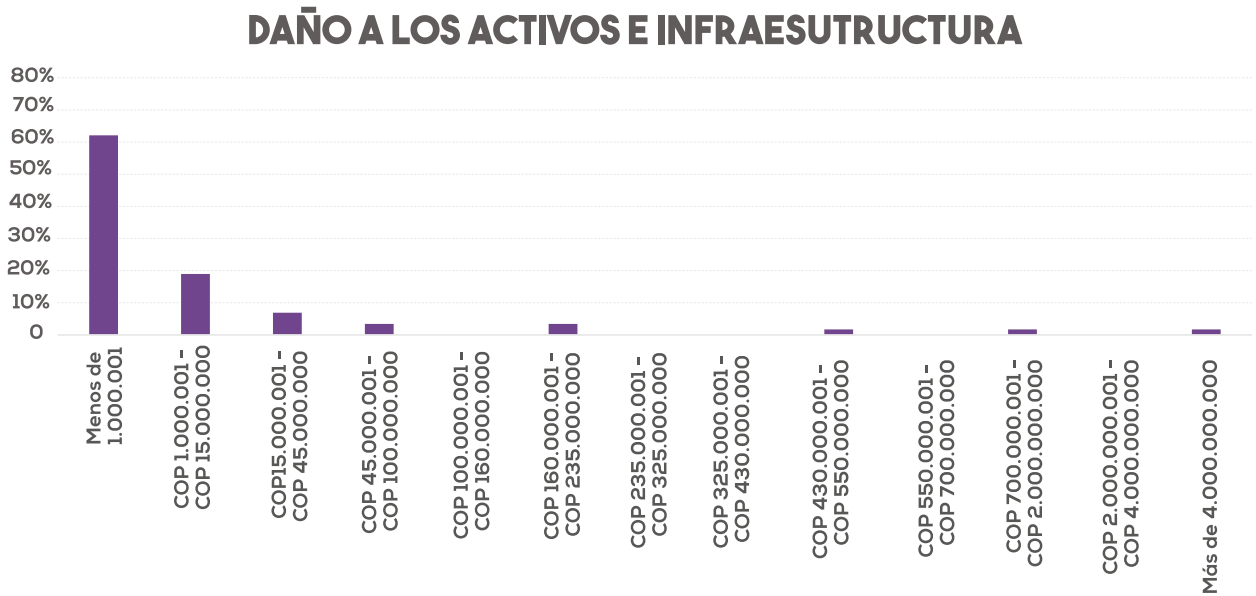
GRÁFICO 21: COSTOS DE INTERRUPCIÓN DE LAS OPERACIONES INCURRIDOS POR LAS EMPRESAS QUE ESTIMARON EL IMPACTO DE LOS INCIDENTES DIGITALES (2016)



Número de observaciones: 58

Con respecto al costo de interrupción de las operaciones normales de la empresa, 50% de las empresas tuvieron un costo más pequeño que COP 1.000.001, 22 % tuvieron un costo entre COP 1.000.001 – COP 15.000.000, y aproximadamente 25 % entre COP 15.000.001 COP 235.000.000. Hay algunas pocas empresas con valores extremos que se alejan del conjunto de datos, llegando a más de COP 4.000.000.000. Las empresas con valores extremos son todas grandes empresas.

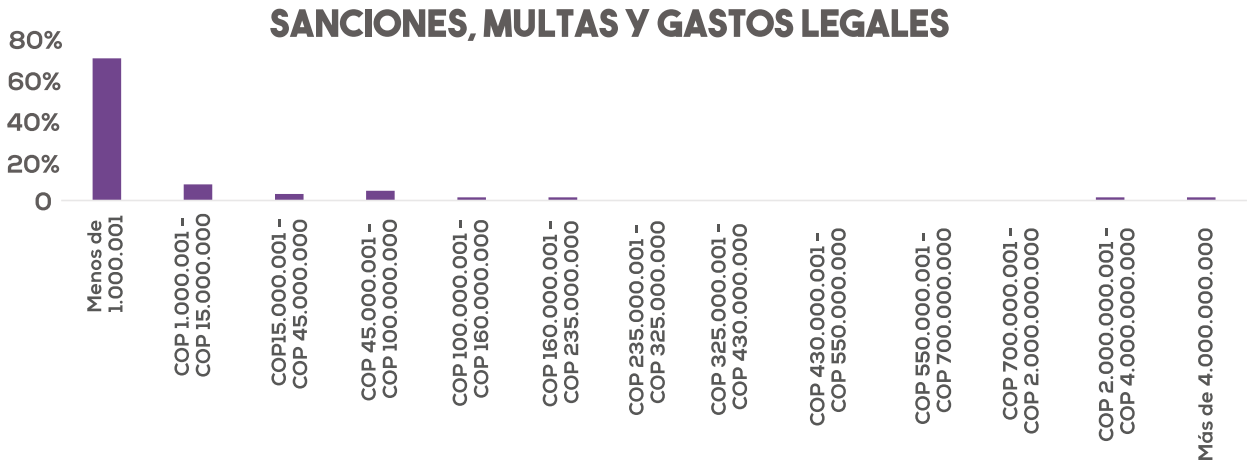
GRÁFICO 22: COSTOS DE DAÑOS A LOS ACTIVOS E INFRAESTRUCTURA INCURRIDOS POR LAS EMPRESAS QUE ESTIMARON EL IMPACTO DE LOS INCIDENTES DIGITALES (2016)



Número de observaciones: 58

Con respecto al daño a los activos e infraestructura de la empresa, más del 60% de las empresas tuvieron un costo más pequeño que COP $1.000.001, aproximadamente 20% tuvieron un costo entre COP $1.000.001 – COP $15.000.000, y aproximadamente 15% entre COP $15.000.001 – COP $235.000.000. Cerca del 5% de las empresas presentaron valores extremos que se alejan del conjunto de datos, llegando a más de COP $4.000.000.000. Además, las empresas con valores extremos son todas grandes empresas.

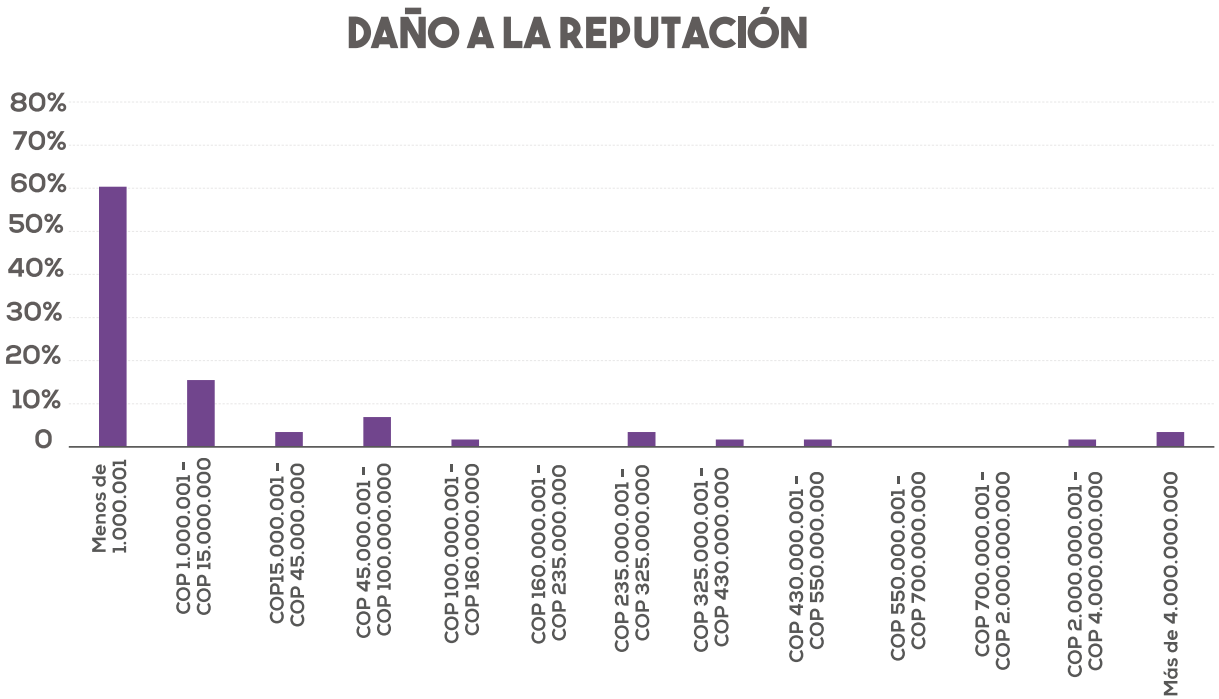
GRÁFICO 23: COSTOS DE SANCIONES, MULTAS Y GASTOS LEGALES INCURRIDOS POR LAS EMPRESAS QUE ESTIMARON EL IMPACTO DE LOS INCIDENTES DIGITALES (2016)



Número de observaciones: 58

Con respecto a sanciones, multas y gastos legales, más de 75% de las empresas tuvieron un costo más pequeño que COP $1.000.001, aproximadamente 12% tuvieron un costo entre COP $1.000.001 – COP $15.000.000, y aproximadamente 10% entre COP $15.000.001 – COP $235.000.000. Cerca de 3% de las empresas presentaron valores extremos que se alejan del conjunto de datos, llegando a más de COP $4.000.000.000 mil millones de pesos colombianos. Cabe remarcar que las empresas con valores extremos eran todas grandes empresas.

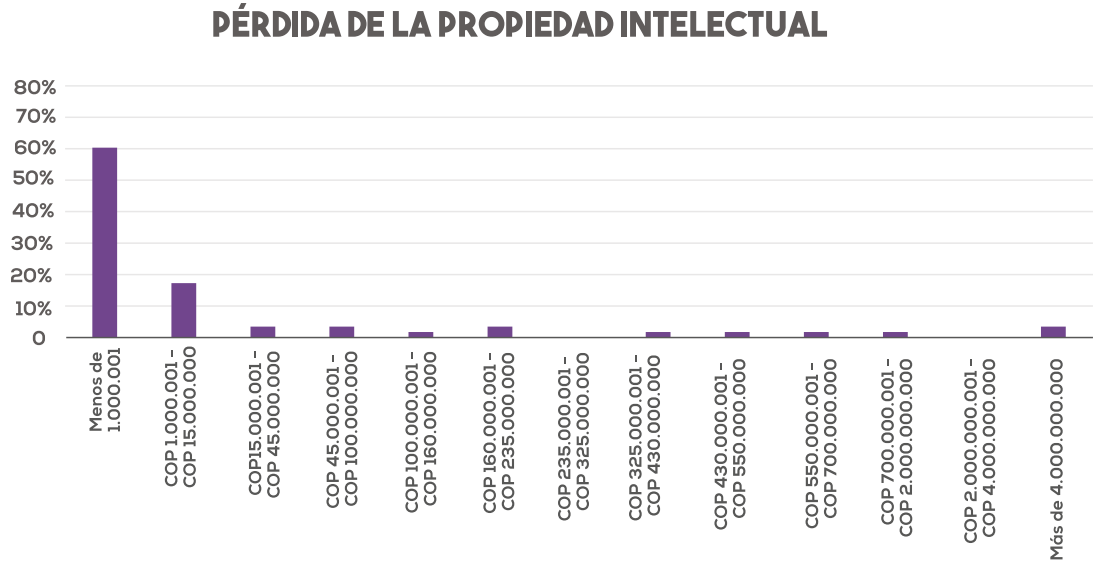
GRÁFICO 24: COSTOS DE DAÑOS A LA REPUTACIÓN INCURRIDOS POR LAS EMPRESAS QUE ESTIMARON EL IMPACTO DE LOS INCIDENTES DIGITALES (2016)



Número de observaciones: 58

Con respecto a daños a la reputación, 60% de las empresas tuvieron un costo más pequeño que COP $1.000.001, aproximadamente 16% tuvieron un costo entre COP $1.000.001 – COP $15.000.000, y aproximadamente 12% entre COP $15.000.001 – COP $235.000.000. Es importante resaltar que de las empresas que participaron en este estudio, hubo un número más grande de empresas con costos relativos a la reputación por encima de los $325 millones de pesos colombianos, el cual corresponde aproximadamente al 12%, mientras que un 5% reportaron que presentaron daños a la reputación de más de COP $2.000.000.000. En este último grupo, la mayoría consistieron en grandes empresas, incluyendo empresas del sector Comercio, de comunicaciones y del sector financiero.

GRÁFICO 25: COSTOS DE PÉRDIDAS DE LA PROPIEDAD INTELECTUAL INCURRIDOS POR LAS EMPRESAS QUE ESTIMARON EL IMPACTO DE LOS INCIDENTES DIGITALES (2016)



Número de observaciones: 58

Finalmente, con respecto a la pérdida de propiedad intelectual, el 60% de las empresas tuvieron un costo más pequeño que COP $1.000.001, aproximadamente 17% tuvieron un costo entre COP $1.000.001 – COP $15.000.000, y aproximadamente 12% entre COP $15.000.001 – COP $235.000.000. Es interesante notar que hay un número más grande de empresas con costos relativos a la pérdida de propiedad intelectual arriba de COP $325 millones: cerca de 10% de las empresas, siendo que 3% presentaron pérdidas a la propiedad intelectual de más de COP $4.000.000.000. En este último grupo, la mayoría consistió en grandes empresas, incluyendo empresas del sector Comercio, y del sector financiero.

Se puede notar que la distribución del costo entre las cinco categorías fue sesgada hacia la derecha, por lo cual se decidió trabajar con la mediana del costo agrupado incurrido por cada empresa, según el tamaño de la empresa. Es decir, el Cuadro 3 presenta el costo de los incidentes digitales que se encuentran en el medio de los valores proporcionados por cada empresa que estimó el impacto de los incidentes digitales.

CUADRO 3: MEDIANA DEL COSTO TOTAL POR EMPRESA QUE ESTIMÓ EL IMPACTO DE LOS INCIDENTES DIGITALES (2016)

TAMAÑO DE LA EMPRESA	COP ($)
Micro	1.5 millón – 6 millones
Pequeña y Mediana	10 – 20 millones
Gran	20 – 45 millones

Número de observaciones: 58

CUADRO 4: COSTO TOTAL POR VENTAS DE LA EMPRESA (2016)

TAMAÑO DE LA EMPRESA	(%)
Micro	1% - 5%
Pequeña y Mediana	0,5% – 1%
Gran	0,005% - 0,015%

Número de observaciones: 58

En el Cuadro 4 se ve representado el costo relativo de incidentes digitales por ventas del año 2016, incurrido por empresa según el tamaño de la empresa. En otras palabras, el porcentaje del costo de incidentes digitales en relación a las ventas de la empresa.

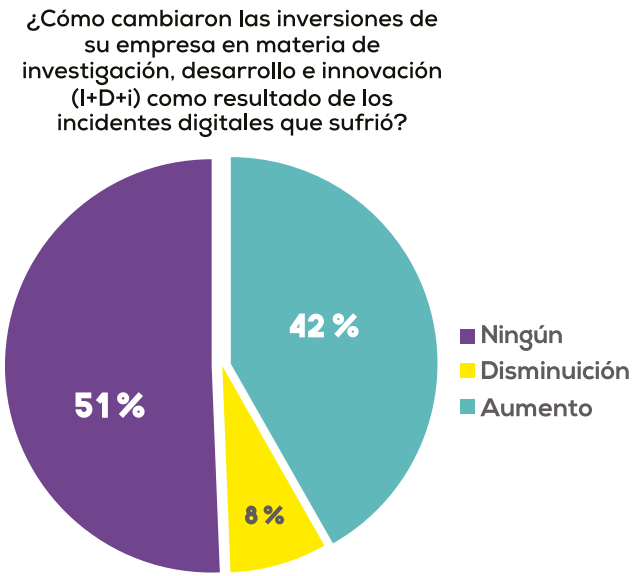
Se logra observar que el costo relativo con incidentes digitales disminuyó a medida que las empresas aumentan de tamaño. Aunque las grandes empresas tuvieron un costo absoluto con incidentes digitales muy superiores que los costos incurridos por una microempresa, por ejemplo, el costo relativo por incidentes digitales de una gran empresa fue significativamente más pequeño.

Cabe destacar que pocas empresas del sector Industria y Comercio proporcionaron información acerca de sus costos. En relación al sector Servicios – que, a su vez, contó con un número más significativo de respuestas se observó que la mediana de sus costos se encuentra entre COP $5.000.000 y COP $11.000.000, con un costo relativo de aproximadamente 0,5% de sus ventas.

Finalmente, se estimó el costo en relación al número de incidentes digitales. Se realizó una regresión lineal en la cual el costo de los incidentes digitales en 2016 fue la variable dependiente y el número de incidentes fue la variable explicativa. Los resultados indican que existe una relación significativa y positiva entre el costo y el número de incidentes. Según el modelo, se estima que **el incremento de una unidad en el número de incidentes aumenta en aproximadamente $500 mil pesos colombianos el costo incurrido por las empresas en Colombia como resultado de incidentes digitales**. Es importante tener en cuenta que este valor es una estimación y que algunos incidentes pueden tener valores más bajos, mientras otros más altos.

Finalmente, se buscó analizar cómo el costo incurridos debido a incidentes digitales en 2016 impactaron las inversiones de las empresas en investigación, desarrollo e innovación (I+D+i), dada la importancia de I+D+i para el desarrollo de una economía digital, así como en el avance de medidas de seguridad digital. Como se muestra en el Gráfico 26 a continuación, entre las empresas entrevistadas, 42% afirmó que han aumentado sus inversiones en I+D+i.

GRÁFICO 26: INVERSIÓN EN I+D+I



Número de observaciones: 58

Entre las empresas que afirmaron que sus inversiones en I+D+i aumentaron como resultado de incidentes digitales, 36% de estas empresas respondieron que sus inversiones aumentaron en más de 15% en 2016. Se nota que la conciencia acerca del impacto causado con los incidentes digitales en las empresas está llevándolas a invertir más en I+D+i.

PARTE 2

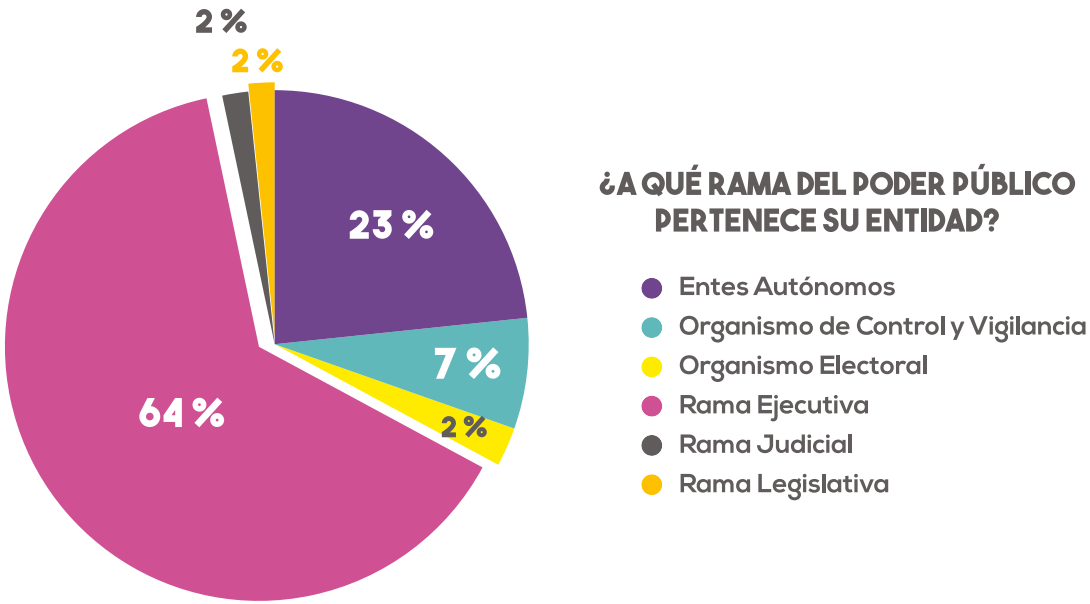
ANÁLISIS DE ENTIDADES DEL SECTOR PÚBLICO

PERFIL DE LAS ENTIDADES

En relación a las entidades públicas colombianas, el 64% de los entrevistados eran de la Rama Ejecutiva, mientras que el 23% eran Entes Autónomos. Los otros entrevistados que constituyeron el otro 13% eran del Organismo Electoral, las Rama Judicial y Legislativa, y Organismos de Control y Vigilancia.

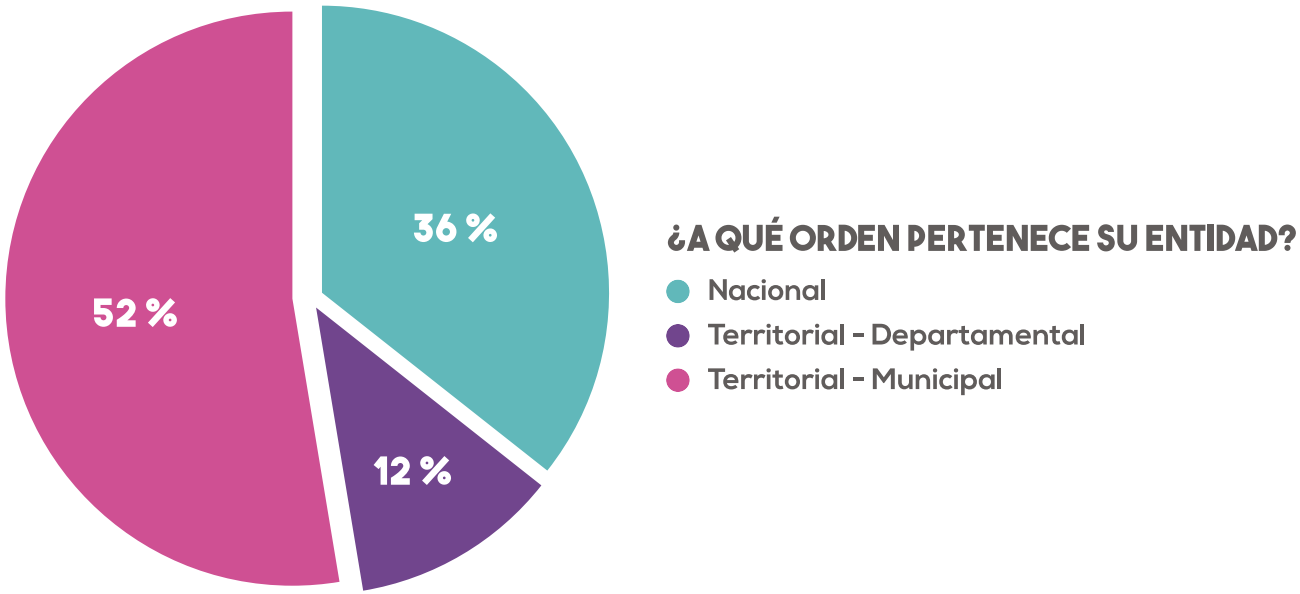
De este número de las Entidades del sector público, el 52% de los entrevistados pertenecían al nivel Territorial-Municipal, frente a un total de 36% de las respuestas pertenecientes a entidades nacionales y 12% del Territorial-Departamental.

GRÁFICO 27: RAMA DEL PODER PÚBLICO A QUE PERTENECE LA ENTIDAD



Número de observaciones: 724

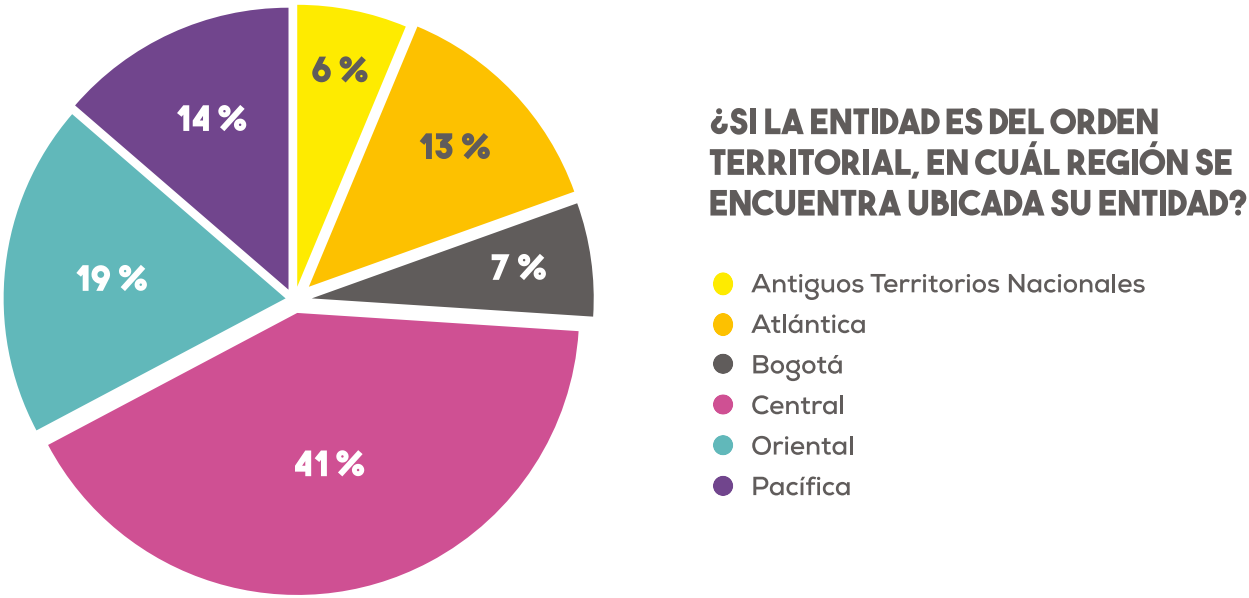
GRÁFICO 28: ORDEN A QUE PERTENECE LA ENTIDAD



Número de observaciones: 724

En cuanto a la distribución regional de los entrevistados del orden territorial (es decir, departamental o municipal), el 41% eran de la Región Central, el 19% de la Región Oriental, el 14% de la Región Pacífica, el 13% de la Región Atlántica, el 7% Bogotá y el restante 6% de la Región de los Antiguos Territorios Nacionales.

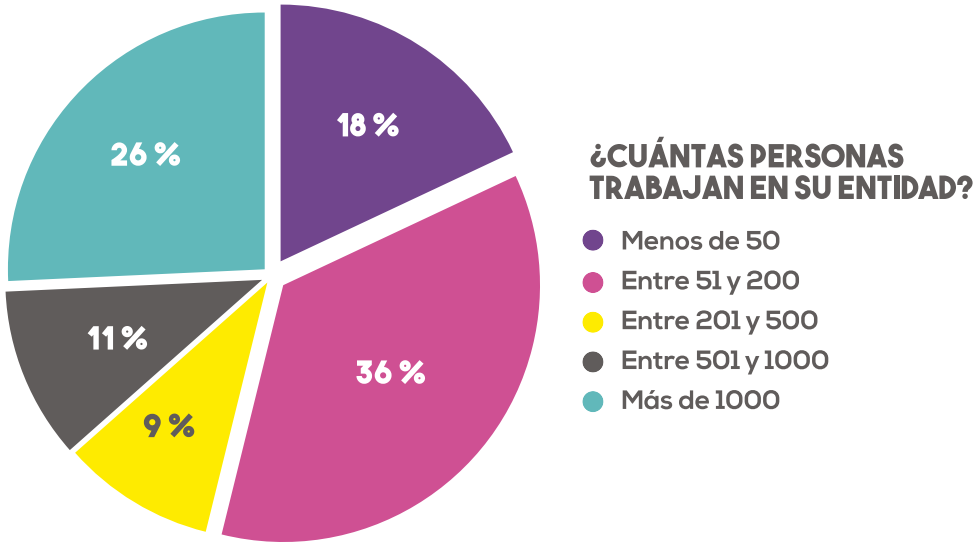
GRÁFICO 29: REGIÓN EN LA CUAL SE ENCUENTRA UBICADA LA ENTIDAD



Número de observaciones: 461

Las Entidades del sector público variaron con un rango justo para los propósitos de este estudio en términos de entidades pequeñas y grandes. Al responder a la pregunta, ***¿Cuántas Personas trabajan en su entidad? (Escoja sólo una respuesta),*** 18% indicaron que tenían menos de 50 empleados, 36% indicaron que tenían entre 51-200 empleados, 9% que tenían entre 201-500 empleados y 11% que tenían entre 501-1000 empleados. La otra respuesta significativa fue que el 26% de los entrevistados indicaron que tenían más de 1.000 empleados.

GRÁFICO 30: NÚMERO DE PERSONAS QUE TRABAJAN EN LAS ENTIDADES



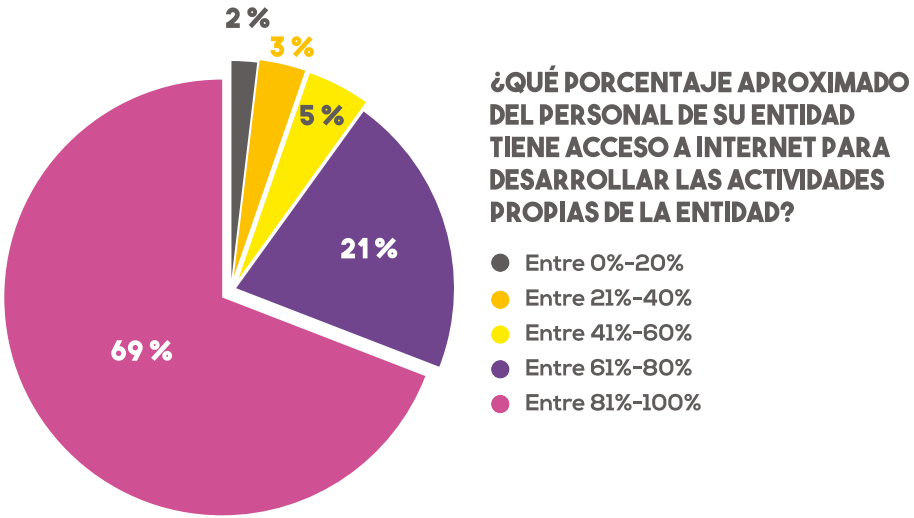
Número de observaciones: 583

A la luz de los resultados anteriores, el perfil de los entrevistados de las entidades estatales podría ser descrito principalmente por entidades de la rama Ejecutiva y la región Central, con más del 46% de los entrevistados con más de 500 empleados.

En relación con los empleados de las Entidades del sector público, el 41% de los entrevistados establecieron una política de BYOD o ***Bring your own device*** ("trae tu propio dispositivo" en español) y permitieron el acceso para el uso de dispositivos USB externos y otros dispositivos de almacenamiento como discos externos, bases de datos y archivos en servidores. 59% de los entrevistados respondieron que no lo hicieron. Entre los entrevistados de las Entidades del sector público, el 60% respondieron que no tenían una política de BYOD comparado con el 40% que tenía uno en funcionamiento.

Más del 69% de los entrevistados de las Entidades del sector público indicaron que entre el 81% y el 100% de sus empleados tenían acceso a Internet en el trabajo; el 21% respondieron que entre 61-80%; y el 10% que entre 0-60%.

GRÁFICO 31: PORCENTAJE DE PERSONAL DE SU ENTIDAD QUE TIENE ACCESO A INTERNET (2016)



Número de observaciones: 583

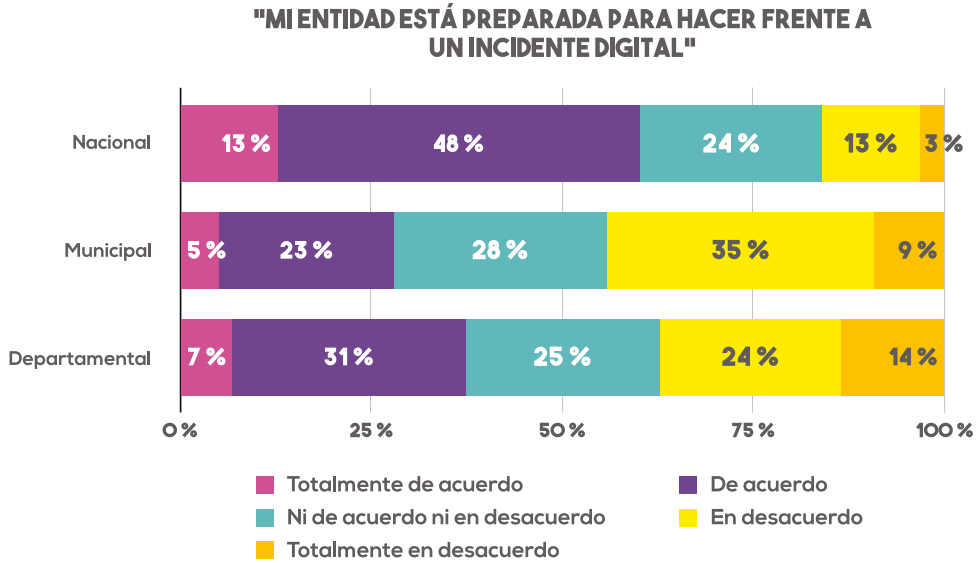
PRÁCTICAS DE SEGURIDAD DIGITAL EN LAS ENTIDADES

Habiendo identificado que la mayoría de las entidades públicas permiten a sus empleados acceder a Internet para realizar las actividades de las entidades, es importante considerar las medidas que las entidades públicas han tomado para protegerse. Cuando se hizo la pregunta, ***Mi entidad/empresa está preparada para hacer frente a un incidente digital,*** era evidente que la mayoría de las entidades a nivel nacional se sentía preparada. Las entidades indicaron que el 13% y el 48%, respectivamente en el nivel nacional se sentían muy preparados o preparados. Estos datos, comparados con el nivel municipal y departamental, muestran que solo el 28% a nivel municipal y el 38% a nivel departamental se sintieron muy preparados o preparados para manejar un incidente.

Se pueden deducir algunas conclusiones de estos resultados, ya que demuestra que existe un nivel más alto de confianza en la preparación a nivel nacional que está respaldado por todas las iniciativas que

está implementando el Gobierno nacional en el desarrollo de una economía digital segura. Por otro lado, también indica que es necesario desarrollar estas iniciativas a nivel municipal y departamental. Véase a continuación el gráfico:

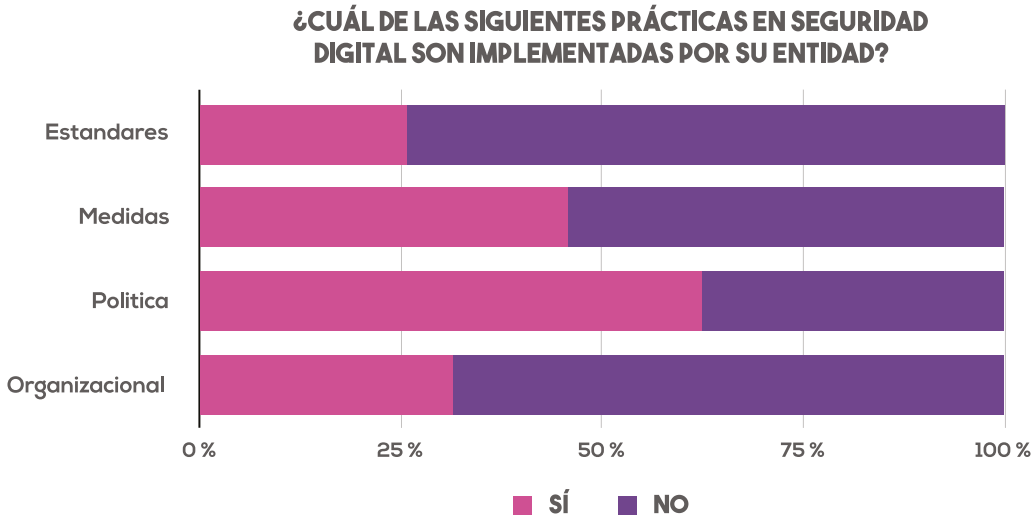
GRÁFICO 32: NIVEL DE PREPARACIÓN DE LA ENTIDAD PARA HACER FRENTE A UN INCIDENTE DIGITAL



Número de observaciones: 559

Esto condujo a un análisis de qué prácticas de seguridad digital han implementado las entidades estatales a este respecto. Cuando se preguntó, ***¿Cuál de las siguientes prácticas en seguridad digital (seguridad digital y/o seguridad de la información) son implementadas por su entidad?,*** similar a la respuesta de las empresas, la mayoría de los entrevistados de entidades públicas indicaron que tienen políticas en funcionamiento, con normas y medidas organizativas de menor prioridad. Del total de entrevistados, el 62% indicó que las políticas se implementaron, comparado con el 46% de las medidas técnicas de implementación, y solo el 31% indicó que implementaron medidas organizativas.

GRÁFICO 33: PRÁCTICAS DE SEGURIDAD DIGITAL IMPLEMENTADAS POR LAS ENTIDADES

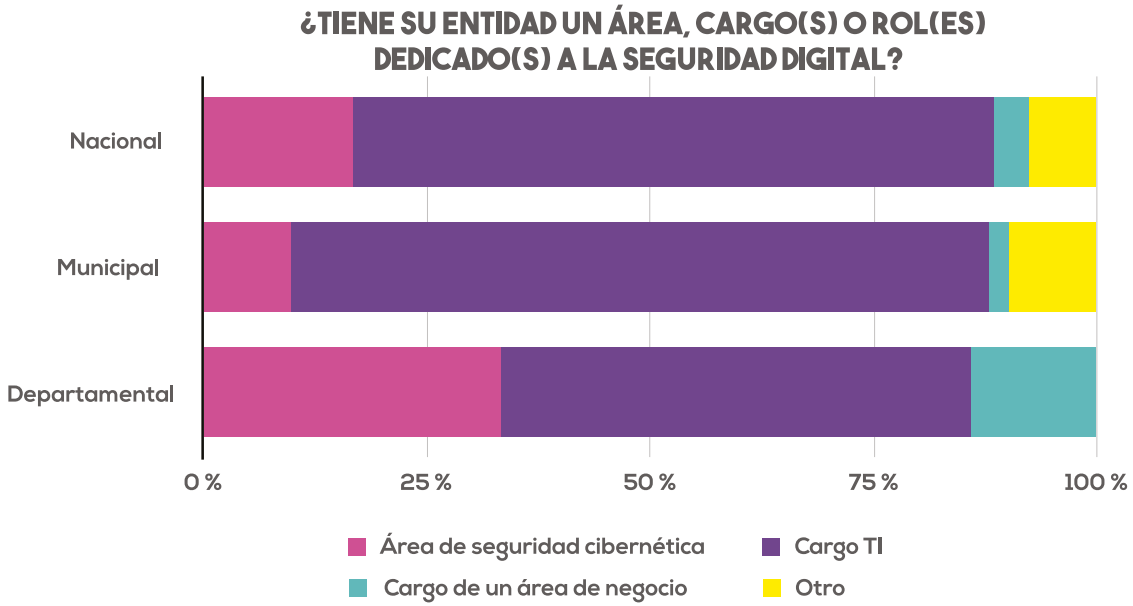


Número de observaciones: 559

Estos resultados son particularmente interesantes cuando se analizan frente a los resultados de la pregunta, ***¿Tiene su entidad un área, cargo (s) o rol(es) dedicado (s) a la seguridad digital (seguridad digital y/o de seguridad de la información)?***, como si la entidad estatal pusiera un bajo énfasis en la implementación de medidas organizacionales, entonces hay una fuerte probabilidad de que no tendrían un cargo dedicado para la seguridad digital. Entre los entrevistados, solo el 33% a nivel nacional y el 10% y 17% respectivamente a nivel municipal y departamental tienen un área dedicada a la seguridad digital dentro de su organización.

Como se destacó en la sección anterior relacionada con las empresas, existe una tendencia general a transferir la responsabilidad de la respuesta a incidentes y la seguridad digital bajo las funciones generales del Departamento de Tecnología de la Información. Como tal, el 52% a nivel nacional, el 78% a nivel municipal y el 72% a nivel departamental abordan la cuestión de la seguridad digital bajo el Departamento de Tecnología de la Información. Solamente un porcentaje muy pequeño de los entrevistados abordó esto bajo las áreas de negocio generales de las entidades u otras áreas. Véase el gráfico a continuación:

GRÁFICO 34: ENTIDADES CON ÁREA, CARGO(S) O ROL(ES) DEDICADO(S) A LA SEGURIDAD DIGITAL



Número de observaciones: 246

Cuando se preguntó, ¿Cuántas personas conforman el equipo o área que tiene a cargo la seguridad digital (seguridad digital y/o seguridad de la información) en su entidad?, es notable que el 44% de los entrevistados tenía solo entre 1-2 empleados, el 27% entre 3-5 personas y el 29% indicaron que tenían más de 5. Estos resultados enfatizan la necesidad de examinar cómo se está abordando el tema de la seguridad digital dentro de las entidades estatales. Algunos han argumentado que cuando se juntan las dos áreas, los puntos de vista de un departamento de TI varían desde el punto de vista de la seguridad en relación con las medidas proactivas y reactivas que una entidad debe implementar. Según Forbes, ***"ser una subdivisión del departamento de TI hace que la seguridad esté ciega a los procesos empresariales importantes y a la toma de decisiones a nivel corporativo***

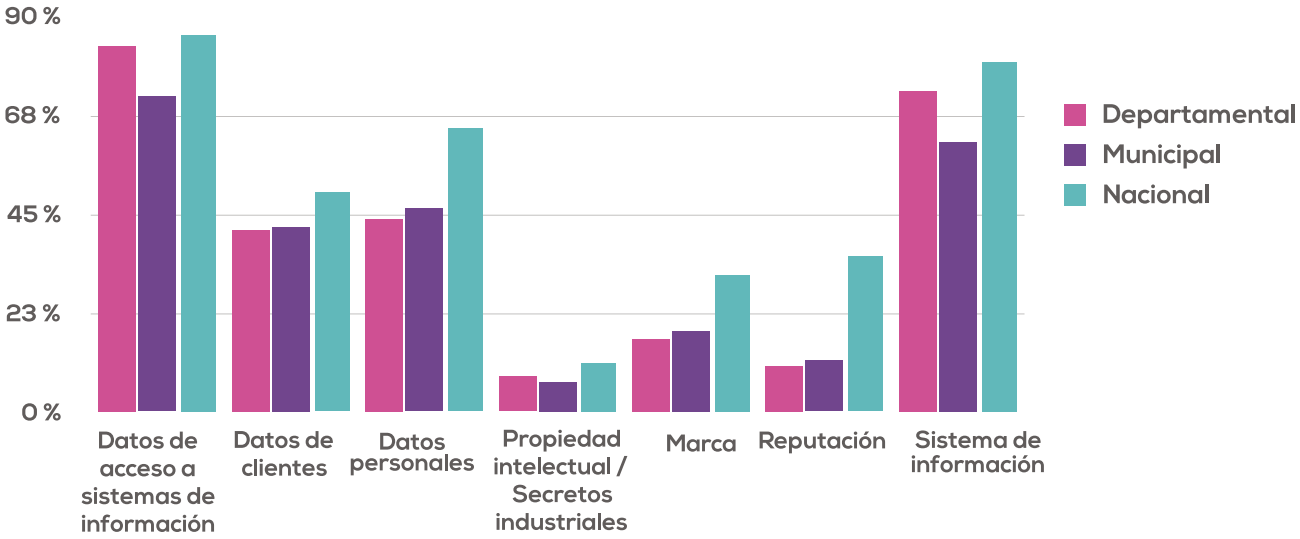
y departamental"[8]. Por ejemplo, los equipos de seguridad a menudo no forman parte de los procesos de planificación en los departamentos de RR.HH., Marketing e I+D, ni se les da la oportunidad de revisar las inversiones antes de que se hagan. Como resultado, los equipos de seguridad se incorporan después del hecho, y esto puede afectar el presupuesto final ya que las entidades pueden terminar gastando más en recuperación en lugar de invertir en el inicio en una solución de seguridad proactiva. Sin embargo, si se les da un rol más prominente dentro de la organización, los equipos de seguridad podrían asesorar a su organización de manera proactiva, reduciendo así los riesgos de manera significativa.

---

8 Forbes (julio de 2015) Why It's Worth Divorcing Information Security From IT, accedida en: https://www.forbes.com/sites/frontline/2015/06/22/why-its-worth-divorcing-information-security-from-it/#3ecd98c342a3, Última entrada: 30 de agosto de 2017

Además, en la identificación de riesgos y la implementación de medidas de mitigación del riesgo, las entidades estatales deben considerar qué activos creen que deberían ser priorizados para su protección. En respuesta a la pregunta, ***¿A la hora de protegerse frente a incidentes digitales, amenazas cibernéticas y/o ataques cibernéticos, cuáles de estos datos y/o activos de información son priorizados por su entidad?***, a nivel nacional, el acceso a los datos en el sistema de información y el acceso a los sistemas de información tenían la mayor prioridad en relación con los datos personales y después de estos, los datos de clientes, en términos de prioridad. A nivel municipal y departamental se observaron resultados similares. Esto es importante ya que, sobre la base de lo que prioriza una entidad, podría ser una indicación de dónde invertirá en términos de seguridad digital. Véase los gráficos abajo:

GRÁFICO 35: DATOS Y ACTIVOS PRIORIZADOS POR LAS ENTIDADES



Número de observaciones: 246

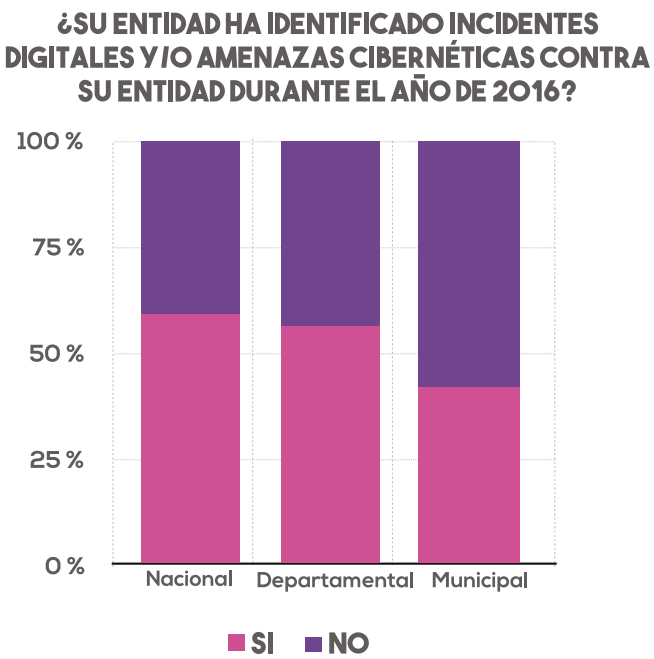
Como se ha mencionado anteriormente, comprender el riesgo es importante. En este Estudio, ***Gestión de riesgos de seguridad digital ha sido definida como*** el conjunto de actividades coordinadas dentro de una organización o entre organizaciones, para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en un conjunto flexible y sistemático de procesos cíclicos, lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital ("medidas de seguridad") sean apropiadas para el riesgo y los objetivos económicos y sociales en juego. Cuando los participantes del Estudio respondieron a la pregunta ***¿Su entidad / empresa realiza una evaluación de riesgo sobre la información que adquiere para mejorar sus operaciones?***, 89% entidades a nivel nacional, 80% entidades a nivel municipal y 88% entidades a nivel Departamental respondieron positivamente.

Posteriormente, cuando se preguntó ***¿La gestión de riesgo de su entidad / empresa está alienada con estándares internacionales,*** es interesante observar que el 87% a nivel nacional respondió positivamente, comparado con el 43% del nivel municipal y el 59% del nivel departamental. El examen de estas prácticas es importante, dado a que, si una entidad toma medidas proactivas como la evaluación de riesgos y la aplicación de normas internacionales, se crea un entorno para la gestión y mitigación de riesgos.

INCIDENTES DIGITALES EN LAS ENTIDADES

Cuando se formuló la pregunta respecto a si se han identificado incidentes digitales contra su organización en 2016, más de la mitad de las entidades estatales de orden nacional y territorial departamental respondieron afirmativamente. El 59% de las Entidades de orden nacional identificaron incidentes digitales, mientras que un 56% de las entidades de orden territorial departamental respondieron de la misma forma. Por otro lado, 42% de las entidades de orden territorial municipal contestaron que han identificado los incidentes digitales.

GRÁFICO 36: PORCENTAJE DE ENTIDADES ESTATALES QUE IDENTIFICARON INCIDENTES DIGITALES (2016)



Número de observaciones: 517

Con el objetivo de comprender el por qué algunas entidades estatales identificaron incidentes digitales y otras no, se adelantó una ecuación de determinantes de la probabilidad que una entidad pública en Colombia identifique incidentes digitales y/o amenazas cibernéticas contra su organización, donde la variable dependiente toma el valor de "1" si la entidad identifica incidentes digitales y "0" si no los identifica.

Dentro de las variables explicativas, se incluyeron cuatro variables dicotómicas: (i) si la entidad pública tiene un área, cargo(s) o rol(es) dedicado(s) a la seguridad digital; (ii) si la entidad pública conoce alguna reglamentación y/o legislación nacional o territorial que requiera las entidades implementen prácticas de gestión de riesgo cibernético; (iii) si la entidad implementa medidas técnicas (por ejemplo, pruebas de vulnerabilidad, mantenimiento de la infraestructura de TI); (iv) si la entidad implementa políticas de seguridad digital (por ejemplo, política de acceso al sistema, política de actualización de contraseñas, concientización); (iv) si la entidad implementa estándares (por ejemplo, ISO 27001, otros estándares internacionales); (v) si la entidad hace alguna evaluación

de riesgo cibernético. Además, se incluyen variables dicotómicas acerca del orden de la entidad. Es decir, nacional, territorial departamental, o territorial municipal.

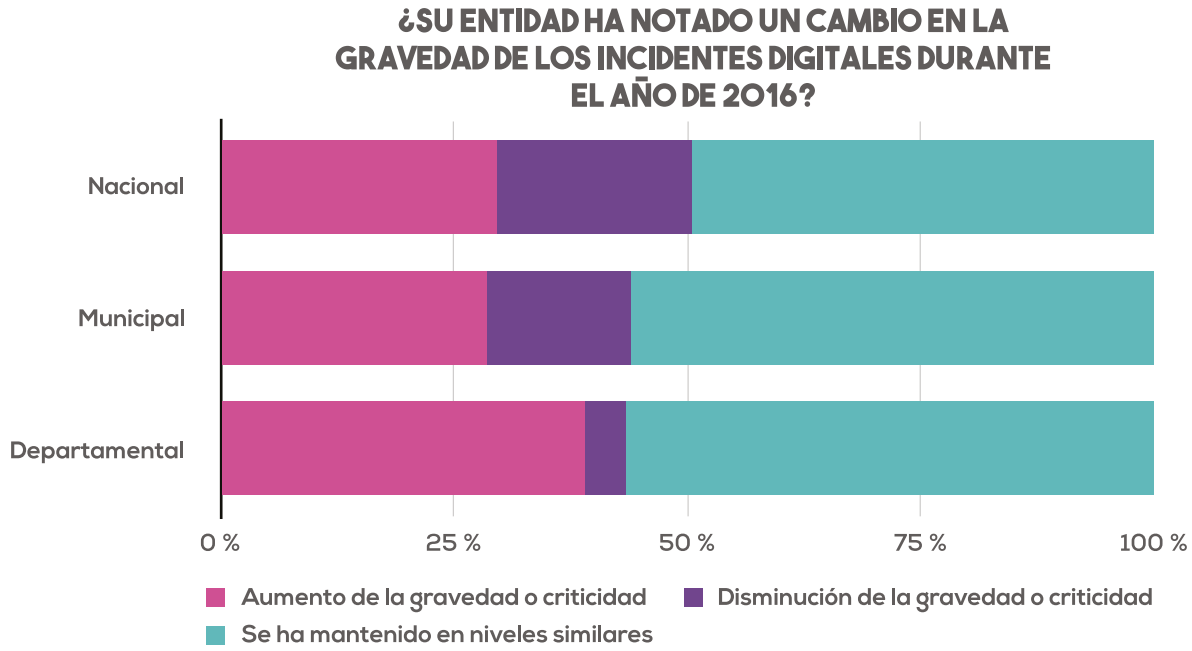
También se incluyeron otras variables explicativas, como el presupuesto total de inversión en pesos colombianos de la entidad durante el año de 2016, el número de personas que trabajan en la entidad, el porcentaje aproximado de personal de la entidad que tiene acceso a Internet para desarrollar sus actividades profesionales, así como el valor aproximado de presupuesto designado por la entidad para la seguridad digital. Dada la naturaleza binaria de la variable dependiente, se utiliza un modelo de estimación ***LOGIT***.[9]

Los resultados muestran que hay una relación estadísticamente significativa positiva entre el conocimiento de alguna reglamentación y/o legislación sobre prácticas de gestión de riesgo y la identificación de incidentes digitales. De hecho, las entidades que identificaron incidentes digitales destacaron su conocimiento acerca de la Política Nacional de Seguridad Digital (Documento CONPES 3854 de 2016), aprobado el 11 de abril de 2016. También hay una relación estadísticamente significativa positiva entre la implementación de medidas técnicas, las prácticas de evaluación de riesgo y la identificación de incidentes digitales. Igualmente existe una relación estadísticamente significativa positiva entre la identificación de incidentes y las siguientes variables explicativas: el valor aproximado de presupuesto designado por la entidad para la seguridad digital, el número de personas que trabajan en la entidad, el porcentaje de personal que tiene acceso a Internet.

Otra área examinada por el estudio fue la experiencia de entidades estatales con incidentes de seguridad digital. En respuesta a la pregunta, ¿***Su entidad/empresa ha notado un cambio en la gravedad (o criticidad) de los ataques cibernéticos durante el año 2016,*** la mayoría de los entrevistados (50% Nacional, 56% Municipal y 57% Departamental) indicaron que la gravedad de los ataques cibernéticos sigue siendo la misma. Solo el 30% a nivel nacional, el 28% a nivel municipal y el 39% a nivel departamental, informaron que habían observado un cambio.

9 Este modelo asume que los efectos individuales han sido promediados, lo que facilita el cálculo y la interpretación de los efectos marginales que, a su vez, miden el efecto de un cambio en uno de los regresores sobre la variable dependiente.

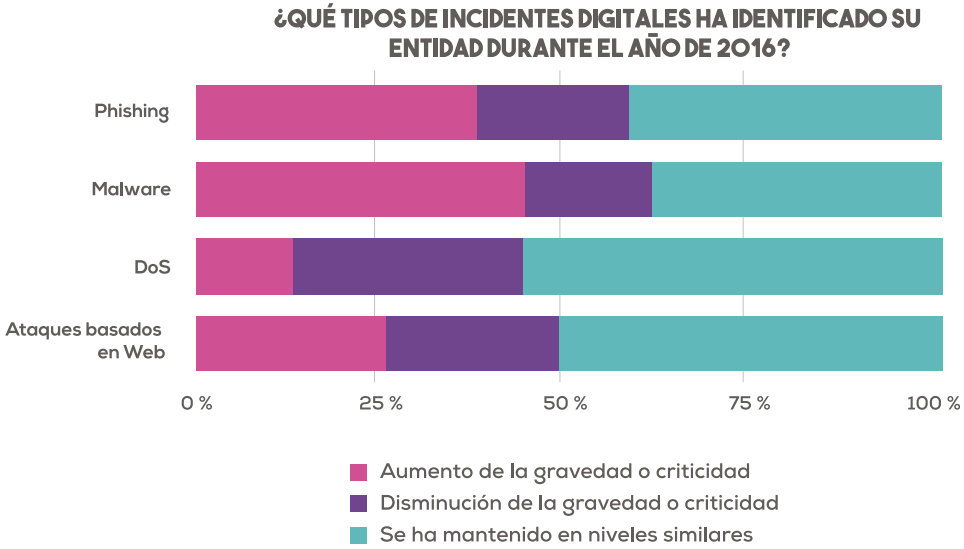
GRÁFICO 37: CAMBIO EN LA GRAVEDAD DE LOS INCIDENTES DIGITALES



Número de observaciones: 240

En términos de entidades colombianas que identifican realmente no solo el aumento en gravedad sino el tipo de ataques, los entrevistados indicaron que han visto el mayor aumento en ataques de phishing y malware. Véase el siguiente gráfico:

GRÁFICO 38: GRAVEDAD DE LOS INCIDENTES DIGITALES



Número de observaciones: 240

A este respecto, cuando se les preguntó, ¿En la ocurrencia de un incidente digital, amenaza cibernética y/o un ataque cibernético, quiénes son notificados en su entidad?, fue interesante que de las entidades que respondieron a la pregunta, el 73% contestó que informarían a los Directivos de la propia organización con solo un 23% indicando que le reportarían al Asesor legal, un 20% informaría a la autoridad local/regional, un 38% a las autoridades nacionales (policía, entidades regulatorias, fiscalías, etc.) y un 25% indicando que se reportarían al Equipo de Respuesta a Incidentes Cibernéticos (CSIRT). La baja indicación en la notificación de incidentes a la autoridad nacional, en última instancia, impacta al Gobierno nacional en la comprensión estatal de los incidentes de seguridad digital en Colombia. Si bien el Estado a nivel nacional continúa invirtiendo en mecanismos para aumentar las denuncias, se puede inferir que es necesario incrementar estos esfuerzos al interior de las entidades estatales.

Estos datos, si se comparan con la pregunta, ¿***A qué nivel pertenece el área a cargo de la seguridad digital (seguridad digital y/o de seguridad de la información) en su entidad? (El nivel superior o jerárquico es el más alto),*** cabe destacar que el 47% a nivel

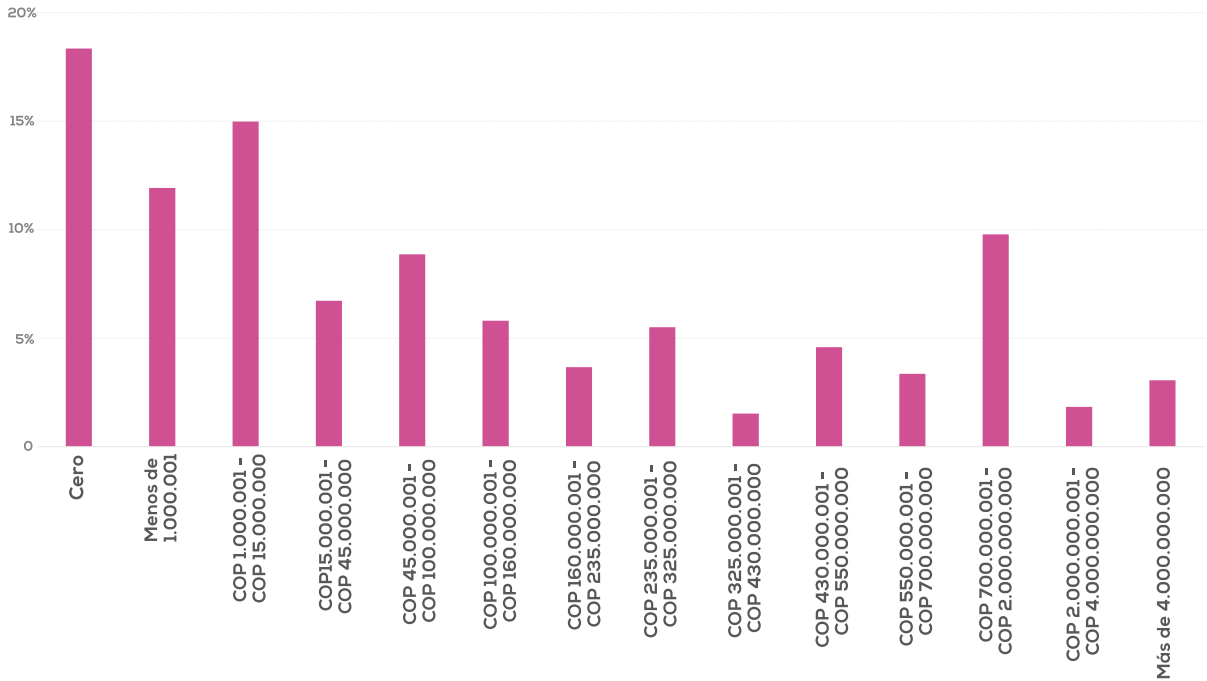
nacional, el 68% a nivel municipal y el 57% a nivel departamental, indica que pertenece en el nivel operativo. En comparación con el nivel jerárquico (o directivo), el 27% a nivel nacional, el 16% a nivel municipal y el 29% a nivel departamental indicaron que pertenece allí. Lo que se podría inferir de estos resultados es que mientras que la seguridad digital no se coloca al nivel de director, sí es al primer nivel dentro de una entidad a la que se informan los incidentes de seguridad digital.

Es importante tomar nota de dónde se denuncian los incidentes cibernéticos y en qué nivel se ubica la seguridad digital, ya que proporciona información sobre cómo una entidad podría abordar estratégicamente incidentes y presupuestos relacionados a este respecto. Cuando se les preguntó: ¿***Cuáles de las siguientes fallas afectan más la capacidad de su entidad/empresa en materia de seguridad digital (seguridad digital y/o seguridad de la información)? Por favor, califique de: 1 (afecta menos o no afecta) a 5 (afecta más),*** la mayoría de los entrevistados identificaron la ***Falta de personal dedicado y Falta de presupuesto*** como las dos razones que los afectan más.

PRESUPUESTO PARA LA SEGURIDAD DIGITAL EN LAS ENTIDADES

Cabe destacar que la mayoría de las entidades que asignaron presupuesto para TI en 2016 también lo hicieron para asuntos de seguridad digital: cerca de 82% de las entidades estatales que asignaron presupuesto a TI también asignaron a la seguridad digital en 2016. Teniendo en cuenta las empresas que asignaron presupuesto para TI, se verificó cuanto fue asignado en 2016 por las entidades estatales, como indicado en el Gráfico 39.

GRÁFICO 39: PRESUPUESTO PARA LA SEGURIDAD DIGITAL (2016)



Número de observaciones: 327

Como la distribución del presupuesto es sesgada a la derecha, el Cuadro 5 presenta la mediana del presupuesto para la seguridad digital en 2016 considerando el orden al cual pertenecen las entidades estatales. Es importante observar que el Cuadro 5 presenta el presupuesto para la seguridad digital que se encuentra en el medio de los valores proporcionados por las entidades nacionales. Sin embargo, se observó que 18% de las entidades estatales que asignaron presupuesto a TI, no asignaron ningún recurso a la seguridad digital, en particular las entidades territoriales de órdenes municipal y departamental. Por otro lado, se observó que algunas entidades que llegaron a invertir más de COP $6.000.000.000 de pesos colombianos, siendo la mayoría del orden nacional, pero también hubo casos aislados de entidades de orden territorial municipal y departamental.

CUADRO 5: MEDIANA DEL PRESUPUESTO PARA LA SEGURIDAD DIGITAL POR ENTIDAD QUE ASIGNARON RECURSOS A TI (2016)

ORDEN	COP ($)
Municipal	1 millón – 5 millones
Departamental	25 – 35 millones
Nacional	235 – 265 millones

Número de observaciones: 327

Al analizar los valores de las entidades estatales que asignaron algún presupuesto a la seguridad digital, se observó que **la mediana del presupuesto de la seguridad digital en relación al presupuesto de inversión fue aproximadamente 0,05% de las inversiones en 2016**. Además, se verificó que, en promedio simple, la mayor parte del presupuesto fue asignado para plataformas y medios tecnológicos, mientras generación de capacidades recibió la menor cantidad de recursos.

Aproximadamente 46% del presupuesto de seguridad digital fue asignado a plataformas y medios electrónicos, y 9% a generación de capacidades que, a su vez, incluye temas como capacitación y concientización.

CUADRO 6: ASIGNACIÓN DEL PRESUPUESTO PARA LA SEGURIDAD DIGITAL POR ENTIDAD QUE ASIGNARON RECURSOS A TI (2016)

CATEGORÍA	PORCENTAJE
Recursos Humanos (ej. empleados, contratistas)	30 %
Plataformas y Medios Tecnológicos (ej. hardware, software)	46 %
Generación de Capacidades (ej. capacitación, concientización, investigación)	9 %
Servicios Especializados (ej. gestión de seguridad, externalización, soporte)	15 %

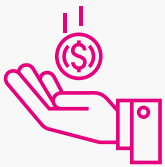
Número de observaciones: 327

Finalmente, se realizó una regresión lineal con el objetivo de identificar los factores que llevan a una entidad estatal a invertir más en seguridad digital. Se realizó una regresión lineal en la cual el logaritmo del presupuesto asignado por las entidades para asuntos de seguridad digital durante el año de 2016 fue la variable dependiente (Anexo 3). Se optó por el logaritmo del presupuesto para la seguridad digital, con vistas a normalizar la distribución de la variable. Además, se incluyeron las siguientes variables independientes: (i) el número de personal; (ii) el porcentaje aproximado de personal de la entidad que tiene acceso a Internet para desarrollar sus actividades profesionales; (iii) el logaritmo del presupuesto de inversión; y (iv) el logaritmo del número de incidentes digitales sufridos por la entidad pública en 2016.

Además, el modelo cuenta con variables dicotómicas que identifican el orden al cual pertenece la entidad pública, tal como nacional, territorial departamental y territorial municipal. Igualmente se incluyen las siguientes variables dicotómicas: (i) si la entidad tiene un área, cargo(s) o rol(es) dedicado(s) a la seguridad digital; (ii) si la entidad implementa medidas técnicas de seguridad (por ejemplo, pruebas de vulnerabilidad, mantenimiento de la infraestructura de TI); (iii) si la entidad adopta políticas de seguridad digital (por ejemplo, política de acceso al sistema, política de actualización de contraseñas, concientización); (iv) si la entidad implementa estándares (por ejemplo, ISO 27001, otros estándares internacionales); (v) si la entidad hace alguna evaluación de riesgo cibernético; y (vi) si la entidad conoce

alguna reglamentación y/o legislación nacional o territorial que requiera que las entidades pública implementen prácticas de gestión de riesgo cibernético.

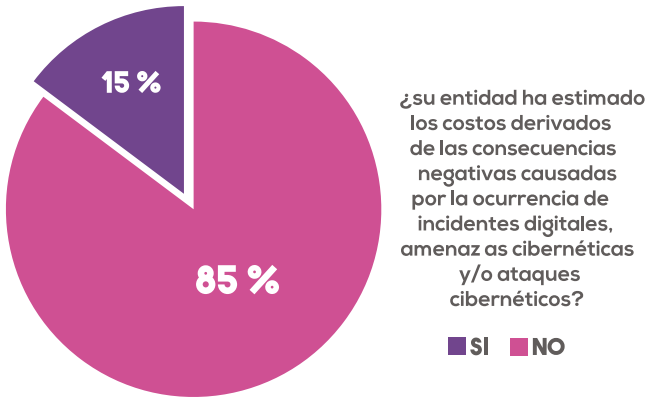
Los resultados indican que hay una relación positiva y estadísticamente significativa entre el número de personal, personal con acceso a Internet, presupuesto de inversión de la entidad estatal y el presupuesto para la seguridad digital. Con respecto a prácticas de seguridad digital, igualmente se verificó una relación significativa y positiva entre el presupuesto para la seguridad digital y las siguientes variables dicotómicas: existencia de un área, cargo(s) o rol(es) dedicado(s) a la seguridad digital, implementación de medidas técnicas e implementación de estándares. En otras palabras, las entidades públicas que implementan estas prácticas de seguridad digital asignan un presupuesto más grande para la seguridad digital que las entidades que no adoptan estas prácticas. Finalmente, cabe destacar la relación positivamente significativa entre las entidades que pertenecen al orden nacional y el presupuesto para la seguridad digital. En otras palabras, las entidades públicas nacionales tienen presupuestos para la seguridad digital más grandes.



COSTO DE LOS INCIDENTES DIGITALES PARA LAS ENTIDADES

Cuando se realizó la pregunta sobre la estimación de los costos derivados de las consecuencias negativas causadas por la ocurrencia de incidentes digitales, el 85% de las entidades estatales afirmaron que no hacen ninguna estimación, como se observa en el Gráfico 40 a continuación:

GRÁFICO 40: ENTIDADES QUE ESTIMARON LAS CONSECUENCIAS NEGATIVAS DE LOS INCIDENTES DIGITALES (2016)

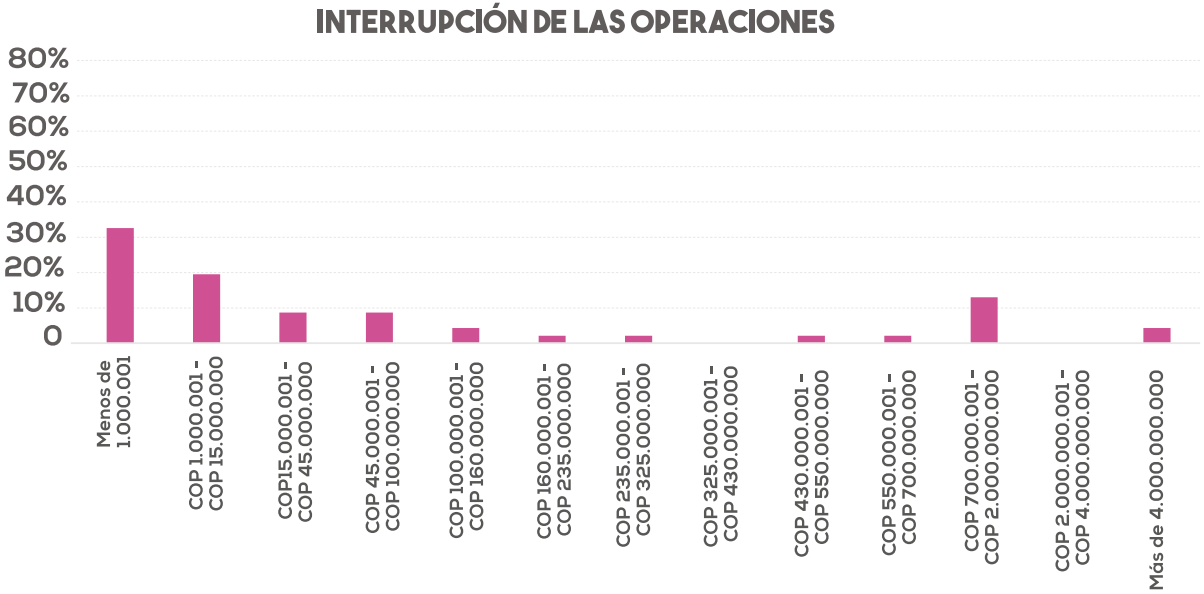


Número de observaciones: 474

Teniendo en cuenta las entidades que estimaron los costos incurridos como resultado de los incidentes digitales, los gráficos a continuación presentan la distribución de los costos con incidentes digitales incurridos en 2016 por las

entidades estatales según cinco categorías de costos: (i) interrupción de las operaciones normales de la empresa; (ii) daño a activos e infraestructura; (iii) sanciones, multas y gastos legales; (iv) daño a la reputación y la imagen; y (v) pérdida de la propiedad intelectual o de otra información sensible.

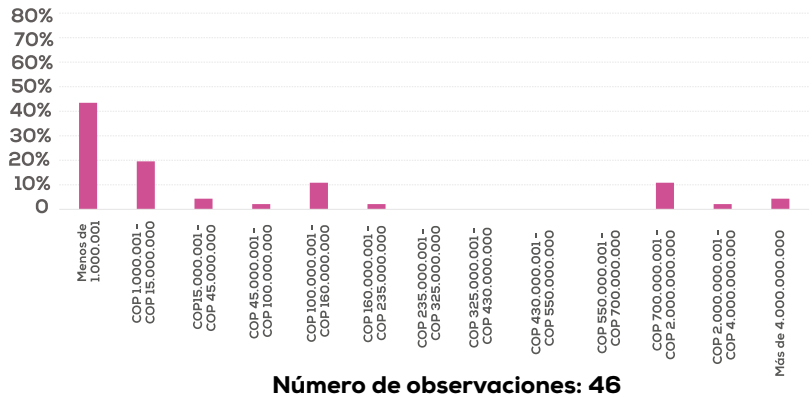
GRÁFICO 41: COSTOS DE INTERRUPCIÓN DE LA INFORMACIÓN INCURRIDOS POR LAS ENTIDADES ESTATALES QUE ESTIMARON EL IMPACTO DE LOS INCIDENTES DIGITALES (2016)



Número de observaciones: 46

Con respecto al costo de interrupción de las operaciones normales de las entidades estatales, 33% de las entidades tuvieron un costo más pequeño que COP $ 1.000.001, 20% tuvieron un costo entre COP $ 1.000.001 COP $ 15.000.000, y aproximadamente 24% entre COP $ 15.000.001 - COP $ 235.000.000. Hay algunas entidades con valores extremos que se alejan del conjunto de datos, llegando a más de 4 mil millones de pesos colombianos.

GRÁFICO 42: COSTOS DE DAÑOS A LOS ACTIVOS E INFRAESTRUCTURA INCURRIDOS POR LAS ENTIDADES ESTATALES QUE ESTIMARON EL IMPACTO DE LOS INCIDENTES DIGITALES (2016)



Número de observaciones: 46

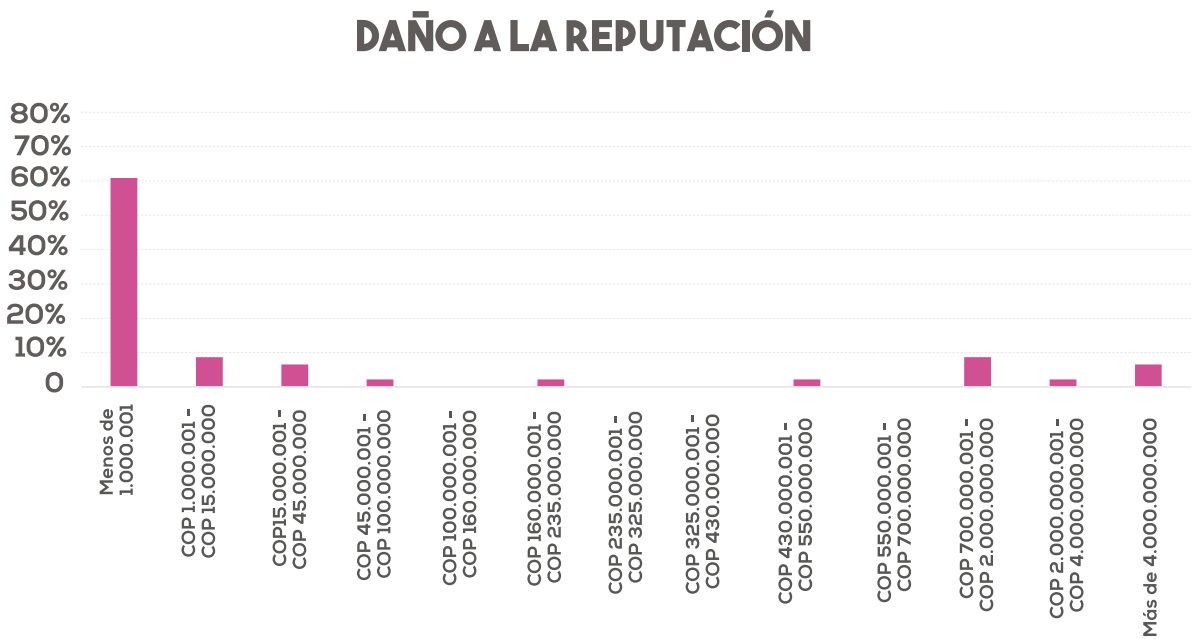
Con respecto al daño a los activos e infraestructura de la entidad, más de 40% de las entidades tuvieron un costo más pequeño que COP $ 1.000.001, 20% tuvieron un costo entre COP $ 1.000.001 – COP $ 15.000.000, y aproximadamente 20% entre COP $ 15.000.001 – COP $ 235.000.000. Sin embargo, cerca de 17% de las entidades presentaron costos relativos a daño a activos de más de 700 millones de pesos colombianos en 2016.

GRÁFICO 43: COSTOS DE SANCIONES, MULTAS Y GASTOS LEGALES INCURRIDOS POR LAS ENTIDADES ESTATALES QUE ESTIMARON EL IMPACTO DE LOS INCIDENTES DIGITALES (2016)

Número de observaciones: 46

Con respecto a sanciones, multas y gastos legales, 65% de las entidades tuvieron un costo más pequeño que COP $ 1.000.001, aproximadamente 13% tienen un costo entre COP $ 1.000.001 – COP $ 15.000.000, y aproximadamente 10% entre COP $ 15.000.001 – COP $ 235.000.000. Cerca del 11% de las entidades tuvieron costos más altas que 700 millones de pesos colombianos, con algunas entidades territoriales departamentales presentando un costo más grande que 4 mil millones de pesos colombianos.

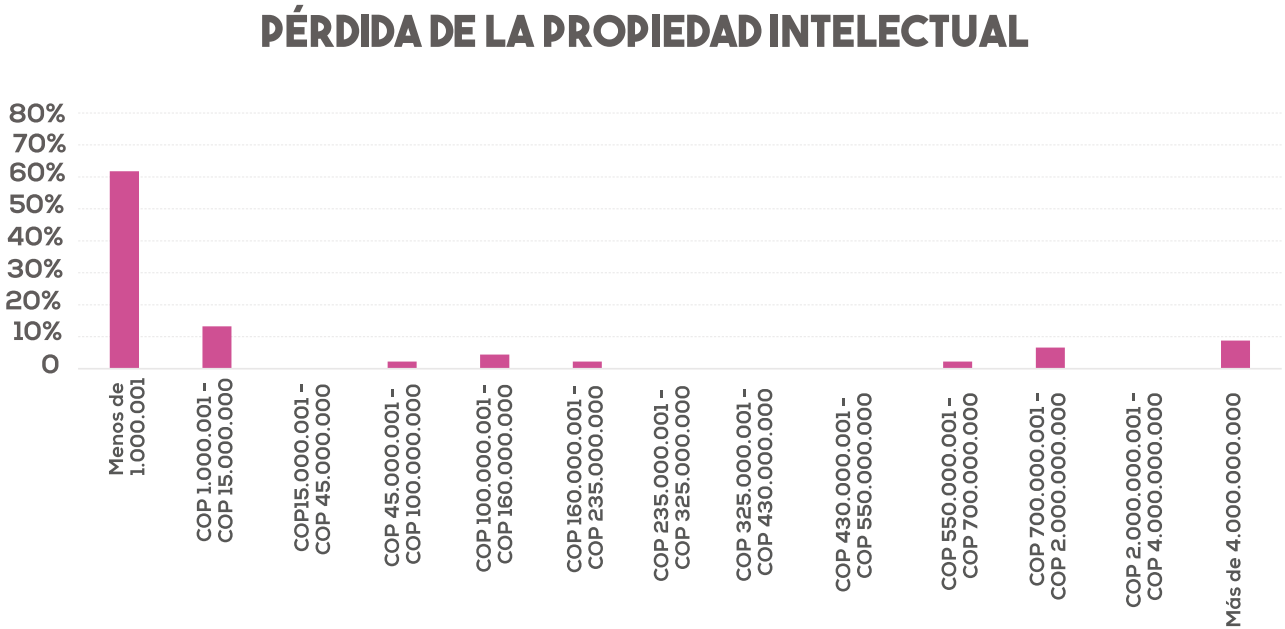
GRÁFICO 44: COSTOS DE DAÑO A LA REPUTACIÓN INCURRIDOS POR LAS ENTIDADES ESTATALES QUE ESTIMARON EL IMPACTO DE LOS INCIDENTES DIGITALES (2016)



Número de observaciones: 46

Con respecto a daños a la reputación, aproximadamente 60% de las entidades tuvieron un costo más pequeño que COP $ 1.000.001 en 2016, aproximadamente el 9% tienen un costo entre COP $ 1.000.001 – COP $ 15.000.000, y aproximadamente 11 % entre COP $ 15.000.001 – COP $ 235.000.000. Por otro lado, es interesante notar que 17% de las entidades presentaron un costo más alto que 700 millones de pesos colombianos.

GRÁFICO 45: COSTOS DE PÉRDIDA A LA PROPIEDAD INTELECTUAL Y DE INFORMACIÓN SENSIBLE INCURRIDOS POR LAS ENTIDADES ESTATALES QUE ESTIMARON EL IMPACTO DE LOS INCIDENTES DIGITALES (2016)



Número de observaciones: 46

Finalmente, con respecto a la pérdida de propiedad intelectual y de información sensible, 61% de las entidades tuvieron un costo más pequeño que COP $ 1.000.001, aproximadamente 13% entre COP $ 1.000.001 – COP $ 15.000.000, y aproximadamente 9% entre COP $ 15.000.001 – COP $ 235.000.000. Por otro lado, se observa que 15% presentaron costos más altos que 700 millones de pesos colombianos, y algunas más de COP $ 4.000.000.000: 9% de las entidades.

Se nota que la distribución del costo entre las cinco categorías es sesgada a la derecha, así que se prefirió trabajar con la mediana del costo agrupado incurrido. En relación a las entidades estatales nacionales, el intervalo del costo es 20 – 40 millones de pesos colombianos, representando aproximadamente menos del 0,5% de la inversión de las entidades. Las entidades nacionales que proporcionaron los datos de costo pertenecen, en su mayoría, a la rama ejecutiva o son entes autónomos. En este contexto, se debe tener en cuenta que estos datos reflejan la situación de entidades públicas con estas características. Además, no hubo un número significativo de entidades territoriales que respondieran la información acerca del costo.

Finalmente, se buscó analizar cómo los costos incurrido debido a incidentes digitales en 2016 impactaron las inversiones de las entidades estatales en investigación, desarrollo e innovación (I+D+i). Como se muestra en el Gráfico 46 a continuación, entre las entidades estatales entrevistadas, 48% afirmó que han aumentado sus inversiones en I+D+i.

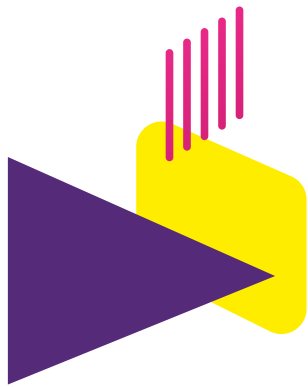
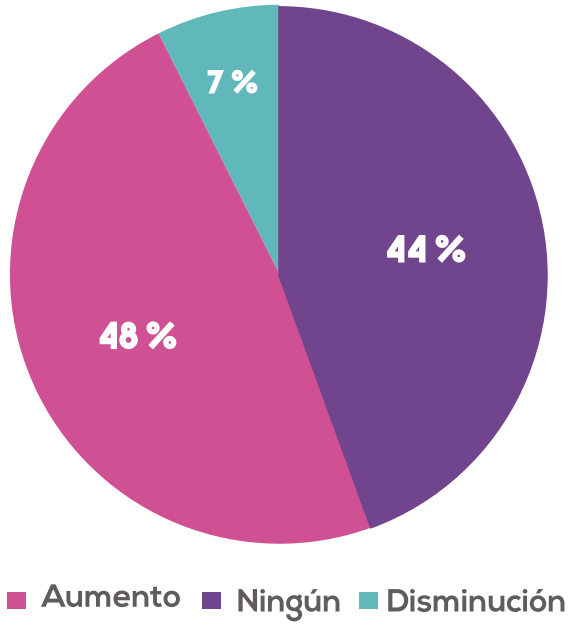


GRÁFICO 46: INVERSIÓN EN I+D+I DE LAS ENTIDADES QUE ESTIMARON EL IMPACTO DE LOS INCIDENTES DIGITALES (2016)

¿CÓMO CAMBIARON LAS INVERSIONES DE SU ENTIDAD EN MATERIA DE INVESTIGACIÓN, DESARROLLO E INNOVACIÓN (I+D+I) COMO RESULTADO DE LOS INCIDENTES DIGITALES QUE SUFRIÓ?



Número de observaciones: 46

Entre las entidades que afirmaron que sus inversiones en I+D+i aumentaron como resultado de incidentes digitales, 46% de estas entidades respondieron que sus inversiones aumentaron en más de 15% en 2016. Cabe destacar que estas entidades son en su mayoría nacionales que pertenecen a la rama ejecutiva, o consistían en entes autónomos u organismos de control y vigilancia.

ANEXO 1

ANÁLISIS SITUACIONAL

GENERALIDADES DE LA SEGURIDAD CIBERNÉTICA EN COLOMBIA

En 2011, el Gobierno de Colombia, a través del Consejo Nacional de Política Económica y Social (CONPES), estableció los Lineamientos de política para ciberseguridad y ciberdefensa, Documento CONPES 3701, bajo los auspicios del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), el Ministerio de Defensa Nacional, el Departamento Nacional de Planeación (DNP) y otras instituciones nacionales clave. Esta estrategia se centró en el establecimiento de instituciones nacionales necesarias para el desarrollo de la capacidad cibernética en Colombia.

En el año 2014 se produjo un importante desarrollo en el sentido que el Gobierno nacional llevó a cabo una revisión a fondo del Documento CONPES 3701 y solicitó apoyo internacional en la revisión y el desarrollo de una nueva estrategia de seguridad nacional digital. En abril de 2016, se aprobó la nueva Política Nacional de Seguridad Digital, CONPES 3854 que articula una visión estratégica en la que se alienta a los colombianos a hacer un uso responsable del entorno digital y fortalecer sus capacidades para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital. Este nuevo Documento CONPES 3854 ahondó en los éxitos de su predecesor y se concentró en promover y asegurar una Colombia digital.

En el marco de la seguridad digital basada en la gestión de riesgos, el Documento CONPES 3854 promueve la participación de múltiples actores, especialmente en las funciones transversales. Como resultado directo, Colombia es el primer país de América Latina y uno de los primeros en el mundo en incorporar plenamente las recomendaciones y mejores prácticas internacionales en materia de gestión de riesgos y seguridad digital emitidas recientemente por la Organización para la Cooperación y el Desarrollo Económicos (OCDE).

GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL PARA LA PROSPERIDAD DE LA OCDE – RECOMENDACIONES SOCIALES Y ECONÓMICAS

La OCDE realiza la promoción de políticas e instrumentos para la innovación y la confianza en la economía digital y la

expedición de las recomendaciones sobre la gestión de riesgos de seguridad digital para la prosperidad económica y social (2015), y proporciona orientaciones para el desarrollo de estrategias nacionales basadas en la gestión de riesgos de seguridad digital y la optimización de los beneficios económicos y sociales derivados de la apertura digital. Las recomendaciones de la OCDE incluyen la promoción de los principios generales sobre el conocimiento, las habilidades y la capacitación, la responsabilidad, los derechos humanos y los valores fundamentales, cooperación, evaluación de riesgos y ciclo de tratamiento, medidas de seguridad, de innovación y de preparación y continuidad. Estas recomendaciones guiadas se incorporaron en varios aspectos del proceso de desarrollo y el contenido del Documento CONPES 3854. Como tal, en la revisión de los progresos realizados en la aplicación de dicha política nacional bajo el análisis de la situación, se tendrían en cuenta las observaciones sobre la alineación de las políticas públicas con la recomendación de la OCDE.

El proceso de adhesión a la OCDE ha sido descrito como de impacto positivo en el proceso de elaboración de políticas públicas de Colombia[10]. En mayo de 2013, Colombia fue invitada a iniciar el proceso formal de adhesión a la OCDE. La invitación incluía una hoja de ruta[11]. Colombia tendría que demostrar ante 23 comités técnicos de la OCDE que ha hecho reformas significativas en el cumplimiento de las normas de la OCDE, dado que estos comités tendrían que presentar conceptos formales sobre la adhesión de Colombia al Consejo.

En el ***Economic Outlook*** de la OCDE[12], Tomo 2016, Número 1, la OCDE concluyó, en general, que las políticas macroeconómicas [en Colombia] eran apropiadas, pero se necesitaban reformas estructurales para aumentar la productividad. A pesar del impacto que ha tenido la volatilidad del mercado financiero mundial y la disminución de los precios del petróleo, la OCDE preveía que, con llevar el proceso de paz a buen término, se podría mejorar la confianza de las empresas y las entradas de capital. Además del proceso de adhesión a la OCDE, Colombia participa en labor de fondo de muchos de los comités especializados de la organización.

10 Why Good Policy-Making Matters: The Accession Case of Colombia to the OECD Source: *https://www.hertie-school.org/the-governance-post/2016/03/why-good-policy-making-matters-the-accession-case-of-colombia-to-the-oecd/-* Consultado Agosto 25, 2016

11 *http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=C(2013)110/FINAL&docLanguage=En*

12 Última consulta el 8 de septiembre de 2016 en: Perfil de Colombia- *http://www.keepeek.com/Digital-Asset-Management/oecd/economics/oecd-economic-outlook-volume-2016-issue-1/colombia_eco_outlook-v2016-1-11-en#page1 Versión completa: http://www.oecd-ilibrary.org/economics/oecd-economic-outlook-volume-2016-issue-1/colombia_eco_outlook-v2016-1-11-en*

Es pertinente considerar el proceso de la OCDE cuando se examina el desarrollo e implementación de políticas públicas, incluyendo el Documento CONPES 3854, ya que toma en cuenta las recomendaciones de la OCDE para la gestión de riesgos de seguridad digital. Como parte de la OCDE, Colombia podría recibir estudio y evaluación constante de la eficacia de sus políticas. Este proceso de evaluación continua, que se conoce como revisión por pares, ha demostrado ser eficaz y útil, ya que expone a los programas de reforma a discusión por parte de buenos investigadores (personal de la OCDE), así como de expertos en formulación de políticas reales en el área específica (miembros de cada comité).[13]

IMPLEMENTACIÓN DEL DOCUMENTO CONPES 3854

El creciente uso del entorno digital en Colombia para desarrollar actividades económicas y sociales genera incertidumbres y riesgos inherentes a la seguridad digital que deben ser gestionados permanentemente. No hacerlo puede resultar en la materialización de amenazas o ataques cibernéticos, con efectos no deseados de tipo económico o social para el país, y afecta la integridad de los ciudadanos en este entorno.

El enfoque de la política de seguridad cibernética y ciberdefensa hasta el año 2015 se había concentrado en contrarrestar el incremento de las amenazas cibernéticas bajo los objetivos de (i) defensa del país; y (ii) lucha contra el delito cibernético. Si bien, dicho enfoque de política había posicionado a Colombia como uno de los líderes en la materia a nivel regional, también había dejado de lado la gestión del riesgo en el entorno digital. El enfoque, esencial en un contexto de incremento en el uso de las TIC para realizar actividades económicas y sociales, ha traído consigo nuevas y más sofisticadas formas de afectar el desarrollo normal de estas en el entorno digital. Este hecho demanda una mayor planificación, prevención y atención por parte de los países.

Teniendo en cuenta lo anterior, se identificó la siguiente problemática en el país: (i) no se cuenta con una visión estratégica en seguridad digital basada en la gestión de riesgos; (ii) las múltiples partes interesadas no maximizan sus oportunidades al desarrollar actividades socioeconómicas en el entorno digital; (iii) se requiere reforzar las capacidades de seguridad cibernética con un enfoque de gestión de riesgos de seguridad digital; (iv) se necesita reforzar las capacidades de ciberdefensa con un enfoque de gestión de riesgos de seguridad digital; y (v) los esfuerzos de cooperación, colaboración y asistencia, nacional e internacional, relacionados con

13 Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document. Consultada el 8 de septiembre de 2016. Disponible en: *http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf*

la seguridad digital no son suficientes y requieren ser articulados.

Con el fin de atender dicha problemática y acoger mejores prácticas internacionales, el Gobierno de Colombia expidió la ***Política Nacional de Seguridad Digital*** (Documento CONPES 3854 de 2016) en el mes de abril de 2016, liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones y el Ministerio de Defensa Nacional de Colombia. Esta política pública tiene como objetivo principal el fortalecimiento de las capacidades de todas las partes interesadas (Gobierno nacional y los territoriales, las organizaciones públicas y privadas, la Fuerza Pública, los propietarios u operadores de las infraestructuras críticas cibernéticas nacionales, la academia y la sociedad civil) para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, bajo un marco de cooperación, colaboración y asistencia a nivel nacional e internacional, con el fin de contribuir al crecimiento de la economía digital nacional y maximizar los beneficios obtenidos de una mayor prosperidad económica, política y social del país.

La expedición de esta nueva política pública fue el resultado de un proceso de participación entre representantes de las múltiples partes interesadas del país y es una de las primeras políticas nacionales en el mundo y primera en la región de Latinoamérica en acoger las recomendaciones en gestión de riesgos de seguridad digital, emitidas en el mes de septiembre de 2015 por la Organización para la Cooperación y el Desarrollo Económicos -OECD-. Se tuvieron en cuenta los aportes realizados por los representantes del las Empresas, el Gobierno nacional, la sociedad civil, los operadores de infraestructuras críticas nacionales y la academia. Asimismo, se incorporaron las recomendaciones de otros organismos internacionales como la Organización de Estados Americanos -OEA-, la Unión Internacional de Telecomunicaciones -UIT- y la Organización del Tratado del Atlántico Norte -OTAN.

La ***Política Nacional de Seguridad Digital*** de Colombia: i) diferencia claramente los objetivos de prosperidad económica y social con los objetivos de defensa del país y de lucha contra el crimen y la delincuencia en el entorno digital, ii) incluye componentes como la gobernanza, la educación, la regulación, la cooperación internacional y nacional, la investigación y desarrollo, y la innovación, y iii) cambia el enfoque tradicional al incluir la gestión de riesgo como uno de los elementos más importantes para abordar la seguridad digital. Esto lo hace bajo cuatro (4) principios fundamentales enfocándose en la salvaguarda de los derechos humanos y los valores fundamentales de los ciudadanos

en Colombia, involucrando activamente a todas las partes interesadas, y asegurando una responsabilidad compartida entre las mismas. Estos principios se reflejan en cinco (5) dimensiones en las que actuará esta política, las cuales determinan las estrategias para alcanzar su objetivo principal.

Finalmente, durante el año 2017 se construirá en Colombia, en conjunto con las múltiples partes interesadas, una ***Agenda Nacional de Seguridad Digital*** con el fin de priorizar los intereses nacionales en torno al tema, identificando variables de impacto (por ejemplo, pérdidas económicas, afectación de personas, consecuencias medioambientales o correlación de la afectación con otras partes), bajo el marco de los principios fundamentales de la ***Política Nacional de Seguridad Digital***. También se prevé la generación de lo siguiente:

1. Documentos estratégicos para la implementación de la política: Mecanismos de Coordinación entre las múltiples partes interesadas, Agenda Estratégica Internacional de cooperación, colaboración y asistencia y Agenda Estratégica Nacional de cooperación, colaboración y asistencia nacional
2. Planes de fortalecimiento de las capacidades institucionales, operativas, administrativas, humanas y de infraestructura física y tecnológica de las instancias actuales.
3. Estudios de viabilización técnica para la creación de nuevas instancias o proyectos de seguridad cibernética y ciberdefensa.
4. Contenidos educativos especializados para capacitar a los funcionarios responsables de la seguridad digital en Colombia.
5. Contenidos educativos complementarios relacionados con la gestión de riesgos de seguridad digital dirigidos a estudiantes de Educación Básica, Media y Superior así como a docentes.

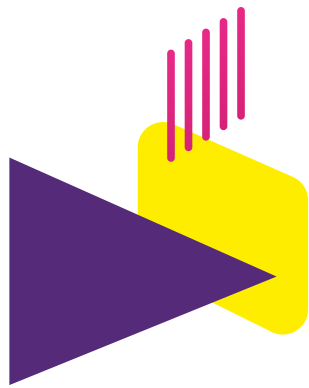
AVANCES EN LA MODELO DE MADUREZ DE CAPACIDAD DE CIBERSEGURIDAD NACIONAL

El Modelo de Madurez de Capacidad (CMM por las siglas en inglés) de Seguridad Cibernética Nacional desarrollado por el Centro Global de Capacitación de Seguridad Cibernética de la Universidad de Oxford fue la base para el ***Informe de Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?.*** Este modelo evalúa la madurez de la seguridad cibernética de un país en 5 dimensiones principales: (1) Política y Estrategia; (2) Cultura y Sociedad; (3) Educación; (4) Marcos legales; y (5) Tecnologías. En este informe se incluyó un perfil de país para Colombia, que muestra un alto nivel de madurez de capacidad de seguridad cibernética en el país según lo evaluado.

Colombia es el primer país que ha llevado a cabo una evaluación de las mejoras efectuadas en relación con la primera evaluación del CMM. Como tal, el análisis a continuación proporciona una comparación paralela de los avances logrados a partir de la aprobación e implementación del Documento CONPES 3854 desde su expedición en el mes de abril de 2016.

En general, la mayoría de los indicadores han experimentado mejoras con un movimiento significativo en la Dimensión 1. Se observó durante este período, que la implementación del Documento CONPES 3854 de 2016 le permitió a Colombia experimentar un nivel de madurez significativo en cuanto a la participación de los actores interesados, la coordinación con políticas nacionales de desarrollo y la incorporación de Gestión de riesgos como parte del marco de aplicación.

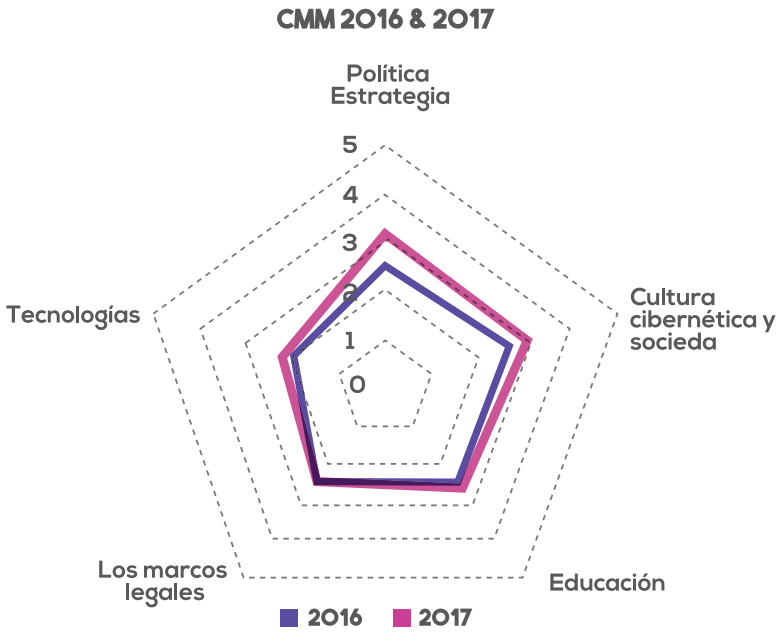
Además, las dimensiones 2 (Cultura y Sociedad) y 3 (Educación) también tuvieron una mejora notable en el último año.



Colombia


2016
2017
Política y estrategia
Estrategia nacional de seguridad cibernética oficial o documentada
Desarrollo de la estrategia
Organización
Contenido
Defensa cibernética
Estrategia
Organización
Coordinación
Cultura y sociedad
Mentalidad de seguridad cibernética
En el gobierno
En el sector privado
En la sociedad
Conciencia de seguridad cibernética
Sensibilización
Confianza en el uso de Internet
En los servicios en línea
En el gobierno electrónico
En el comercio electrónico
Privacidad en línea
Normas de privacidad
Privacidad del empleado
Educación
Disponibilidad nacional de la educación y formación cibernéticas
Educación
Formación
Desarrollo nacional de la educación de seguridad cibernética
Desarrollo nacional de la educación de seguridad cibernética
Formación e iniciativas educativas públicas y privadas
Capacitación de empleados en seguridad cibernética
Gobernanza corporativa, conocimiento y normas
Comprensión de la seguridad cibernética por parte de empresas privadas y estatales
2016
2017
Marcos legales
Marcos jurídicos de seguridad cibernética
Para la seguridad de las TIC
Privacidad, protección de datos y otros derechos humanos
Derecho sustantivo de delincuencia cibernética
Derecho procesal de delincuencia cibernética
Investigación jurídica
Cumplimiento de la ley
La fiscalía
Tribunales
Divulgación responsable de la información
Divulgación responsable de la información
Tecnologías
Adhesión a las normas
Aplicación de las normas y prácticas mínimas aceptables
Adquisiciones
Desarrollo de software
Organizaciones de coordinación de seguridad cibernética
Centro de mando y control
Capacidad de respuesta a incidentes
Respuesta a incidentes
Identificación y designación
Organización
Coordinación
Resiliencia de la infraestructura nacional
Infraestructura tecnológica
Resiliencia nacional
Protección de la Infraestructura Crítica Nacional (ICN)
Identificación
Organización
Planeación de respuesta
Coordinación
Gestión de riesgos
Gestión de crisis
Planeación
Evaluación
Redundancia digital
Planeación
Organización
Mercado de la ciberseguridad
Tecnologías de seguridad cibernética
Seguros de delincuencia cibernética

GRÁFICO 47: COMPARATIVO DE LOS RESULTADOS DEL CMM (2016 Y 2017)



Dimensiones

En relación con la **Dimensión 1 (Política y Estrategia),** actualmente se implementa en Colombia la nueva ***Política Nacional de Seguridad Digital*** (Documento CONPES 3854 de 2016) que busca involucrar a las múltiples partes interesadas en la gestión del riesgo de seguridad digital, de tal forma que asuman la responsabilidad que les corresponde de acuerdo a su rol y función y participen activamente tanto en la fase de construcción de los elementos que se consignan en este documento, como en la implementación de la política. Para esto, el Coordinador Nacional de Seguridad Digital diseñará y pondrá en marcha durante el segundo semestre de 2017 un mecanismo dinámico de coordinación que define (i) los roles, las responsabilidades y las funciones de las múltiples partes interesadas; y (ii) una matriz de comunicación y seguimiento

entre el Coordinador Nacional de Seguridad Digital, la instancia de máximo nivel del Gobierno (Comisión Nacional Digital y de Información Estatal) y las múltiples partes interesadas, con el fin de abordar los temas de seguridad digital en Colombia.

La Política Nacional de Seguridad Digital incluye un Plan de Acción y Seguimiento -PAS- en el cual se incluyen todas las acciones que se implementarán con el fin de lograr tanto el objetivo general como los objetivos específicos de la Política. En específico, este PAS establece procesos de medición y métricas para cada acción como sigue: responsable de la ejecución, tiempo de la ejecución, importancia relativa de la acción, relación con otras acciones, indicadores de cumplimiento, costo de la acción, recursos financieros asignados para la acción y sus fuentes y seguimiento a la implementación mediante cortes anuales de avance. Este PAS es revisado periódicamente por el Departamento Nacional de Planeación -DNP- en conjunto con el Coordinador Nacional de Seguridad Digital con el fin de renovar, si es del caso, lo dispuesto en la Agenda Nacional de Seguridad Digital (instrumento para priorizar los intereses nacionales en torno al tema, identificando variables de impacto).

En el marco de estrategias y acciones establecidas en el PAS vale la pena resaltar que el Ministerio de Defensa Nacional realizará y participará en ejercicios de simulación y entrenamiento, nacionales e internacionales, que permitan desarrollar habilidades y destrezas para las múltiples partes interesadas responsables de las infraestructuras críticas cibernéticas nacionales y de la defensa nacional en el entorno digital, con el fin de fortalecer las capacidades de los responsables de garantizar la defensa nacional en el entorno digital.

En el marco de la Política Nacional de Seguridad Digital (Documento CONPES 3854 de 2016) se establece un marco institucional claro en torno a la seguridad digital en Colombia. Para esto, se crean las máximas instancias de coordinación y orientación superior en torno a la seguridad digital en el Gobierno nacional y se establecen figuras de enlace sectorial en todas las entidades de la rama ejecutiva a nivel nacional. En particular, se creó la figura de Coordinador Nacional de Seguridad Digital quien dirige la implementación de la política nacional de seguridad digital y hace el seguimiento continuo de la misma, en conjunto con el Departamento Nacional de Planeación.

Finalmente, el Coordinador Nacional de Seguridad Digital llevará a cabo la coordinación interinstitucional e intersectorial en todos los temas de seguridad digital en el país. Adicionalmente, en el largo plazo, se espera que se cree una Dirección de Seguridad Cibernética

y Defensa Cibernética, dependiente del Viceministerio de Defensa para las Políticas y Asuntos Internacionales, la cual se constituiría como un elemento relevante para implementar niveles de escalonamiento para el reporte de incidentes digitales y garantizar la participación de las múltiples partes interesadas en la gestión de riesgos de la seguridad digital. En el corto plazo, se comenzará por implementar el plan de fortalecimiento para el colCERT. Lo anterior permitirá desarrollar las capacidades necesarias para implementar un esquema de gobernabilidad participativa de múltiples partes interesadas, y definir los niveles de escalamiento para el reporte de incidentes digitales.

En relación de **Dimensión 2 (Cultura y Sociedad),** actualmente, se diseña un modelo de gestión de riesgos de seguridad digital y se generarán los mecanismos administrativos para que todas las entidades y departamentos administrativos de la rama ejecutiva lo adopten y lo implementen, de forma permanente. También se adelantan programas, proyectos y campañas de concientización y sensibilización, así como capacitaciones, jornadas de intercambio y transferencia respecto de las mejores prácticas en seguridad digital a todas las múltiples partes interesadas. Se resaltan las acciones que se adelantan frente a las organizaciones públicas, en particular todas las entidades públicas del sector ejecutivo. De igual forma, se adelantan jornadas de sensibilización a entes territoriales.

El Gobierno nacional continúa implementando y fortaleciendo su estrategia de gobierno electrónico (***e-government***) llamada "Gobierno en línea", con el fin de construir un Estado más eficiente, más transparente y más participativo gracias a las Tecnologías de la Información y las Comunicaciones -TIC-. En el marco de dicha estrategia se adelantan actividades bajo los siguientes ejes temáticos: i) ***TIC para el Gobierno Abierto***: Busca construir un Estado más transparente y colaborativo, donde los ciudadanos participan activamente en la toma de decisiones gracias a las TIC, ii) ***TIC para servicios***: Busca crear los mejores trámites y servicios en línea para responder a las necesidades más apremiantes de los ciudadanos, iii) ***TIC para la gestión***: Busca darle un uso estratégico a la tecnología para hacer más eficaz la gestión administrativa, y iv) ***Seguridad y privacidad de la información***: Busca guardar los datos de los ciudadanos como un tesoro, garantizando la seguridad de la información.

La privacidad en línea también se está abordando. A tono con los principios recomendados por la OCDE y las recomendaciones de organismos como la OEA, la Política Nacional de Seguridad

Digital de Colombia se rige por cuatro principios fundamentes definidos de acuerdo al contexto nacional. Se salvaguardan los derechos humanos y los valores fundamentales de los ciudadanos en Colombia, involucrando activamente a todas las partes interesadas, y asegurando una responsabilidad compartida entre las mismas. Estos principios se reflejan en las dimensiones en las que esta política actúa, las cuales determinan las estrategias para alcanzar su objetivo principal.

El primer principio fundamental se estableció así: "***Salvaguardar los derechos humanos y los valores fundamentales de los ciudadanos en Colombia, incluyendo la libertad de expresión, el libre flujo de información, la confidencialidad de la información y las comunicaciones, la protección de la intimidad y los datos personales y la privacidad, así como los principios fundamentales consagrados en la Constitución Política de Colombia. En caso de limitación a estos derechos, debe ser bajo medidas excepcionales y estar conforme con la Constitución Política y los estándares internacionales aplicables. Estas medidas deben ser proporcionales, necesarias y estar enmarcadas en la legalidad."***

En relación de **Dimensión 3 (Educación),** Colombia ha avanzado significativamente en la generación de oferta académica especializada en seguridad digital. En el año 2011, Colombia contaba con doce programas académicos a nivel nacional, desde el nivel técnico hasta el de maestría, mientras que a la fecha cuenta con más de cincuenta programas y una amplia gama de cursos de educación informal, que incluyen certificaciones de reconocimiento internacional.

Adicionalmente, una de las funciones que se le otorgan al Coordinador Nacional de Seguridad Digital es garantizar que los programas, proyectos y campañas de concientización y sensibilización, así como las capacitaciones que adelanten las diferentes entidades, se diseñen a partir de los lineamientos y orientaciones que emita la Comisión Nacional Digital y de Información Estatal, con el fin de evitar la duplicación de esfuerzos y garantizar la eficiencia en el manejo de los recursos.

La política se dirige al Desarrollo nacional de la educación de seguridad cibernética y también plantea estrategias como el fortalecimiento de las instancias y entidades responsables de seguridad cibernética, evaluando la creación de nuevas instancias en las que se desarrolle formación, investigación e innovación, especialmente en relación con capacidades técnicas inherentes a la seguridad digital. Para garantizar la pertinencia de la creación de las nuevas instancias, el Ministerio de Defensa Nacional efectuará los estudios de viabilidad para la creación de un ***Centro***

de excelencia de seguridad digital, entre otros.

De igual manera, se fortalecerán las capacidades de los responsables de garantizar la defensa nacional en el entorno digital. El Ministerio de Defensa Nacional diseñará contenidos educativos especializados y capacitará a las múltiples partes interesadas responsables de garantizar la defensa nacional en el entorno digital. El mismo ministerio realizará y participará en ejercicios de simulación y entrenamiento, nacionales e internacionales, que permitan desarrollar habilidades y destrezas para las múltiples partes interesadas responsables de las infraestructuras críticas cibernéticas nacionales y la defensa nacional en el entorno digital. En estas actividades participarían las múltiples partes interesadas responsables de las infraestructuras críticas cibernéticas nacionales y la defensa nacional en el entorno digital.

Finalmente, teniendo en cuenta los antecedentes generados por la implementación de los lineamientos de seguridad cibernética y defensa cibernética en el país (Documento CONPES 3701 de 2011), actualmente los órganos de decisión de las empresas estatales y privadas en Colombia conocen que sus organizaciones pueden estar en riesgo y generalmente toman decisiones de inversión en medidas de seguridad de modo reactivo.

Además, en relación de **Dimensión 4 (Marcos legales),** mientras que el nivel de madurez se mantiene estable, la nueva Política Nacional de Seguridad Digital establece un conjunto de acciones orientadas a disponer el marco legal y regulatorio que soporta todos los aspectos necesarios para cumplir los objetivos de la política. Para este propósito, la política prevé que las diferentes instancias someterán a consideración del Ministerio de Justicia y del Derecho de Colombia las propuestas de ajuste y de nueva normativa que se requieran y este verificará la coherencia constitucional y legal. Igualmente, la Comisión de Regulación de Comunicaciones (CRC) ajustará en 2017 el marco regulatorio del sector TIC teniendo en cuenta asuntos necesarios para la gestión de riesgos de seguridad digital, como la protección de usuarios de comunicaciones o el régimen de calidad de las redes de telecomunicaciones.

El marco de delitos establecido en la Ley 1273 de 2009 se realizó considerando aspectos esenciales de la tipificación de delitos señalados en el Convenio sobre la Ciberdelincuencia (Convención de Budapest),, sin embargo, aún está en proceso el trámite legislativo requerido para lograr la adhesión a esta convención. Para este propósito, la política prevé que las diferentes instancias someterán a consideración del Ministerio de Justicia y del Derecho de Colombia las propuestas

de ajuste y de nueva normativa que se requieran. El país ha avanzado en su incorporación en redes de información relacionadas con delitos cibernéticos y de equipos de respuesta y, principalmente a través del Centro Cibernético Policial -CCP-, colabora activamente en procesos de investigación en esta materia.

Finalmente, en relación de **Dimensión 5 (Tecnologías),** la Política Nacional de Seguridad Digital establece acciones para las capacidades de gestión de riesgos de la seguridad digital, incluyendo adopción de buenas prácticas y estándares en todas las partes interesadas. La Resiliencia Nacional es muy importante. La construcción de la Política Nacional de Seguridad Digital aprobada el año pasado por el Gobierno de Colombia, así como espacios existentes como las Reuniones de Infraestructura Critica, Riesgo Operacional y defensa cibernética, han generado una dinámica de interacción entre el sector público y el privado. De hecho, las mesas específicamente dispuestas para trabajar en los temas de infraestructura crítica, lideradas por el sector Defensa del país hacen periódicamente (una vez al mes).

En el marco de las mesas de trabajo, se realizan charlas sobre las vulnerabilidades a las que están expuestos activos de información de las Infraestructuras críticas. No obstante, no se ha consolidado un protocolo o mecanismo que garantice el reporte periódico de vulnerabilidades ni el alcance que debería tener la presentación de informes. También se realizan charlas para sensibilizar a los operadores de Infraestructuras críticas sobre seguridad cibernética. Colombia cuenta con una oferta creciente de formación especializada en seguridad cibernética (cursos certificados e incluso existen programas de maestría) a la cual han accedido algunos de los operadores de Infraestructura Crítica Cibernética - ICC.

En relación al desarrollo de software, la nueva Política Nacional establece acciones para el fortalecimiento de las capacidades de gestión de riesgos de la seguridad digital en todas las partes interesadas. En particular, el Gobierno de Colombia está promoviendo el desarrollo de la industria de Tecnologías de Información y el emprendimiento digital a través de diferentes iniciativas. Algunas de ellas incluso promueven diplomados en seguridad para personal de las empresas, así como la financiación de diplomados en modelos de madurez ampliamente conocidos como CMMI.

En respecto de Seguros de delincuencia cibernética, en Colombia existen compañías de seguros que ofrecen pólizas de seguro (con amparos adicionales y opcionales) destinadas a empresas y personas naturales en órganos de decisión de las mismas, con el fin de: i) hacer

frente a la responsabilidad ***por el uso y el tratamiento de información*** (derivada de la protección de datos, la gestión y manejo de datos personales y las consecuencias de la pérdida de información corporativa) y ii) para hacer frente a la ***responsabilidad por la seguridad de datos*** (perjuicios y gastos de defensa asociados con contaminación de datos de terceros por un virus, denegación inadecuada o errónea de los derechos de acceso a los datos a un tercero autorizado, hurto de un código de acceso de las instalaciones de la empresa, un sistema informático, o de empleados, destrucción, modificación, corrupción, daño o eliminación de datos almacenados en cualquier sistema informático, hurto de hardware de la empresa, que contenga datos personales o corporativos o revelación de datos como consecuencia de una violación a la seguridad de datos).

ANÁLISIS FODA

Un análisis FODA (fortalezas, oportunidades, debilidades y amenazas) se aplicó a los datos recolectados hasta la fecha, como una forma de obtener una comprensión más profunda de la capacidad de seguridad cibernética en Colombia. Este análisis FODA tuvo en cuenta la investigación documental, la información recopilada durante las consultas con los actores interesados y los datos sobre Colombia públicamente disponibles, incluyendo sus realidades económicas y políticas, al igual que sus objetivos de desarrollo económico. Sin embargo, el análisis FODA no pretende llevar a cabo un amplio análisis nacional, sino que se centra en el impacto que ciertos factores externos pueden tener en la aplicación del Documento CONPES 3854, el desarrollo de nuevas iniciativas de seguridad cibernética y la mejora de la madurez de la seguridad cibernética de Colombia.

La aplicación de un análisis FODA de la capacidad de la seguridad cibernética a nivel nacional tiene en cuenta los factores internos, incluyendo los recursos y la experiencia disponible y bajo el control del país que podrían ser clasificados según sus fortalezas y debilidades. Por otro lado, también se identifican los factores externos (sin importar si están o no conectados directa o indirectamente), que pueden presentarse como oportunidades y amenazas. Algunas de las cuestiones examinadas fueron:

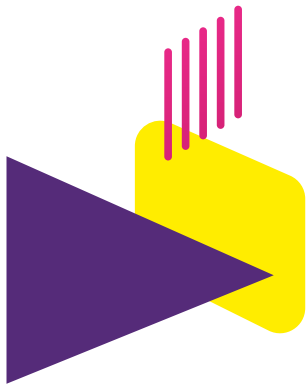
1. Fortalezas - Cuáles son los factores desde una perspectiva interna y desde el punto de vista de los actores externos, que hacen que el país sea fuerte en esa área.

2. Debilidades - Desde una base interna y externa, qué consideran los actores externos como debilidades percibidas que podrían evitarse o mejorarse.

3. Oportunidades - Con base en las fortalezas y debilidades identificadas, qué oportunidades se presentan y pueden estas oportunidades ayudar a reducir o eliminar las debilidades.

4. Amenazas - ¿Qué obstáculos y factores externos actuales están fuera del control del país y podrían amenazar su éxito? ¿Pueden las consideraciones económicas amenazar la posición de seguridad cibernética del país?

La ventaja del análisis FODA es que sus resultados puedan tenerse en cuenta en la planificación y ejecución permanente del CONPES 3854, ya que no solo identifica las amenazas y debilidades que afectan la eficacia de la estrategia de seguridad digital, sino también las oportunidades y fortalezas que puedan ser aprovechadas para alcanzar el éxito.



FODA

FORTALEZAS

Avances en la implementación del CONPES 3854 de 2016 – Política Nacional de Seguridad Digital

Designación de coordinador nacional en Presidencia de la República

Presupuesto específico para la seguridad cibernética priorizado mediante CONPES

ColCert

Capacidades cibernéticas del Ministerio de Defensa

Capacidad Técnica del MinTIC

Normatividad especializada (ej. Delitos informáticos, protección de datos personales, etc.)

OPORTUNIDADES

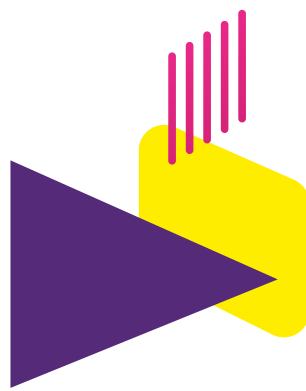
- Seguimiento de alto nivel en la implementación CONPES
- Nuevos programas de educación (como la Maestría en Seguridad Cibernética)
- La implementación de los acuerdos de paz
- Programas de becas e iniciativas de co-pago de MinTIC
- Proceso de adhesión a la OCDE
- Inversión en infraestructura y educación
- Mayor nivel de conciencia en Seguridad Digital
- Nuevo modelo para participación de toda las partes interesadas

DEBILIDADES

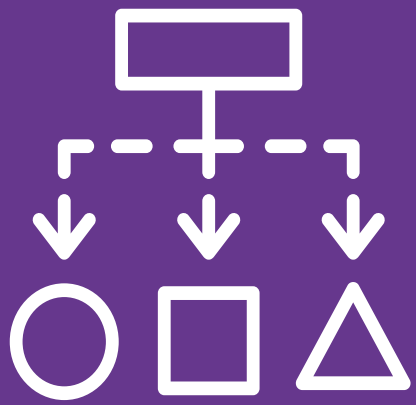
- Depreciación del valor del Peso
- Reducción de los presupuestos ministeriales en todas las áreas
- Insuficiente capacidad en jueces y fiscales en aspectos de seguridad digital

AMENAZAS

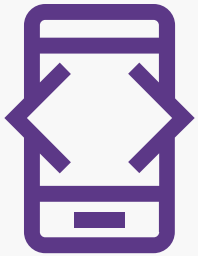
- Disminución del crecimiento económico en el PBI
- Cambios en liderazgo desde el Gobierno
- Demoras en la aprobación legislativa para la adhesión de Colombia al convenio de Budapest



ANEXO 2



METODOLOGÍA



DESARROLLO DEL INSTRUMENTO

Para reunir información sobre los diversos incidentes digitales, se desarrollaron dos (2) tipos de instrumentos para el siguiente análisis: 1) Análisis Situacional (estilo de la entrevista); y 2) Análisis del impacto (en línea).

El proceso de desarrollo inició con la investigación y revisión de diversos estudios públicamente disponibles e informes sobre seguridad cibernética y el análisis del impacto de la delincuencia cibernética. Aunque se revisaron varios documentos, no se intentó resumir las postulaciones de esos estudios. En general, se concluyó que la mayoría de los estudios disponibles se centraban en la estimación general del impacto económico de la delincuencia cibernética y, en menor medida, en los incidentes cibernéticos. Estos estudios se realizaron tanto a nivel transnacional con varios países involucrados como a nivel nacional, pero con una pequeña muestra de las diversas industrias.

El instrumento fue desarrollado durante un período de seis meses e involucró varias etapas. La Etapa Piloto fue uno de los hitos significativos del Proyecto ya que se les solicitó a las entidades participantes que aplicaran el instrumento a sus entidades/instituciones en el contexto de probar la aplicabilidad de los términos y definiciones utilizados, la comprensión de las preguntas formuladas y la usabilidad y lógica del instrumento en línea.

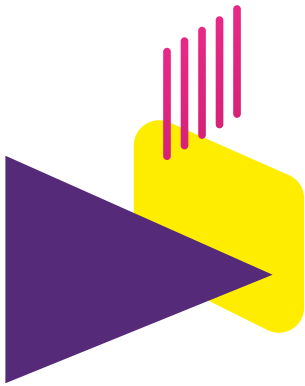
Con respecto al Análisis Situacional (Anexo 1), se utilizaron como punto de referencia los resultados de la herramienta de aplicación desarrollada por la OEA, el BID y el Centro Global de Capacitación de Seguridad Cibernética de la Universidad de Oxford, resumidos en el informe ***"Ciberseguridad: Estamos preparados en América Latina y el Caribe?"***, para elaborar un cuestionario que fue diligenciado por las partes interesadas pertinentes del Gobierno nacional en torno a cinco áreas principales: 1) Política y Estrategia; (2) Cultura y Sociedad; (3) Educación; (4) Marcos Legales; y (5) Tecnologías. Las respuestas facilitaron el análisis de las principales fortalezas, oportunidades, debilidades y amenazas (análisis FODA) para el país en términos de desarrollo de sus capacidades en seguridad digital, así como una actualización de las diversas dimensiones e indicadores.

ANÁLISIS DE LAS RESPUESTAS

Con el análisis de las respuestas de las entidades del sector público y privado que participaron en el instrumento en Colombia, este Estudio proporciona a nivel macro un resumen de la estimación de costos relacionados con los incidentes cibernéticos y las posibles pérdidas incurridas. Hubo varios factores y limitaciones que tuvieron que ser tomados en cuenta. Muchas empresas, por ejemplo, ocultan sus pérdidas mientras que otras no poseen las habilidades para identificar sus pérdidas. Adicionalmente, en la metodología de recopilación de datos, a saber, el uso de un instrumento, algunos de los resultados pueden no ser precisos, ya que se usaron rangos para las estimaciones de valor, los entrevistados seleccionaron los resultados y algunas de las respuestas se basaron en una percepción de sí mismo, que algunos entrevistados pueden distorsionar. Por lo tanto, el análisis de este estudio consideró y tuvo en cuenta varios factores al derivar sus conclusiones:

1) varios sectores económicos que están incluidos; 2) tamaño de los sectores; 3) número de entrevistados; 4) variación entre los entrevistados que diligenciaron el instrumento por completo y aquellos que no lo completaron; y 5) factores de control, tales como 'sí'/'no' para asegurar que se medían manzanas con manzanas.

Un total de 1.606 organizaciones comenzaron el instrumento, pero solamente un total de **1.098 entrevistados** (515 Empresas y 583 Entidades del sector público) completaron la sección del perfil. En la respuesta a cómo supieron sobre el instrumento, el 37% respondió que fue a través de una carta oficial del Gobierno nacional, el 24% indicó que fue a través de un sitio web del Gobierno nacional y el 23% dijo que era otro sitio web. Se observó que el 16% fue informado como resultado de la divulgación que se llevó a cabo con las asociaciones de la industria y gremios. No se estableció ninguna cuota por industria y tamaño de la empresa (ingresos), sino un margen razonable, y se obtuvieron respuestas representativas de empresas de distintos tamaños y sectores económicos.



ANEXO 3

ANÁLISIS ESTADISTICO COMPLEMENTARIO

CUADRO 7: ESTIMACIÓN DE LA PROBABILIDAD QUE UNA EMPRESA IDENTIFIQUE LOS INCIDENTES DIGITALES (2016)

Modelo de estimación: logit

Variable dependiente: 1 si la empresa identifica incidentes digitales, 0 si no los identifica.

VARIABLES	EFECTO MARGINAL (DY/DX)*	ERROR ESTÁNDAR	Z	P > IZI	$\bar{x}$
Presupuesto para seguridad digital	1.,2e-10	9,01E-11	1,24	0,215	1,47E+08
Número de empleados	0,0003791	0,0001581	2,40	0,017**	150,0771
Personal con acceso a Internet	-0,000852	0,0010589	-0,80	0,421	64,31776
Ventas	5,82E-16	3,78E-15	0,15	0,877	2,03E+12
Capital social extranjero	0,0005361	0,0011843	0,45	0,651	8,418224
d_cargos de seguridad digital	0,0801065	0,0603055	1,33	0,184	0,4509346
d_medidas técnicas	0,1329351	0,0622521	2,14	0,033**	0,4929907
d_políticas de seguridad digital	-0,0211699	0,0632615	-0,33	0,738	0,6051402
d_estándares	0,0451697	0,0686568	0,66	0,511	0,2429907
d_evaluación de riesgo	0,1430716	0,0629847	2,27	0,023**	0,4252336
d_legislación	-0,0054669	0,0641935	-0,09	0,932	0,2616822
d_industria	-0,0668821	0,1018324	-0,66	0,511	0,1121495
d_servicios	0,0067912	0,067205	0,10	0,920	0,6775701
d_micro	-0,1204211	0,0671351	-1,79	0,073*	0,4182243
d_mediana	0,0796988	0,0945996	0,84	0,400	0,1214953
d_gran	-0,0621638	0,1070584	-0,58	0,561	0,2242991

(*) dy/dx corresponde al cambio discreto de la variable ***dummy*** de 0 a 1.

Número de observaciones = 428
LR chi
Prob > chi^2 = 0,0000
Log-Likelihood = -243,5582
Pseudo R^2 = 0,1542

***Variables significativas al 1%
**Variables significativas al 5%
*Variables significativas al 10%

CUADRO 8: RESULTADOS DE LA REGRESIÓN NÚMERO DE INCIDENTES (2016)

Modelo de regresión lineal

Variable dependiente: logaritmo del número de incidentes

VARIABLES	COEFICIENTE	ERROR ESTÁNDAR ROBUSTO	T	P > ITI
Presupuesto para seguridad digital	5,42E-10	1,74E-10	3,11	0,002***
Número de empleados	0,0003852	0,0006597	0,58	0,560
Personal con acceso a Internet	0,0011143	0,0027034	0,41	0,680
Ventas	-7,30E-15	5,68E-15	-1,29	0,199
Capital social extranjero	-0,0037696	0,0041925	-0,90	0,369
d_cargos de seguridad digital	0,0649893	0,1919606	0,34	0,735
d_medidas técnicas	0,5166059	0,1724034	3,00	0,003***
d_políticas de seguridad digital	-0,0027982	0,1667429	-0,02	0,987
d_estándares	0,4788695	0,2640027	1,81	0,070*
d_evaluación de riesgo	0,3383868	0,1761986	1,92	0,055*
d_legislación	0,2083957	0,2382764	0,87	0,382
d_industria	0,0598495	0,4063326	0,15	0,883
d_servicios	0,0328707	0,2181484	0,15	0,880
d_micro	-0,2104846	0,1693744	-1,24	0,215
d_mediana	0,2147467	0,361134	0,59	0,552
d_gran	0,0250505	0,379239	0,07	0,947

Número de observaciones = 428

R^2 = 0,1712

***Variable significativa al 1%**Variable significativa al 5% *Variable significativa al 10%

CUADRO 9: RESULTADOS DE LA REGRESIÓN – PRESUPUESTO ASIGNADO POR LA EMPRESA PARA SEGURIDAD DIGITAL (2016)

Modelo de regresión lineal
Variable dependiente: logaritmo del presupuesto asignado por la empresa para la seguridad digital

VARIABLES	COEFICIENTE	ERROR ESTÁNDAR	T	P > ITI
Número de empleados	0,0049112	0,0018714	2,62	0,009***
Personal con acceso a Internet	0,0079542	0,012715	0,63	0,532
Logaritmo de las ventas	0,1399672	0,0567257	2,47	0,014**
Capital social extranjero	0,0108605	0,0143105	0,76	0,448
Logaritmo del número incidentes	0,2919303	0,1823273	1,60	0,110
d_cargos de seguridad	1,930772	0,7623268	2,53	0,012**
d_medidas técnicas	2,061519	0,7886683	2,61	0,009***
d_políticas de seguridad	1,603038	0,7658178	2,09	0,037**
d_estándares	2,148676	0,8688742	2,47	0,014**
d_evaluación de riesgo	2,151299	0,7983848	2,69	0,007***
d_legislación	0,8557661	0,7844744	1,09	0,276
d_industria	0,5255468	1,23481	0,43	671
d_servicios	1,502679	0,8042185	1,87	0,062*
d_micro	-1,597504	0,8421082	-1,90	0,059*
d_mediana	0,5863965	1,216569	0,48	0,630
d_gran	0,7025586	1,345639	0,52	0,602

Número de observaciones = 428
R^2 = 0,4251

***Variable significativa al 1% **Variable significativa al 5% *Variable significativa al 10%

CUADRO 10: RESULTADOS DE LA REGRESIÓN COSTO CON INCIDENTES DIGITALES (2016)

Modelo de regresión lineal
Variable dependiente: costo con incidentes digitales

VARIABLES	COEFICIENTE	ERROR ESTÁNDAR	T	P > ITI
Número de incidentes	531651	190266.3	2,79	0,008*

Número de observaciones = 42
R^2 = 0,1633

*Variable significativa al 1%

CUADRO 11: ESTIMACIÓN DE LA PROBABILIDAD QUE UNA ENTIDAD PÚBLICA IDENTIFIQUE LOS INCIDENTES DIGITALES (2016)

Modelo de estimación: logit

Variable dependiente: 1 si la entidad identifica incidentes digitales, 0 si no los identifica.

VARIABLES	EFECTO MARGINAL (DY/DX)*	ERROR ESTÁNDAR	Z	P>|Z|	$\bar{x}$
Presupuesto para seguridad digital	8,01E-11	4,34E-11	1,85	0,065*	2,92E+08
Número de personal	0,0001993	0,0000785	2,54	0,011**	325,4097
Personal con acceso a Internet	0,0047247	0,0016747	2,82	0,005***	72,07505
Presupuesto de inversión	1,59E-15	3,91E-15	0,41	0,684	7,00E+11
d_cargos de seguridad digital	-0,0862007	0,0610058	-1,41	0,158	0,4381339
d_medidas técnicas	0,1214568	0,056219	2,16	0,031**	0,4604462
d_políticas de seguridad digital	0,0695837	0,0568544	1,22	0,221	0,6308316
d_estándares	0,0745173	0,0743717	1,00	0,316	0,2636917
d_evaluación de riesgo	0,151459	0,0608966	2,49	0,013**	0,3853955
d_legislación	0,1359538	0,0530307	2,56	0,010***	0,4685598
d_nacional	-0,146032	0,1024856	-1,42	0,154	0,356998
d_municipal	0,0074466	0,0947813	0,08	0,937	0,5557809

(*) dy/dx corresponde al cambio discreto de la variable ***dummy*** de 0 a 1.

***Variables significativas al 1%
**Variables significativas al 5%
*Variables significativas al 10%

Número de observaciones = 493
LR chi
Prob > chi^2 = 0,0000
Log-Likelihood = -298,91209
Pseudo R^2 = 0,1247

CUADRO 12: RESULTADOS DE LA REGRESIÓN – PRESUPUESTO ASIGNADO POR LA ENTIDAD PÚBLICA PARA SEGURIDAD DIGITAL (2016)

Modelo de regresión lineal

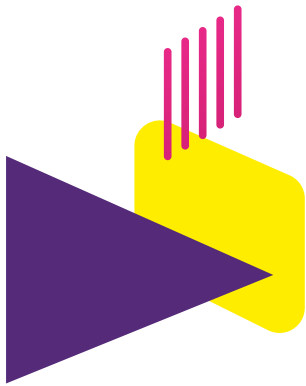
Variable dependiente: logaritmo del presupuesto asignado por la entidad pública para la seguridad digital

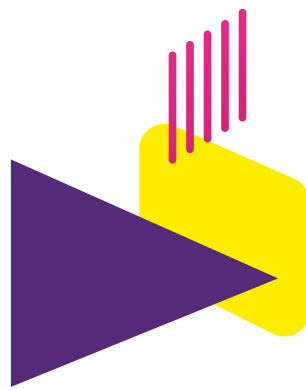
VARIABLES	COEFICIENTE	ERROR ESTÁNDAR	T	P > ITI
Número de personal	0,005017	0,0010813	4,64	0,000***
Personal con acceso a Internet	0,0716088	0,020742	3,45	0,001***
Logaritmo del presupuesto de inversión	0,1234978	0,0619476	1,99	0,047**
Logaritmo del número de incidentes	0,0091293	0,1740777	0,05	0,958
d_cargos de seguridad digital	1,588953	0,8025929	1,98	0,048**
d_medidas técnicas	2,396737	0,767671	3,12	0,002***
d_políticas de seguridad digital	1,120887	0,7730728	1,45	0,148
d_estándares	1,984836	1,013148	1,96	0,051**
d_evaluación de riesgo	0,7157857	0,8250376	0,87	0,386
d_legislación	0,6282294	0,73377	0,86	0,392
d_nacional	5,451329	1,356875	4,02	0,000***
d_municipal	1,14657	1,237875	0,93	0,355

Número de observaciones = 453

R^2 = 0,4379

***Variable significativa al 1% **Variable significativa al 5% *Variable significativa al 10





IMPACTO DE LOS INCIDENTES DE SEGURIDAD DIGITAL

EN COLOMBIA 2017