PROTECCIÓN DE LA INFRAESTRUCTURA CRÍTICA EN AMÉRICA LATINA Y EL CARIBE 2018

OAS More rights for more people

Microsoft

PROTECCIÓN DE LA INFRAESTRUCTURA CRÍTICA EN AMÉRICA LATINA Y EL CARIBE 2018

PROTECCIÓN DE LA INFRAESTRUCTURA CRÍTICA EN AMÉRICA LATINA Y EL CARIBE 2018

CRÉDITOS

Luis Almargo
Secretario General de la Organización de los Estados Americanos (OEA)

Tom Burt
Vicepresidente y Director Jurídico Adjunto de Digital Trust Microsoft Corporation

Equipo técnico de la OEA
Claudia Paz y Paz
Alison August Treppel
Belisario Contreras
Kerry-Ann Barrett
Bárbara Marchiori de Assis
Carina Pietsch

Equipo técnico de Microsoft
Andres Rengifo
Kaja Ciglic
Seema Kathuria

Colaboradores
Raúl Millán, Supervisor Especialista en Tecnología de la Información (Seguridad), Unidad de Seguridad de Sistemas - TIGU, Vicepresidente Ejecutivo de Tecnología y Tecnología de la Información, Canal de Panamá
Kaja Ciglic, Director, Política y Estrategia de Seguridad Cibernética, Microsoft
Hernán Vázquez, Gerente de Tecnología de la Información de la Asociación Regional de Empresas del Sector de Petróleo, Gas y Biocombustibles en América Latina y el Caribe (ARPEL)
Peter Burnett, Proceso Meridian

INTRODUCCIÓN

Luis Almagro
Secretario general
Organización de Estados Americanos

Como región, América Latina y el Caribe ha experimentado una de las tasas más rápidas de crecimiento de Internet desde principios de siglo. La tasa de penetración de Internet en América Latina y el Caribe se estima ahora en 65,1% con más de 400 millones de usuarios de Internet.

Si bien este crecimiento ha traído nuevas oportunidades para la región, la evolución de las amenazas relacionadas con el ciberespacio en los últimos años también ha aumentado las preocupaciones sobre el uso real y potencial de Internet con fines ilegales. Datos recientes muestran que el costo de la delincuencia cibernética ha alcanzado U$S8 mil millones en Brasil, U$S3 mil millones en México y U$S 464 millones en Colombia.

La infraestructura crítica pública y privada también sufre un mayor número de ciberataques: propietarios y operadores encuestados para el informe 2015 de OEA-Trend Micro Ciberseguridad e Infraestructuras Críticas en las Américas informaron un aumento del 53% de los incidentes cibernéticos que afectan sus sistemas informáticos durante el año anterior.

Los ataques a la infraestructura crítica tienen el potencial de alterar significativamente el funcionamiento del gobierno y las empresas por igual y dar lugar a un efecto dominó en los ciudadanos de nuestras naciones.

Estos ataques podrían ampliarse e incluso producir pérdidas catastróficas si los actores malintencionados deciden utilizar componentes de la infraestructura crítica de un país -sistemas y activos vitales para la seguridad de una nación- como armas de destrucción masiva.

La Organización de los Estados Americanos (OEA) se complace en presentar este informe como un producto de nuestra asociación en curso con Microsoft.

La colaboración con el sector privado es indispensable para la Protección de Infraestructuras Crítica (IC) e Infraestructuras Críticas de Información (CII). La OEA considera un enfoque de múltiples partes interesadas, especialmente el sector privado, esencial para el desarrollo de investigación y recursos para la región y para el desarrollo de soluciones para las cuestiones identificadas.

Este Informe presenta una actualización de las experiencias en la región en relación con los ciberataques contra propietarios y operadores de infraestructuras críticas y algunas de las mejores prácticas que han implementado para proteger estos activos vitales.

Desde 2004, la OEA ha enfatizado la "importancia de desarrollar una estrategia integral para proteger la infraestructura de la información que adopte un enfoque integral, internacional y multidisciplinario". Con este fin, en 2015, el Quinto Período Ordinario de Sesiones del Comité Interamericano contra el Terrorismo (CICTE) emitió una declaración sobre la "Protección de Infraestructuras Críticas de Amenazas Emergentes", mediante la cual los Estados Miembros declararon "su compromiso de identificar y combatir amenazas terroristas, independientemente de su origen o motivación, como infraestructura crítica y seguridad cibernética, entre otras, y la necesidad de cooperación del sector privado para prevenir, desarrollar la capacidad de recuperación de la infraestructura crítica y facilitar la resolución de delitos terroristas y conexos que se cometen a través de redes de comunicación globales".

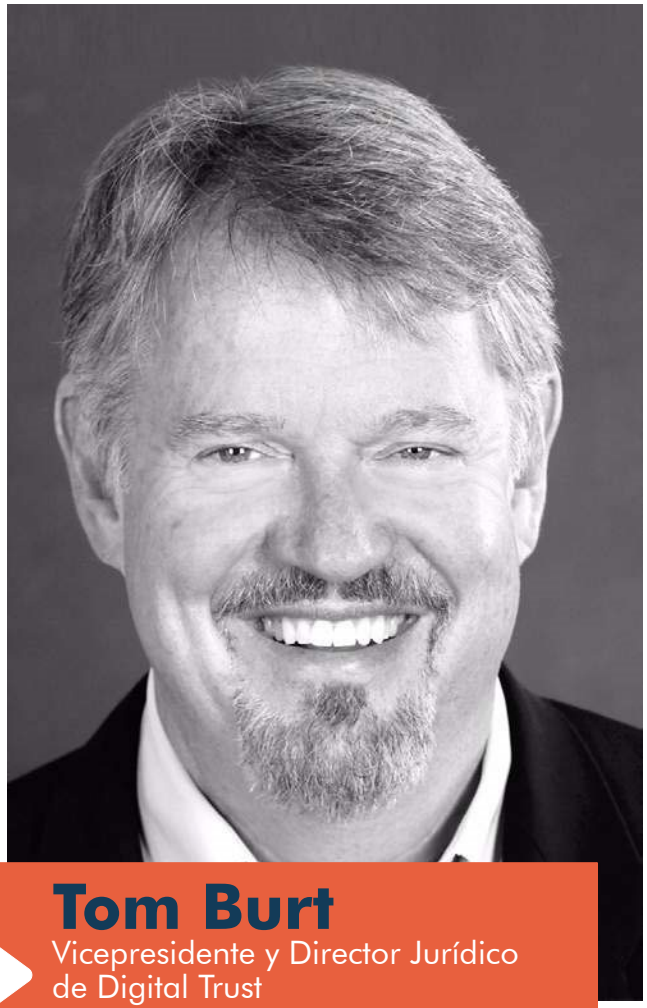
En este contexto, este Informe ha tenido el beneficio de la participación de más de 28 de nuestros 34 estados miembros, y algunas de las conclusiones positivas de los resultados indican que el 53% de los que encuestados poseen capacidades de detección y mantienen registros de estos eventos cibernéticos.

Sin embargo, desde una perspectiva regional, una de las deficiencias identificadas fue que solo el 49% de los encuestados respondió positivamente a la existencia de una agencia con la responsabilidad de proteger las infraestructuras críticas. Además, cuando se les preguntó si existían incentivos en el ámbito nacional para que los operadores de infraestructuras críticas implementaran medidas de seguridad, casi el 78% indicó que no existían tales incentivos, y un 61% adicional indicó que no había una regulación específica del sector relacionada. a la Protección de Infraestructuras Críticas de Información.

En la OEA, centramos nuestros esfuerzos en garantizar "más derechos para más personas". En el contexto de este estudio, eso significa proteger los derechos de los americanos para disfrutar de un entorno cibernético seguro. Los resultados de este informe confirman la necesidad de que los líderes regionales redoblen sus esfuerzos para apoyar la protección de nuestros diversos activos nacionales críticos.

Como región, hemos avanzado mucho y continuamos mejorando la cooperación efectiva en el área de la seguridad hemisférica. Nuestro enfoque ahora debe centrarse a pensar más estratégicamente en la infraestructura crítica y en la protección de la información crítica en la región y proporcionar los incentivos y el entorno necesarios para fomentar las buenas prácticas en esta área.

INTRODUCCIÓN



Tom Burt
Vicepresidente y Director Jurídico de Digital Trust
Microsoft Corporation

Protección de infraestructuras críticas: El momento de actuar es ahora

Los gobiernos de todo el mundo están centrando su atención en la ciberseguridad. Sus prioridades van desde el aumento de las habilidades de seguridad cibernética, a la adopción de nuevas leyes de cibercrimen y la comprensión de cómo las reglas internacionales nuevas o existentes podrían aplicarse al nuevo panorama Una prioridad comúnmente identificada es la protección de las infraestructuras críticas -los servicios, sistemas y funciones de las que dependen las naciones modernas- del ataque cibernético.

Los ataques cibernéticos a gran escala que hemos presenciado en 2017, WannaCry y NotPetya en particular, trajeron esa realidad más cerca de casa. Si bien las infraestructuras mundiales escaparon relativamente ilesas, teniendo en cuenta el considerable costo económico incurrido por los gobiernos y las empresas privadas de todo el mundo, el impacto potencial se dio mucho más en nuestros hospitales, puertos, telecomunicaciones, suministro de energía y otros servicios gubernamentales. En esta nueva era de amenazas cibernéticas, proteger y aumentar la resiliencia de las infraestructuras críticas es fundamental.

Este informe, en el que Microsoft se complace de haber podido asociarse con la Organización de Estados Americanos (OEA), es por lo tanto mucho más oportuno. En el informe, nosotros: i) examinamos las amenazas que enfrentan los países de América Latina y el Caribe, ii) estudiamos la ciberseguridad regional, y iii) presentamos las mejores prácticas y sugerencias para el futuro.

El informe es el último de una serie de iniciativas de Microsoft, a menudo en asociación con otros, para alentar a los gobiernos a desarrollar y adoptar un enfoque prioritario de la protección de infraestructuras críticas, basada en la gestión de riesgos. Entre estos esfuerzos, hemos pedido el desarrollo y la adopción de líneas base de ciberseguridad globalmente armonizadas para infraestructuras críticas. Con este fin, nos hemos asociado con el Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos en su desarrollo y revisión del Marco de Ciberseguridad del NIST y abogamos por su adopción como norma internacional.

Sin embargo, también hemos llegado a la conclusión de que nuestros llamados a una mayor inversión en prácticas defensivas podrían no ser suficientes. Por lo tanto, también hemos propuesto una Convención Digital de Ginebra, pidiendo a los gobiernos que ejerzan moderación cuando se trata de invertir en operaciones cibernéticas ofensivas y compromisos de no atacar a civiles en tiempos de paz. Uno de sus pilares sugeridos es que el gobierno no debe atacar las infraestructuras críticas de otras naciones. Espero que nuestra propuesta sea atendida, pero en cualquier caso este informe ayudará a aumentar la resiliencia de las infraestructuras críticas, no solo en América Latina, sino en todo el mundo.

PROTECCIÓN DE LA INFRAESTRUCTURA CRÍTICA EN AMÉRICA LATINA Y EL CARIBE 2018

TABLA DE CONTENIDO

Introducción 15

Los desafíos de la protección CII 16

Panorama de amenazas: Tendencia regional 18

Mejores Prácticas Globales para CIP 20

Resultados de la encuesta 25

Aspectos destacados y conclusiones 25

Experiencias y buenas prácticas: estudios de caso 43

Lecciones aprendidas del desarrollo y la implementación de Política de seguridad de la tecnología de la información (TI) en el Canal de Panamá Sistemas de Control Industrial (ICS) 44

La ciberseguridad es vital para proteger la infraestructura crítica 48

Ciberseguridad industrial y el desafío de la cooperación entre IT y TO en la industria del petróleo y el gas 53

Crear una conciencia global de Protección de Infraestructuras Críticas de Información: la Conferencia Anual de Meridian: más de una década de experiencia 55

Apéndice 58

Recursos adicionales 58

PROTECCIÓN DE LA INFRAESTRUCTURA CRÍTICA EN AMÉRICA LATINA Y EL CARIBE 2018

INTRODUCCIÓN

Los avances en la tecnología digital han revolucionado completamente la forma en que las personas, las empresas y los estados interactúan. La prestación de servicios gubernamentales, así como el flujo general de bienes y servicios, se han transformado debido a la mayor conectividad a Internet y al advenimiento del comercio electrónico y las transacciones electrónicas. Sin embargo, las nuevas tecnologías traen consigo desafíos y amenazas propias.

La adopción de nuevas tecnologías digitales permite una gestión más eficiente de las infraestructuras críticas en términos de escala, distancia y tiempo, pero también introduce nuevas vulnerabilidades que hacen que la protección de las infraestructuras críticas de información sea una tarea importante y desafiante. La protección de los activos y sistemas de información que respaldan y forman infraestructuras críticas, es decir, las infraestructuras de información críticas (CII) se ha convertido en una preocupación importante para las políticas de seguridad nacional a medida que se adoptan nuevas tecnologías. La Protección de Infraestructuras Críticas de Información (CIIP) se puede definir como: "Todas las actividades destinadas a garantizar la funcionalidad, continuidad e integridad de CII para disuadir, mitigar y neutralizar una amenaza, riesgo o vulnerabilidad o minimizar el impacto de un incidente".[1]

Si bien las infraestructuras críticas y la CII están interrelacionadas y ambas son cruciales para el buen funcionamiento de una sociedad y su seguridad, estos conceptos no se puede utilizar indistintamente y requieren diferentes métodos de gestión, control y protección. Si bien existen varias definiciones de infraestructura crítica, y las naciones difieren en qué sectores se incluyen en la clasificación, las infraestructuras comúnmente críticas se consideran "aquellas infraestructuras que son esenciales para el mantenimiento de las funciones vitales de la sociedad, la salud, la seguridad, el bienestar económico o social de las personas y la interrupión o destrucción de las mismas presentaría graves consecuencias".[2] Por lo tanto, la protección continua y la gestión de riesgos de esas infraestructuras son cruciales para su resiliencia y la seguridad de cada nación.[3]

Las tecnologías digitales son cada vez más adoptadas para la gestión, el mantenimiento, el control y la protección de infraestructuras críticas, por ejemplo con sistemas de control industrial (ICS), o se utilizan como infraestructura en sí, como los servicios de telecomunicaciones o los puntos de intercambio de tráfico de Internet.[4] Estas se denominan CII y comúnmente son definidas como "redes de tecnologías de la información y la comunicación (TIC) y datos que respaldan, vinculan y permiten operaciones de infraestructura críticas, y cuya interrupción, destrucción o explotación podría tener un impacto debilitante" ".[5]

Este informe tiene como objetivo reflejar las experiencias y prácticas de infraestructuras críticas y protección de infraestructura críticas de información en América Latina y el Caribe. Como región con una larga historia de cooperación y una de las primeras en cooperar en el tratamiento de amenazas de ciberseguridad, estos aprendizajes pueden ser una referencia valiosa para la ciberseguridad y la comunidad de infraestructura críticas en su conjunto.

1. GFCE (2016). P.6.

2. Consejo Europeo, Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección: www.eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008L0114

3. Microsoft (2014), Protección de Infraestructuras Críticas: Conceptos y contancia: www.query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVtZU

4. GFCE (2016), La Guía de Buenas Prácticas de GFCE-MERIDIAN sobre Infraestructuras Críticas de la Información Protección para los responsables de las políticas gubernamentales:
www.meridianprocess.org/siteassets/meridian/gfce-meridian-gpg-to-ciip.pdf

5. Microsoft (2014). P.4.

Los desafíos de la protección CII

La protección de la CII es difícil por varias razones que incluyen, entre otras, las siguientes: (1) la interconexión global de las infraestructuras de información; (2) la incapacidad de medir con precisión el impacto de un ciberataque; (3) la responsabilidad dispersa por la ciberseguridad; y (4) el panorama de ciberamenazas en constante evolución.

Interconectividad global

Al igual que con todos los aspectos de nuestras vidas, las CII está cada vez más conectadas y operan en un mundo sin fronteras claras, lo que permite flujos de información y datos mucho más libres y menos controlables. Hay claros beneficios para esto, particularmente en términos de eficiencia y productividad. Sin embargo, esta misma interconexión también hace que la infraestructura crítica sea vulnerable a los ciberataques. La CII de un país en particular puede convertirse en un blanco de ciberataques o, de hecho, un medio para atacar la CII de otra nación. En resumen, una CII vulnerable puede convertirse en el eslabón más débil de la red global, haciendo de CIIP un punto focal para la colaboración y el esfuerzo universales.[6]

Sin embargo, antes de emprender una alianza, los países deben reconocer que se trata de un ámbito de política en el que odos tienen interés y es vital cooperar. Para ello, las naciones necesitan comprender sus amenazas y vulnerabilidades nacionales específicas. Una estrategia nacional de ciberseguridad, y más específicamente un marco nacional de CIP, puede ayudar con eso. Es importante señalar que dicho marco, para ser eficaz, debe reflejar no solo una comprensión evolutiva de las motivaciones y capacidades de los actores de la amenaza; sino también los posibles riesgos sistémicos que surgen de las complejidades de estos sistemas. Además, las actividades deben llevarse a cabo para promover la confianza entre las naciones para que, por ejemplo, la información sobre las amenazas e incidentes que se dirigen a la CII pueda compartirse más fácilmente.

Capacidad de evaluar el impacto y la pérdida

Uno de los principales desafíos, tanto a nivel organizacional como nacional, es la incapacidad de medir con precisión el impacto de un ciberataque en particular. Esto es difícil incluso para la corporación más sofisticada, ya que debe tener en cuenta problemas, tales como el impacto en las operaciones, daños a la marca, multas y compensación. Sin embargo, mientras que a nivel organizacional es probable que el impacto sea exclusivamente económico, la situación se agrava para los responsables de la formulación de políticas, que podrían tener que evaluar las consecuencias sociales de que un servicio particular que no está disponible.

Además, las dos partes interesadas están motivadas por diferentes prioridades. A nivel organizacional, la prioridad es proteger a la entidad en cuestión. Como resultado, la mayoría de las organizaciones no entienden cómo sus riesgos o vulnerabilidades pueden interactuar con otros en el sistema. Por el contrario, a nivel nacional, los estrategas políticos deben evaluar cuándo los riesgos de negocios agregados podrían constituir un riesgo nacional y, por lo tanto, deben comprender los vínculos entre las diferentes CII. Por ejemplo, el impacto nacional potencial del compromiso, daño o destrucción de una única IIC no puede elevarse al nivel de consecuencia nacional hasta que se considere en el contexto más amplio de otros incidentes que ocurran y que agraven su impacto. Cuando se agrega, tales vulnerabilidades podrían crear un riesgo para la seguridad económica nacional.

Responsabilidad dispersa

Las CII son propiedad de partes interesadas tanto públicas como privadas, por lo que su protección, por definición, es una responsabilidad que abarca ambos sectores. Sin embargo, los diferentes sectores consideran sus responsabilidades particulares de diferentes maneras. Los gobiernos tienden a considerar la infraestructura crítica como una colección monolítica de sistemas y servicios

6. GFCE (2016); Perry, W. J. (2016): Infraestructura crítica en América Latina: Conectada, Dependiente y Vulnerable. Centro de Estudios Hemisféricos; www.hds.dodlive.mil/files/2016/05/Pub-OP-Saavedra.pdf

en comparación con el sector privado, que analiza los elementos básicos dentro de su control directo o sus obligaciones contractuales para prestar servicios. Más específicamente, los gobiernos tienden a asignar recursos para abordar las amenazas más acuciantes de su país, asegurando los activos más importantes con un esfuerzo y atención sustanciales. Por el contrario, el sector privado se concentra en la prestación de servicios, la innovación y la participación en el mercado. Estas diferencias en el enfoque pueden ser difíciles de superar y pueden agravar los desafíos en la comunicación entre las audiencias técnicas, administrativas y gubernamentales.

Por lo tanto, proteger las CII requiere una cooperación y colaboración continuas entre el gobierno y los actores del sector privado. Por consiguiente, las asociaciones público-privadas y los grupos de trabajo deben estar en la primera línea de la evaluación, gestión y protección de riesgos de la CII7.[7] Es importante que las organizaciones privadas, especialmente las que poseen y gestionan las infraestructuras de información, comprendan su papel en CIIP.[8] Del mismo modo, los gobiernos, que son responsables de la seguridad nacional y que crean los procedimientos necesarios para el intercambio de información entre las partes interesadas, deben comprender que el sector privado posee conocimientos expertos sobre el tema.[9]

Panorama de amenazas en constante cambio

Las amenazas en el ciberespacio evolucionan considerablemente más rápido que en otros campos, como el terrorismo internacional o las amenazas a las capacidades militares convencionales. Si bien estos últimos pueden tardar años en cambiar, las amenazas cibernéticas lo hacen constantemente.[10] Además, tales amenazas pueden provenir de una gran cantidad de actores motivados de forma diferente, desde ciberdelincuentes hasta gobiernos que realizan espionaje o incluso operaciones militares ofensivas. Dado el entorno externo cambiante, las CII y los países deben evaluar sus riesgos con frecuencia y regularidad. Como se mencionó anteriormente, un marco de gestión de riesgos puede ayudar a garantizar que cada organización individual sea consciente del riesgo al que se enfrenta, esté de acuerdo con sus niveles de tolerancia al riesgo y ponga las mitigaciones correspondientes en su lugar. De igual manera puede ayudar a nivel nacional, teniendo en cuenta que los niveles de tolerancia pueden variar de un país a otro, así como de una situación a otra. Por ejemplo, un corte de energía prolongado a raíz de un huracán puede ser tolerable, pero un ciberataque inesperado que destruya los componentes críticos de la distribución de energía podría no serlo.

También es importante señalar que la gestión continua y eficaz del riesgo de ciberseguridad es una tarea compleja y de recursos intensivos. Priorizar las CII implica un duro intercambio entre los múltiples roles que los gobiernos deben desempeñar para proteger a los ciudadanos y proporcionar seguridad nacional y una cooperación más dinámica con los socios de la industria. CIIP requiere nuevas herramientas y marcos para poder evaluar y gestionar de manera eficaz los riesgos de ciberseguridad y proteger las infraestructuras de información virtual y las infraestructuras tradicionales y físicas por igual.[11] Por lo tanto, es vital que los gobiernos se centren principalmente en funciones y servicios que son realmente críticos. y que se establezca un proceso claro para asegurar que todos los activos, sistemas, redes o datos sean identificados y, cuando sea necesario, designados como "alta prioridad".

7. Perry, W. J. (2016); Microsoft (n.d.).

8. ENISA (2015); Enfoques de Protección de Infraestructuras Críticas de la información en la UE: www.resilience.enisa.europa.eu/enisas-ncss-project/CIIPApproachesNCSS.pdf

9. Abele-Wigert, I., & Dunn, M. (2006). Manual Internacional CIIP Vol. I - Un inventario de 20 políticas nacionales y 6 internacionales críticas de protección de infraestructuras críticas de información. Zurich: Centro de Estudios de Seguridad, ETH Zurich.

10. Assante, M. J. (2009); Protección de Infraestructuras en el Mundo Antiguo: 42.º Conferencia Internacional de Hawaii sobre Ciencias de Sistemas, Big Island, HI. doi: 10.1109 / HICSS.2009.260

11. Un Marco para la Gestión de Riesgos de Infraestructuras Críticas de la Información; www.query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc7

PANORAMA DE AMENAZAS
TENDENCIAS REGIONALES[12]

El Informe de Inteligencia de Seguridad de Microsoft es una publicación semestral que se basa en la experiencia interna de Microsoft para presentar el estado actual de las amenazas cibernéticas. La inteligencia que lo informa proviene de las señales relacionadas con la seguridad del consumidor y de los sistemas de negocios en las instalaciones y los servicios en la nube que Microsoft opera a escala global. Por ejemplo, cada mes se escanean 400 mil millones de correos electrónicos en busca de phishing y malware, se procesan 450 mil millones de autenticaciones y se ejecutan más de 18 mil millones de escaneos de páginas web.

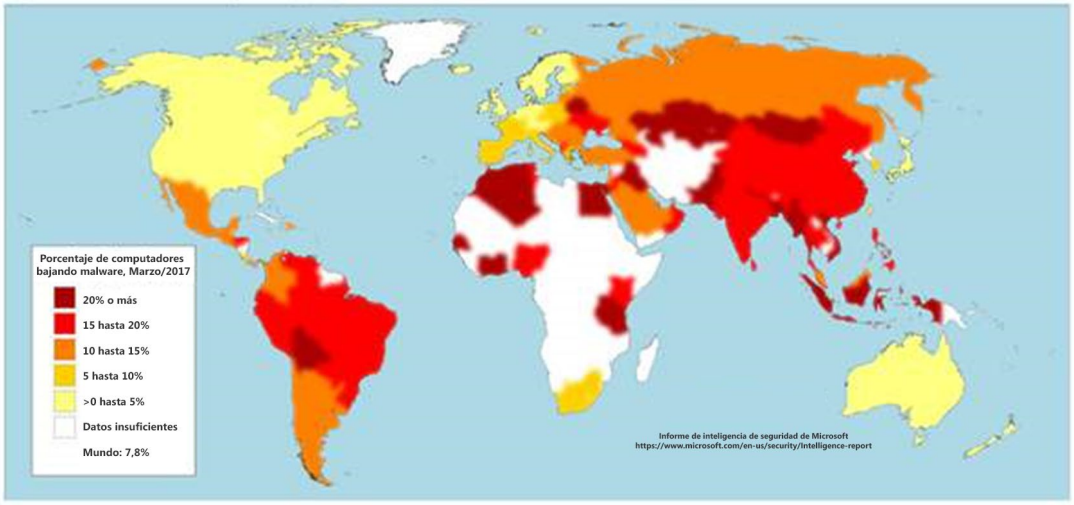
Esta información permite la observación de tendencias a través de las diversas plataformas de Microsoft, así como las regiones.

Por ejemplo, el año pasado se observó un aumento del 300 por ciento en el número de cuentas de usuarios atacadas. También se observó la metodología para las infracciones de cuenta y, por lo tanto, se pueden desarrollar recomendaciones para la prevención De hecho, la gran mayoría de los compromisos que acabamos de mencionar son el resultado de contraseñas débiles y fáciles de adivinar y de una gestión de contraseñas deficiente, seguidas de ataques de phishing dirigidos y violaciones de servicios de terceros.

Entre otros hallazgos, el informe analiza el porcentaje de equipos que ejecutan el software de seguridad en tiempo real de Microsoft que informa detectar malware o software potencialmente no deseado o informa sobre la detección de una amenaza específica de la familia, la llamada "tasa de encuentro". Por ejemplo, la tasa de encuentro de la familia de malware Win32 / Banload en Brasil en marzo de 2017 fue del 0,4 por ciento. Estos datos significan que, de las computadoras en Brasil que estaban ejecutando el software de seguridad en tiempo real de Microsoft en marzo de 2017, el 0.4 por ciento informó que tuvo contacto con la familia Banload, y el 99,6 por ciento no.

Los datos de telemetría generados por productos de seguridad de Microsoft de lo equipos cuyos administradores o usuarios optan por proporcionar datos a Microsoft incluyen información sobre la ubicación del equipo, según lo determinado por la geolocalización de IP. Estos datos permiten comparar tasas de encuentro, patrones y tendencias en diferentes ubicaciones alrededor del mundo. Utilizando las tasas de encuentro, Microsoft toma conocimiento de las amenazas más prevalentes en bases globales y por país, y utiliza esta información para mejorar sus productos y servicios de seguridad para hacer frente a esas amenazas.

Figura 12. Índice de registro por país/región, Marzo de 2017



12. Informe de inteligencia de seguridad de Microsoft, 2017 https://www.microsoft.com/en-us/security/Intelligence-report

Los resultados para América Latina y el Caribe en general siguen siendo más altos que el promedio mundial, aunque existen diferencias significativas entre los distintos países. Puerto Rico, Canadá y Estados Unidos preforman particularmente bien, superando al resto del mundo, mientras que Costa Rica y Panamá lo siguen de cerca[13].

PAÍS	ENERO 2017	FEBRERO 2017	MARZO 2017
Argentina	13.0%	11.5%	11.1%
Bolivia	19.4%	18.0%	21.1%
Canadá	6.0%	5.0%	3.2%
Brasil	19.4%	16.8%	17.0%
Chile	12.0%	10.3%	10.8%
Colombia	15.7%	14.6%	13.3%
Costa Rica	13.0%	11.1%	9.4%
Rep. Dominicana	17.3%	15.4%	14.9%
Ecuador	18.8%	16.9%	17.9%
El Salvador	15.5%	14.0%	13.7%
Guatemala	15.5%	13.7%	12.8%
Honduras	17.8%	16.4%	16.4%
Jamaica	14.1%	12.3%	12.8%
México	14.1%	12.8%	12.1%
Panamá	12.1%	10.5%	10.7%
Paraguay	16.7%	14.6%	15.5%
Perú	18.2%	16.3%	16.9%
Puerto Rico	7.5%	6.4%	6.0%
Trinidad y Tobago	12.1%	9.9%	9.4%
Estados Unidos	4.7%	4.0%	2.4%
Uruguay	12.2%	11.1%	10.7%
Venezuela	21.4%	18.1%	19.5%
Mundo	10.3%	9.1%	7.8%

Los resultados del informe aclaran que todos los actores involucrados en la protección de infraestructuras críticas deben tomar en serio la ciberseguridad. Los siguientes pasos son acciones simples que ayudan a proteger su entorno:

- Reduzca el riesgo de compromiso de credenciales educando a los usuarios sobre por qué deberían evitar contraseñas simples, haciendo cumplir la autenticación de factores múltiples y aplicando métodos de autenticación alternativos (por ejemplo, gesto o PIN).
- Impone políticas de seguridad que controlan el acceso a datos confidenciales y limita el acceso de la red corporativa a usuarios, ubicaciones, dispositivos y istemas operativos (SO) apropiados.
- No trabaje en zonas Wi-Fi públicas donde los atacantes puedan espiar sus comunicaciones, capturar inicios de sesión y contraseñas, y acceder a sus datos personales.
- Actualice periódicamente sus sistemas operativos y otro software para garantizar que se instalen los últimos parches.

13. El análisis detallado por país está disponible para Argentina, Bolivia, Brasil, Chile, Colombia, Ecuador, Paraguay, Perú, Venezuela y Uruguay: www.microsoft.com/en-us/security/Intelligence-report

MEJORES PRÁCTICAS GLOBALES PARA CIP

La gestión de riesgo[14]se ha convertido en una práctica crítica en ciberseguridad. Consiste típicamente en dos sistemas de prácticas: una centrada en la evaluación de riesgos (identificación, análisis, evaluación del riesgo) y otra centrada en la gestión (aceptación, transferencia, tratamiento de riesgos). El objetivo de la gestión de riesgos de ciberseguridad es avanzar y mantener un excelente estado de ciberseguridad basado en las necesidades, consideraciones y mejores prácticas únicas de la industria de la organización.

> *Con una comprensión de la tolerancia al riesgo, las organizaciones pueden priorizar las actividades de ciberseguridad, permitiendo a las organizaciones tomar decisiones informadas sobre los gastos de ciberseguridad. La implementación de programas de gestión de riesgos ofrece a las organizaciones la capacidad de cuantificar y comunicar los ajustes a sus programas de seguridad cibernética. Las organizaciones pueden optar por manejar el riesgo de diferentes maneras, incluyendo la mitigación, la transferencia, la prevención o la aceptación del riesgo, según el impacto potencial en la prestación de los servicios críticos.*
>
> *Marco de ciberseguridad del NIST*

Tradicionalmente, la gestión de riesgos dependía en gran medida del desarrollo de "listas de verificación" que pueden ser utilizadas por entidades públicas o privadas para medir el cumplimiento. Este enfoque de la gestión del riesgo de ciberseguridad es estático en sus controles y objetivos y rígido en su implementación y generalmente no produce resultados que conduzcan a una mitigación óptima de los riesgos de ciberseguridad, dejando a las organizaciones y personas expuestas al ataque y la explotación. En cambio, la gestión del riesgo necesita garantizar que se implementen medidas de protección basadas en la integración de información de amenazas, vulnerabilidades identificadas y una estrategia de reducción de riesgos. Si bien no es una solución completa en sí misma, la gestión de riesgos promueve prácticas organizacionales sólidas que incluyen la planificación, los procedimientos, la priorización presupuestaria y la asignación de recursos clave (humanos, monetarios y técnicos).

Una revisión exhaustiva de la literatura relevante[15] indica lo siguiente como mejores prácticas comunes para considerar en el desarrollo de una política o marco de CIIP sostenible.

14. La gestión de riesgos se define como el proceso de identificación de riesgos, evaluación de riesgos y adopción de medidas para reducir los riesgos a un nivel aceptable (Guía de gestión de riesgos NIST para sistemas de tecnología de la información) - www.csrc.nist.gov/publications/detail/sp/800-30/archive/2002-07-01)

15. Trend Micro y OAS. (2015) Informe sobre Ciberseguridad e Infraestructura Crítica en las Américas; ENISA (2015) Enfoques de Protección de Infraestructuras Críticas de Información en la UE; Brunner, E., & Suter, M. (2009) Manual Internacional de CIIP - Un inventario de 25 políticas nacionales y 7 internacionales de protección de infraestructuras críticas de información. Zurich: Centro de Estudios de Seguridad, ETH Zurich; Dunn, M., y Mauer, V. (2006) Manual Internacional de CIIP 2006 - Análisis de problemas, desafíos y perspectivas Zurich: Centro de Estudios de Seguridad, ETH Zurich; García Zaballos, A., y Jeun, I. (2016). Mejores prácticas para la Protección de Infraestructuras Críticas de Información (CIIP) - Experiencias de América Latina, el Caribe y Países Seleccionados. Banco Interamericano de Desarrollo (BID) y Agencia de Internet y Seguridad de Corea
(KISA); ENISA. (2014). Manejo de incidentes durante el ataque a Infraestructuras Críticas de Información; (2016) La Guía de buenas prácticas GFCE-MERIDIAN sobre Protección de
Infraestructuras Críticas de la información para los responsables de la formulación de políticas gubernamentales; Microsoft. (n.d.). Un marco para la Gestión de Riesgos de Infraestructuras Críticss de la Información (Borrador de documento de trabajo); Instituto Nacional de Estándares y Tecnología. (2017). Marco para Mejorar la Ciberseguridad de las Infraestructuras Críticas (Versión 1.1 Proyecto 2) 42)2007; Un Marco Nacional Genérico para Protección de Infraestructuras Críticas de la Información Zurich: Centro de Estudios de Seguridad, ETH Zurich.

MEJORES PRÁCTICAS GLOBALES PARA CIP

A. Asegurar una división clara de las responsabilidades:

Dado que CIIP involucra a múltiples partes interesadas, con diferentes intereses y puntos de vista con respecto a ella, se requiere un fuerte liderazgo del gobierno para coordinar las múltiples agencias que deben participar en el proceso de desarrollo de una estrategia CIIP, así como en su implementación. La estrategia también debe determinar claramente las diversas responsabilidades de las CIIP, tanto en operadores públicos como privados, así como en los diferentes sectores. También deberían asignarse plazos y presupuestos. El "Plan Nacional para la Protección de Infraestructuras Críticas de Información"[16], así como la Recomendación del Consejo de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) sobre la Protección de Infraestructuras Críticas de Información[17] son guías útiles para lograrlo.

B. Participar en un enfoque holístico:

Una política eficaz de CIIP debe adoptar un enfoque holístico que considere aspectos y puntos de vista técnicos, económicos, organizacionales, de cumplimiento de la ley y de políticas de seguridad. La razón de esto es que la operación y protección de CIIP implica una sección representativa de actores con diferentes roles. Por ejemplo, en el caso de un incidente cibernético, se puede llamar al equipo de respuesta para contener el evento; sin embargo, si el incidente se identifica como un ataque intencional, se puede llamar a la policía u otro personal de seguridad para investigar. Por lo tanto, la política debe delinear roles claros de responsabilidad y canales de comunicación para todos los actores involucrados para asegurar la coordinación y una respuesta estratégica.

C. Desarrollar marcos, pautas y procedimientos:

Los gobiernos deberían, mediante un proceso consultivo abierto, elaborar procedimientos y directrices claros para los procesos y aspectos clave de la CIIP. Los marcos deben estar integrados en la gestión de riesgos, al tiempo que se asegure que los operadores CII puedan adoptar la última tecnología, como la computación en la nube, para lograr las eficiencias necesarias. Un marco de gestión de riesgo recomendado, por ejemplo, incluye el marco de gestión de NIST, que enfatiza que "la gestión del riesgo organizacional es un elemento clave en el programa de seguridad de la información de la organización y proporciona un marco efectivo para seleccionar los controles de seguridad apropiados para un sistema - los controles de seguridad necesarios para proteger a las personas y las operaciones y los activos de la organización".

16. Suter, M. (2007). Un Marco Nacional Genérico para Protección de Infraestructuras Críticas de Información (CIIP). Zurich: Centro de Estudios de Seguridad, ETH Zurich.

17. Recomendación de la Organización para la Cooperación y el Desarrollo Económicospara la Protección de Infraestructuras Críticas de Información: www.oecd.org/sti/40825404.pdf

MEJORES PRÁCTICAS GLOBALES PARA CIP

D. *Establecer líneas de base de seguridad:*

Las líneas de base de seguridad son un conjunto fundamental de políticas, resultados, actividades, prácticas y controles destinados a ayudar a gestionar el riesgo de seguridad cibernética. Las líneas de base de seguridad son particularmente útiles para mejorar la ciberseguridad, ya que deben abarcar una serie de riesgos que suelen aplicarse en ciertos entornos. La mayoría de los riesgos que enfrentan los gobiernos y las empresas son similares, por lo que la mayoría de las actividades "básicas" o de gestión de riesgos también son similares. Por ejemplo, todas las organizaciones deben pensar en revisar y actualizar regularmente las evaluaciones de riesgos, administrar cómo se accede a los recursos para evitar usuarios o comportamientos no autorizados, y planificar y mitigar el impacto de los incidentes.

E. *Soporte de soluciones dinámicas:*

Debido a la continua evolución del panorama cibernético, cualquier solución y enfoque CIIP debe ser dinámica y de naturaleza flexible. La situación regular y frecuente y las reevaluaciones de riesgos son importantes para mantener soluciones actualizadas y garantizar mejoras constantes. Un ejemplo de cómo garantizar ese enfoque es el Programa Voluntario Cibernético Comunitario de Infraestructura Crítica (C3 - pronunciado 'C-Cubed')[18], que fue establecido por el Departamento de Seguridad Nacional de los Estados Unidos. El Programa C3 se estableció para ayudar a los propietarios y operadores de infraestructuras críticas a utilizar el Marco NIST para gestionar sus riesgos cibernéticos.

F. *Fomentar la confianza:*

Como se ha señalado anteriormente, las alianzas público-privadas entre las CII y el gobierno son esenciales para la CIIP y deben basarse en un intercambio abierto de información y experiencia. Para facilitar dicho intercambio, la confianza entre las partes es esencial. La generación de confianza puede ser particularmente desafiante cuando las alianzas implican empresas competidoras que tienen un interés particular en s mantener sus activos y posibles problemas de seguridad de los competidores. Es fundamental que los gobiernos ayuden a facilitar estos intercambios y ayuden a proteger sectores enteros en lugar de solo empresas individuales.

G. *Crear proyectos que demuestren beneficios mutuos:*

Las alianzas público-privadas, así como las redes nacionales e internacionales, deben tener como objetivo el intercambio de información y el apoyo mutuo con respecto a las amenzas cibernéticas. Sin embargo, estos son difíciles de despegar. De hecho, para que el intercambio de información sea exitoso a largo plazo, sus beneficios deben ser claros para todas las partes involucradas. Por lo tanto, es importante que todos los participantes, ya sean públicos o privados, compartan cualquier información de inteligencia y descubran que podrían tener que habilitar la seguridad del grupo en su conjunto.

18. Programa Voluntario de la Comunidad Cibernética de Infraestructuras Críticas: www.us-cert.gov/ccubedvp

MEJORES PRÁCTICAS GLOBALES PARA CIP

H. Desarrollar mecanismos de alerta temprana:

Los sistemas de alerta temprana desempeñan un papel clave en la prevención de la propagación de ataques cibernéticos y en la minimización del impacto de las amenazas cibernéticas. Por lo tanto, tanto el sector público como el privado deberían priorizar las funciones que permiten mecanismos de alerta temprana. El intercambio de información entre las diferentes CII, así como con el gobierno, por ejemplo, aumentaría la conciencia situacional de los operadores de las CII, les permitiría detectar un ataque potencial y frustrarlo o mitigar su impacto.

I. Invertir en recursos humanos y técnicos:

La CIIP requiere empleados con habilidades particulares. La identificación, el reclutamiento y la retención de expertos en ciberseguridad es crucial para garantizar un alto nivel de seguridad y protección continua. Además, es importante que las organizaciones entiendan que las habilidades de ciberseguridad no son un término monolítico y que pueden necesitar diferentes expertos para ayudarles con la gestión de riesgos y la seguridad informática tradicional, por ejemplo Además, las organizaciones deberían proporcionar capacitación periódica de seguridad para todo el personal, ya que la falta de higiene en materia de seguridad cibernética en toda la organización a menudo es donde las entidades son más vulnerables.

Además, garantizar que los empleados estén equipados con los recursos técnicos necesarios para llevar a cabo su trabajo de manera efectiva es igualmente importante. Como resultado, se recomienda una asignación presupuestaria suficiente para productos y servicios de ciberseguridad técnica.

J. Mejorar la resiliencia cibernética:

Los estados y las empresas deberían implementar una estrategia de resiliencia cibernética para garantizar la continuidad del negocio y del servicio en caso de un incidente de seguridad. Es fundamental que vayan más allá de centrarse en la ciberseguridad, pero se aseguren de que estén preparados para que cuando ocurra una crisis, sean receptivos a ella y sean capaces de reinventar su estructura de TIC frente al estrés sostenido y las interrupciones agudas. En otras palabras, ser ciber-resilientes asegurará que las empresas o los servicios puedan continuar estando disponibles y operar a pesar del impacto de las amenazas cibernéticas o de los desastres naturales y causados por el hombre.

K. Participar en una red internacional:

Como las amenazas cibernéticas no tienen fronteras físicas, la cooperación entre organizaciones y países es esencial para la prevención, identificación, respuesta y recuperación efectivas. Identificar y participar en estructuras y marcos internacionales existentes, por ejemplo a través de la OEA, Meridian (ver más abajo) o FIRST[19], puede ayudar a los gobiernos a comprender el entorno de amenazas y mantenerlos al tanto de las últimas tendencias de ciberseguridad y mejores prácticas.

19. www.first.org

Parte 1

EXPERIENCIAS Y PRÁCTICAS ADOPTADAS PARA LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS Y INFRAESTRUCTURAS CRÍTICAS DE LA INFORMACIÓN

RESULTADOS DE LA ENCUESTA

Aspectos destacados y conclusiones

Las CII desempeñan un papel central en las sociedades y economías modernas, convirtiendo su protección en una importante preocupación nacional e internacional. Su complejidad e interconexión solo amplifican la importancia de esta preocupación. Las CII suelen ser el resultado agregado de funciones proporcionadas por muchos propietarios y operadores, vendedores de tecnología y servicios, y gobiernos. La complejidad de esta cadena de valor, junto con las diferentes partes interesadas que en última instancia brindan servicios de infraestructura críticos, hacen que la seguridad y la resiliencia de estas operaciones sean una responsabilidad desafiante y compartida.

La comprensión de los niveles de cooperación entre las diferentes entidades involucradas fue uno de los temas abordados por la encuesta de las partes interesadas de Protección de Infraestructuras Críticas (CIP) en América Latina y el Caribe. Esta encuesta es la primera de su tipo para la región y saca a la luz una serie de hallazgos importantes relacionados con la percepción de amenazas, así como la preparación de organizaciones y países individuales.

Los resultados de la encuesta se reproducen en detalle en la siguiente sección, pero cabe destacar una serie de cuestiones por adelantado. Si bien los gobiernos a nivel mundial han estado trabajado cada vez más en la adopción de marcos y directrices de ciberseguridad para abordar la protección de infraestructuras críticas, este no ha sido el caso en la región. Las iniciativas globales abarcan desde el desarrollo e implementación de estrategias, prácticas de intercambio de información, evaluación y gestión de riesgos, hasta la introducción de líneas de base de seguridad, estándares y otros requisitos técnicos. **Esta encuesta confirmó que la mayoría de los gobiernos de la región no ha establecido programas de incentivos que puedan fomentar la implementación voluntaria de medidas de ciberseguridad por parte de los operadores y propietarios de CII y CIIP, o que de hecho hayan comenzado a implementar marcos obligatorios. Esperamos que las mejores prácticas ofrecidas en esta publicación los alienten a hacerlo.**

Sin embargo, a pesar de la falta de marcos oficiales, los resultados de la encuesta indican que **existe comunicación y colaboración entre el sector privado y el gobierno.**. De hecho, el 69% de los encuestados indicó que participó en grupos de trabajo, el 64% indicó que se lleva a cabo el diálogo informal y/o la cooperación, y el 42% destacó la existencia de alianzas público-privadas. Estas respuestas reflejan las asociaciones y prácticas establecidas dentro de la región, que han emergido orgánicamente.

El CIIP eficaz requiere empleados con un conjunto de habilidades particular y tecnología de soporte para su protección. La identificación, el reclutamiento y la retención de expertos cibernéticos es crucial para garantizar un alto nivel de seguridad y protección continua. **Según los resultados del estudio, el 53% de las organizaciones que respondieron indicaron que tenían la capacidad de detectar y registrar incidentes cibernéticos. Además, el 73% indicó que habían detectado un ciberataque en los últimos 12 meses.**

Los encuestados también destacaron las buenas prácticas. **El 48% de los encuestados indicó que contaban con capacitaciones sobre seguridad cibernética para sus empleados, el 46% indicó que tenían un plan de recuperación ante desastres, el 42% indicó que tenían un plan de respuesta ante incidentes cibernéticos, el 41% indicó que tenían una estrategia documentada de ciberseguridad.** En cuanto a las medidas de ciberseguridad empleadas por su organización, el 82% respondió "firewalls" y "gateways de Internet", el 68% indicó "control de acceso", el 61% afirmó "protección contra malware", el 55% "auditorías" y el 50% afirmó "backup automatizado." **En lo que respecta a la gestión de riesgos, el 55% de los que respondieron a esa pregunta indicó que su organización implementó prácticas de gestión de riesgo de ciberseguridad y el 49% de los encuestados indicó que planeaba realizar una evaluación de riesgos**. Además, el 62% de los encuestados indicó que existe un rol dedicado dentro de su organización al responsable de la ciberseguridad.

Sin embargo, cuando se les preguntó si había un presupuesto específico para las medidas de ciberseguridad, **el 57% de los que respondieron indicó que no contaban con un presupuesto específico para las medidas de ciberseguridad.**. La ausencia de un presupuesto dedicado a menudo limita la capacidad de una organización de invertir en los recursos que necesita (es decir, tanto humanos como técnicos) para responder eficazmente a las amenazas cibernéticas. Sin embargo, entre los que tenían un presupuesto dedicado, un resultado positivo fue cuando se les preguntó si sus presupuestos aumentaron en el último año, el 59% de los que respondieron indicaron que sí.

A pesar de estos avances positivos, el 69% de los encuestados indicaron que han notado un aumento en el número de ataques a sus sistemas informáticos y/o redes en los últimos 12 meses. Además, **en términos de los activos que han sido blanco de ciberataques en los últimos 12 meses, el 61% de los encuestados identificó "datos", el 58% "perímetro de la red de la empresa", el 18% "sistemas de personal" y el 13% indicó "propiedad intelectual".** En relación con los métodos de ataque específicos, **el 76% de los que respondieron indicó "phishing", seguido por un 71% que identificó "malware" (por ejemplo, virus, gusanos, troyanos.)**. Otras actividades identificadas incluyen la detección de puertos (sin intrusión real) e ingeniería social. Curiosamente, algunos identificaron el ransomware y los ataques de denegación de servicio (distribuido), que cuando se consideran las CII, son amenazas críticas para su consideración en la gestión de riesgos y respuesta a incidentes.

En conclusión, el informe muestra que tanto los propietarios como los operadores de las infraestructuras críticas en América Latina y el Caribe han estado implementando medidas de ciberseguridad para responder al cambiante panorama de amenazas. Y es positivo y alentador ver que la industria responda a las amenazas de manera responsable Sin embargo, también es evidente que aún queda mucho por hacer a nivel nacional en toda la región. Los gobiernos deben estar más preparados, dada la creciente conectividad de sus servicios esenciales y desarrollar, promover e implementar incentivos, mejores prácticas y cualquier regulación necesaria para garantizar mayores niveles de seguridad en este espacio.

Perfil de los encuestados [20]

Cuando se les preguntó, el 15% de los encuestados indicó que eran operadores / propietarios de infraestructura críticos, el 60% identificados como operadores / propietarios de infraestructura de información crítica, y el 25% respondió "otros". La última categoría, "otros", incluía reguladores nacionales, comando de defensa cibernética, proveedores de servicios de Internet (ISP) y equipos de respuesta a incidentes de seguridad informática. A los efectos de esta pregunta, Infraestructura crítica se definió como sistemas y activos, ya sean físicos o virtuales, tan vital para el país que la incapacidad o destrucción de tales sistemas y activos tendría un impacto debilitante en la seguridad, seguridad económica nacional, seguridad pública nacional, o cualquier combinación de esas materias.

60% de los encuestados identificados como operador/propietario de infraestructura de información crítica

Del mismo modo, las industrias representadas cubrieron un amplio espectro de sectores De los 497 encuestados, 29% provenían del gobierno central, 19% de telecomunicaciones/TIC, 9% de banca y finanzas, y 7% representaban instalaciones de defensa/ ejército /defensa militar. Otros encuestados procedían de sectores de energía/electricidad (químico, nuclear, gas, petróleo, otros) y transporte (aire, mar, tierra) /logística/distribución, entre otros.

20. En el desarrollo de este informe, se realizó una encuesta para informar nuestros hallazgos. 881 personas respondieron a la encuesta, con un 11% de los encuestados del Caribe y un 89% de América Latina y una tasa promedio de finalización de 341 encuestados.

Cuando se trata del tipo de sistemas operados por los encuestados, cuando se les pregunta "¿Cuentan con un sistema de Control de Supervisión y Adquisición de Datos (SCADA / ICS)?", Que comprende sistemas que se usan para monitorear y controlar procesos industriales, el 80% respondieron que no.

¿A QUÉ SECTOR PERTENECE USTED?

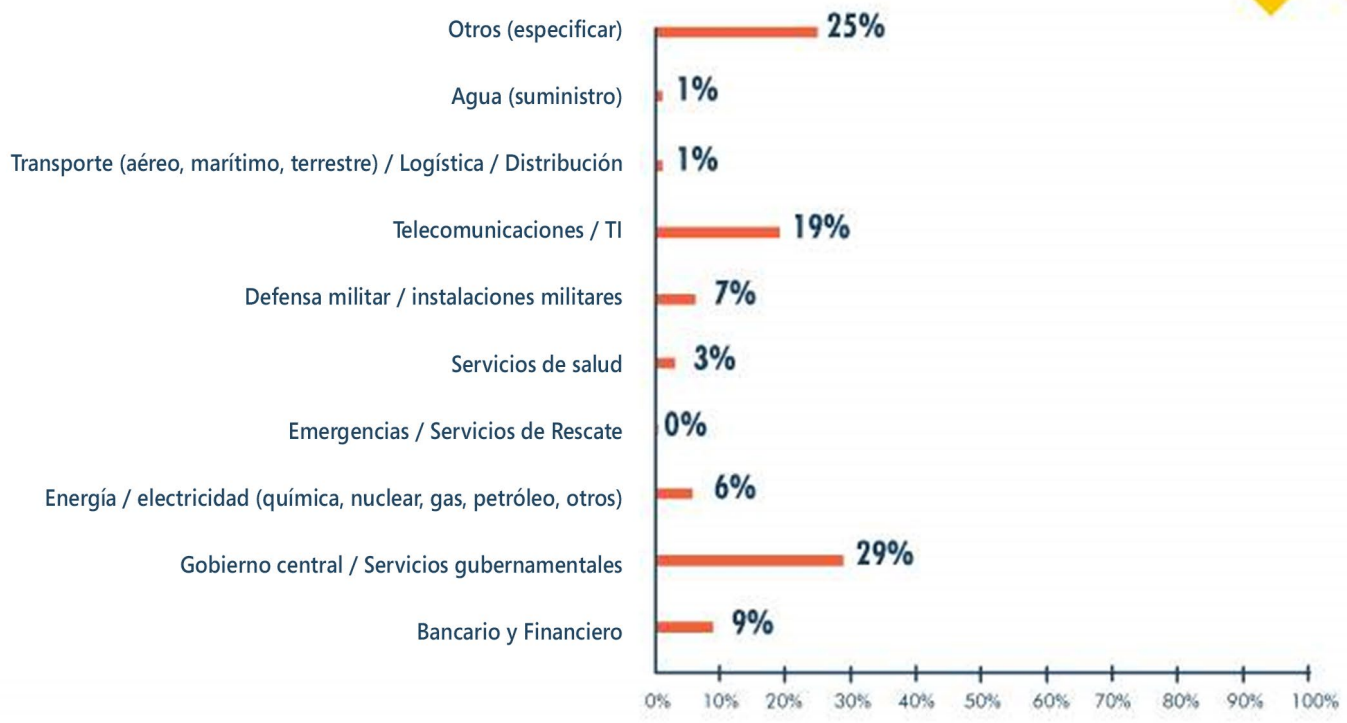


Figura 1 Total de entrevistados, n = 497

En términos del tamaño, el 42% de los encuestados indicó que tenían 1 a 500 empleados, mientras que el 58% indicó que tenían más de 500.[21]

21. Total de encuestados, n = 462

Capacidad de detectar incidentes cibernéticos

Un plan de respuesta eficaz a incidentes depende de tres capacidades básicas: ser capaz de proteger, detectar y responder a las amenazas. La protección tiene que ver con la prevención de incidentes, la detección consiste en identificar las amenazas de manera temprana y la respuesta es desalojar al atacante y restaurar los sistemas para mitigar los impactos de una brecha La capacidad de detectar un ataque en la red es particularmente importante, ya que cuanto antes se detecte un incidente, más pronto se podrán implementar medidas para reducir el impacto del mismo Es importante que las encuestas que analizan el tiempo que lleva detectar un ataque, una y otra vez descubran que la detección no suele ocurrir en minutos u horas, sino que a menudo se identifican meses después de la primera intrusión.

La detección puede ser incluso más difícil para la CII. A menudo se requiere que estén operativos en todo momento, dificultando el parchado y las actualizaciones regulares, las actualizaciones de emergencia irregulares son casi imposibles. Eso puede hacerlos más vulnerables y, por lo tanto, es crucial un software integrado de detección e intrusión que admita la detección precoz, así como contar con personal bien capacitado.

Cuando se les preguntó si su organización tenía la capacidad de detectar incidentes cibernéticos, el 53% de los encuestados indicó que tenían capacidades de detección implementadas y que monitoreaban la frecuencia con la que ocurrían los incidentes cibernéticos. En comparación, el 11% creía que su organización no tenía implementadas medidas de detección o ningún plan para implementarlas. El 35% de los encuestados planeaba invertir en herramientas apropiadas para permitir la detección de incidentes.

Los resultados fueron similares en todo el Caribe y América Latina, con el 59% de los encuestados del Caribe y el 53% de los encuestados de América Latina que indicaron que tenían capacidades de detección; y el 27% de los encuestados del Caribe y el 36% de los latinoamericanos indicaron que planeaban invertir en la implementación de medidas de detección.

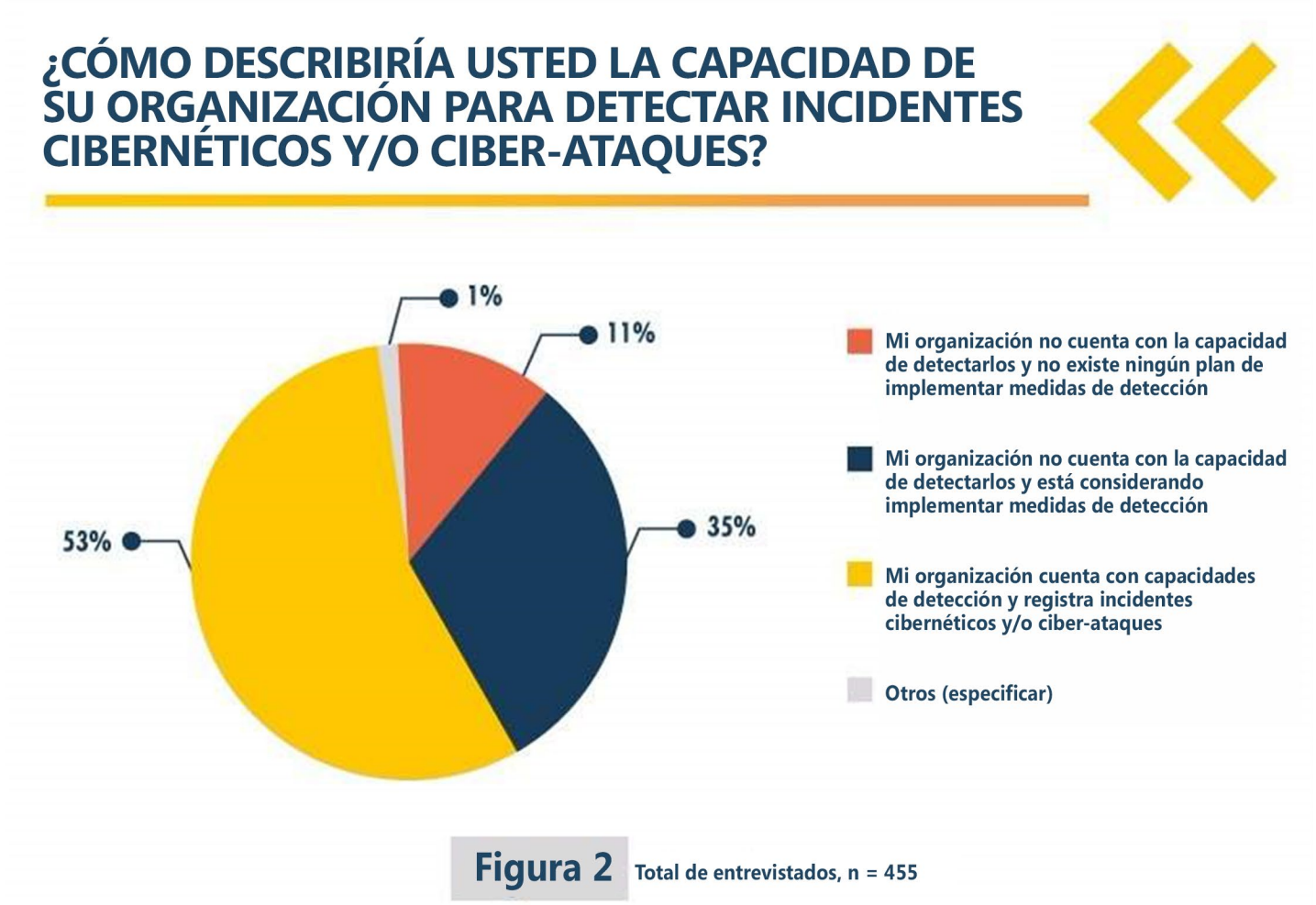


Figura 2 Total de entrevistados, n = 455

Como una pregunta de seguimiento, se preguntó a los encuestados si han detectado ataques contra los sistemas o redes informáticos de su organización en los últimos 12 meses. El 73% de los encuestados respondió afirmativamente.[22]

¿SU ORGANIZACIÓN A DETECTADO ATAQUES Y O INCIDENTES EN O CONTRA SUS SISTEMAS DE COMPUTACIÓN Y/O RED EN LOS ÚLTIMOS 12 MESES?

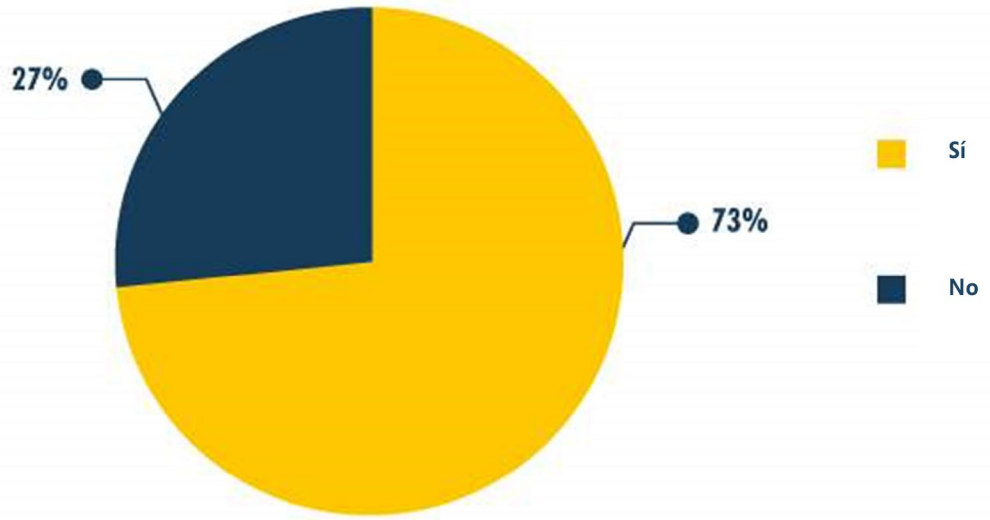


Figura 3 Total de entrevistados, n = 453

Frecuencia de incidentes cibernéticos

Según el Informe de Riesgos Mundiales del Foro Económico Mundial 2018,[23], los ciberataques se encuentran entre los principales riesgos mundiales, junto con los fenómenos meteorológicos extremos, los desastres naturales, el fraude o el robo de datos y el fracaso de la mitigación y la adaptación al cambio climático. Independientemente de la encuesta o informe que recopile, la frecuencia de incidentes cibernéticos parece estar aumentando, y dramáticamente. El Informe de Inteligencia de Seguridad de 2017 de Microsoft[24] mostró un aumento del 300% en los ataques a plataformas en la nube, mientras que otras encuestas mostraron un crecimiento similar de tres cifras en ransomware u otros ataques.

Nuestra encuesta mostró resultados similares. Al responder si las organizaciones detectaron un aumento en el número de ataques en sus sistemas informáticos y/o redes, casi el 69% de los encuestados indicó que notaron un aumento, con solo el 22% sin cambios y solo el 9% ellos han notado una disminución. Estos resultados muestran que invertir en ciberseguridad es fundamental.

22. Total de encuestados, n = 453

23. Informe de Riesgo Global del Foro Económico Mundial, 2018: www.reports.weforum.org/global-risks-2018/

24. Informe de Inteligencia de Seguridad de Microsoft, 2017: www.download.microsoft.com/download/F/C/4/FC41DE26-E641-4A20-AE5B-E38A28368433/Security_Intelligence_Report_Volume_22.pdf.

¿USTED HA OBSERVADO UN AUMENTO, REDUCCIÓN O NINGUNA ALTERACIÓN EN EL NÚMERO DE ATAQUES A LOS SISTEMAS DE COMPUTACIÓN Y/O RED DE SU ORGANIZACIÓN EN LOS ÚLTIMOS 12 MESES?

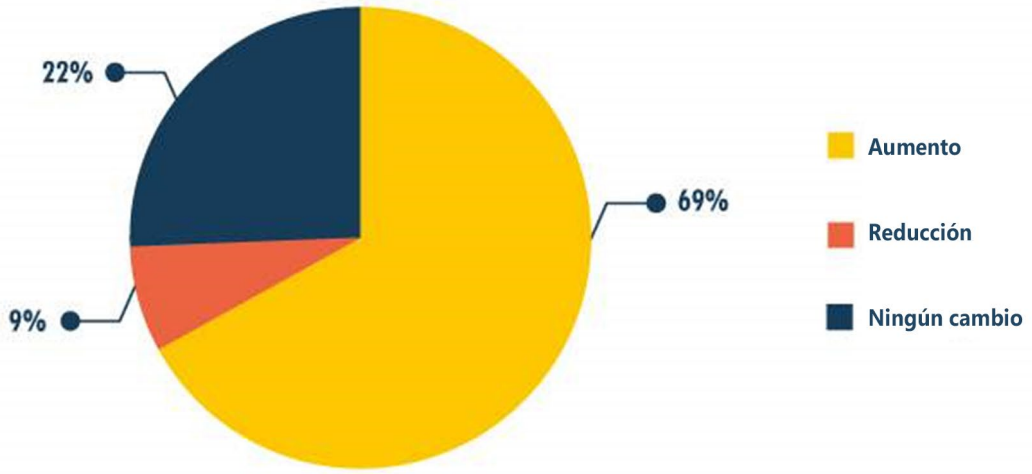


Figura 4 Total de entrevistados, n = 330

Tipos y métodos de incidentes cibernéticos

Las CII pueden ser objetivos particularmente atractivos para una amplia gama de actores maliciosos, desde delincuentes hasta otras naciones. Esto no es solo porque contienen información y datos valiosos, sino también porque sus operaciones son críticas para la seguridad nacional. Por lo tanto, los actores malintencionados pueden atacarlos no con la intención de robar, sino con la intención de sabotear sus operaciones. En 2017, por ejemplo, un vendedor de seguridad[25]identificó una campaña basada en ataques cibernéticos, ahora conocida como Dragonfly 2.0, que tenía como objetivo instalaciones de energía en Europa y América del Norte. El grupo Dragonfly parece estar interesado en aprender cómo funcionan las instalaciones de energía y también acceder a los sistemas operativos, en la medida en que el grupo ahora tiene la capacidad de sabotear o controlar estos sistemas en caso de que decida hacerlo.

Por lo tanto, los riesgos para las CII pueden ser mayores y más complejos de lo que sería el caso con cualquier otra entidad del sector privado. La probabilidad de que los actores sofisticados se dirijan a ellos es mayor, dado el papel vital que desempeñan en la sociedad. Además de las amenazas que ya hemos destacado, a medida que el terrorismo global continúa evolucionando y estos grupos obtienen mayores capacidades en línea, también es probable que se centren en dónde podrían tener el mayor impacto adverso en las economías nacionales y la seguridad: es probable que las CII entre sus objetivos principales.

Si bien nuestra encuesta no buscó atribuir los ataques a actores particulares, hemos tratado de determinar dónde se originó la maroría de loss incidentes cibernéticos. A los encuestados se les preguntó qué tipo de han experimentado en los últimos 12 meses, con las opciones dadas incluyendo amenazas internas, fuerza mayor, falla técnica, y ciberataque. La gran mayoría de los encuestados (54%) destacó los ataques externos a sus activos cibernéticos, el 24% indicó que la falla técnica era culpa del incidente, el 18% culpó a los incidentes de ciberseguridad interna y el 11% indicó fuerza mayor.

25. Symantec, Dragonfly: Sector energético occidental dirigido por sofisticado grupo de ataque www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks

¿CUÁLES DE LOS SIGUIENTES INCIDENTES LE HAN OCURRIDO EN LOS ÚLTIMOS 12 MESES? (MARQUE TODOS LOS CORRESPONDIENTES)

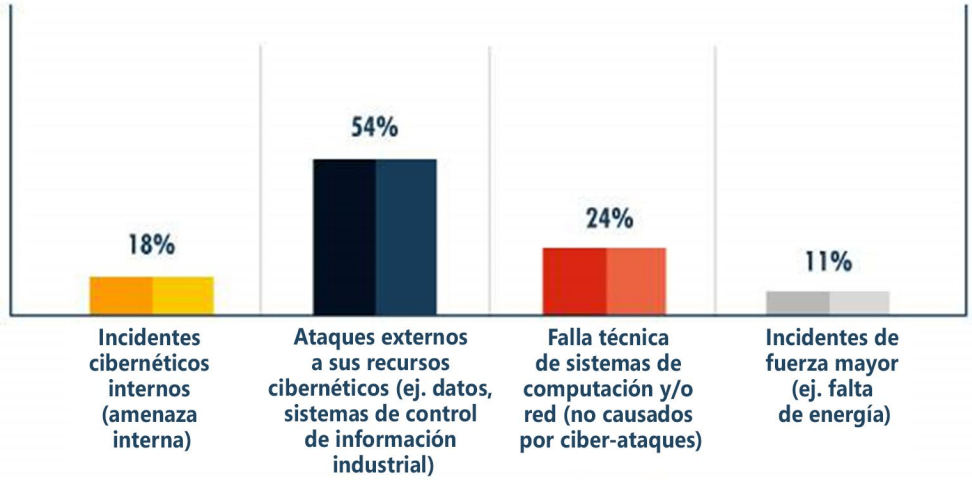


Figura 5 Total de entrevistados, n = 317

Cuando se les preguntó qué métodos se usaron en el ataque, el 76% de los encuestados indicó phishing y el 71% varios ataques de malware. Otros métodos observados incluyen la detección de puertos (sin intrusión real) y la ingeniería social. El 46% identificó ataques de ransomware y 36% (distribuido) de denegación de servicio. Si bien el phishing en particular puede asociarse con ataques sofisticados y persistentes, los dos últimos son particularmente importantes de mencionar en el contexto de CII, ya que es probable que resulten en una serie de interrupciones en el servicio.

A RESPECTO DE LOS CIBER-ATAQUES ¿CUÁLES FUERON LOS MÉTODOS UTILIZADOS CONTRA SU ORGANIZACIÓN?

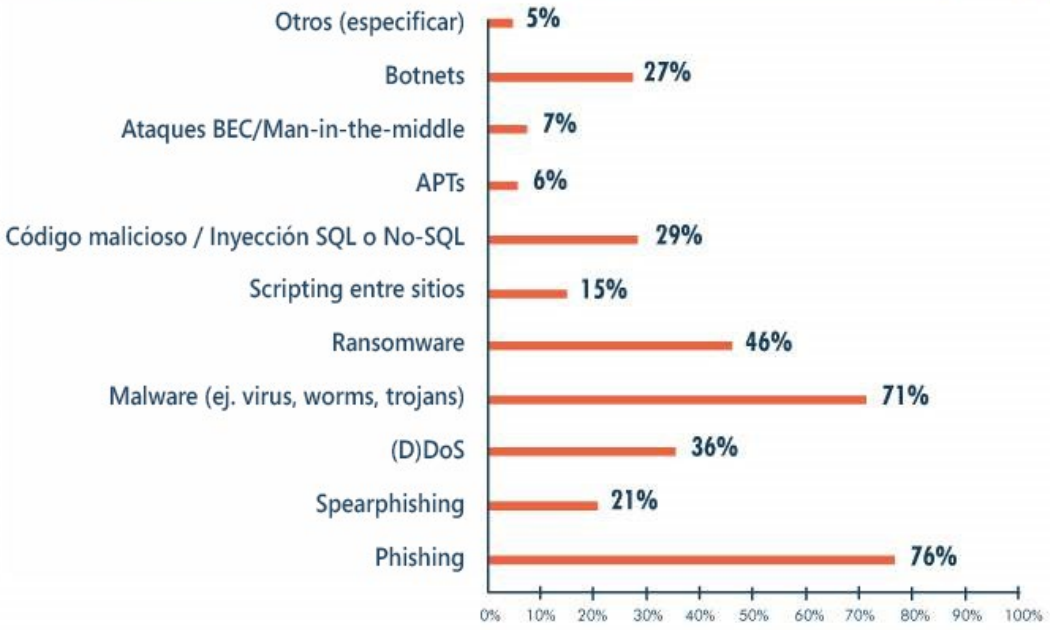


Figura 6 Total de entrevistados, n = 311

Sofisticación de ataques cibernéticos

Un ciberataque sofisticado empleará una variedad de herramientas y tácticas efectivas: fraudes de phishing, ataques de malware y spyware, vulnerabilidades del navegador y del software, acceso a través de dispositivos perdidos y robados, e ingeniería social. Las herramientas de seguridad tradicionales se han centrado principalmente en la prevención. Sin embargo, la sofisticación y la escala de las amenazas persistentes avanzadas (APT) significa que, si bien prevenir una brecha es ideal y una parte fundamental de las operaciones, no es realista centrarse exclusivamente en la protección. Las organizaciones deben reconocer que las brechas son difíciles de detectar y suponer que ya se ha producido antes.

De hecho, cuando se preguntó a los encuestados si los ciberataques en sus sistemas se estaban volviendo más sofisticados, el 62% de los encuestados indicó que sí, y el 30% indicó que no estaban seguros. Una posible explicación de por qué los encuestados pueden no estar seguros del nivel de sofisticación es que, a nivel mundial, algunos de estos ataques son cada vez más difíciles de detectar. Además, es posible que muchos no tengan las herramientas y capacidades para medir el progreso a lo largo del tiempo, dada la proporción bastante grande de encuestados que al inicio indicaron tener capacidades de detección limitadas. Como se indicó anteriormente, rastrear un incidente a menudo requiere los recursos técnicos y humanos adecuados y, aun así, la detección no está garantizada.

Figura 7 Total de entrevistados, n = 320

Impacto de los incidentes cibernéticos

Como principio básico de la gestión del riesgo de ciberseguridad, una organización no solo debería ser capaz de detectar incidentes cibernéticos, sino también tener la capacidad de evaluar su impacto potencial antes de tiempo y así poder priorizar activos que son más críticos. Del mismo modo, es importante que las organizaciones identifiquen, analicen y aprendan de las intrusiones que se producen. Este enfoque asegurará que puedan evitar cometer los mismos errores en el futuro, haciendo que su organización sea más resistente en el proceso.

En respuesta a la pregunta: "¿Qué le sucedió a su organización como resultado de los ataques experimentados?", El 44% de los encuestados indicó que no sucedió nada, mientras que el 33% indicó que experimentaron alguna interrupción comercial (tiempo de inactividad). El 22% de los encuestados indicó que los atacantes eran capaces de ganar el acceso no autorizado y/o el robo de información confidencial o

clasificada, y el 17% indicó que hubo cierta modificación, destrucción o supresión de datos o información. Otras áreas identificadas incluyen daños a la reputación y secuestro de datos.

¿QUÉ LE HA OCURRIDO A SU ORGANIZACIÓN COMO RESULTADO DE LOS ATAQUES SUFRIDOS? (MARQUE TODOS LOS CORRESPONDIENTES)

Figura 8 Total de entrevistados, n = 303

Causa de intrusión

Comprender qué provocó el incidente es fundamental para la capacidad de la organización para aprender del pasado y aumentar su resiliencia cibernética. En respuesta a la pregunta, "¿Cuáles son las 5 principales causas que podrían haber originado los ataques?", Las 5 principales causas en orden de mayor clasificación fueron:

1. Falta de conciencia de ciberseguridad entre los empleados
2. Falta de habilidades de seguridad
3. Mala o inadecuada gestión de parches
4. Controles de acceso inadecuados
5. La falta de presupuesto para apoyar las iniciativas de seguridad de las aplicaciones y los problemas de la aplicación de la seguridad dentro de la organización están empatados.

Las otras áreas identificadas incluyeron desarrollo de código inseguro, metodologías de prueba deficientes o inadecuadas e implementación y configuración deficientes.[26] Estos hallazgos están en consonancia con muchas de estas encuestas, incluido el Informe de Seguridad de Inteligencia de Microsoft mencionado anteriormente, y subrayan la necesidad de una seguridad básica de ciberseguridad en todas las organizaciones. Además, muchas prácticas recomendadas destacan la gestión de parches y los controles de acceso como elementos vitales para proteger a cualquier entidad; de hecho, algunos han afirmado que su implementación puede reducir los ataques cibernéticos hasta en un 90%. El esquema esencial de seguridad cibernética del Reino Unido[27], por ejemplo, destaca esas dos mejores prácticas, pero también asegura la conexión a Internet, dispositivos y software, y la implementación de software antivirus. Asimismo destacan la importancia de dedicar recursos específicos, tanto humanos como monetarios y técnicos, a la ciberseguridad, asegurando que siga siendo una prioridad continua.

26. Un ejemplo de medidas de seguridad cibernética es el Water ISAC 2015 10 Medidas básicas de ciberseguridad, a las que se accede en: www.ics-cert. us-cert.gov/sites/default/files/ documents/10_Basic_Cybersecurity_ Measures-WaterISAC_June2015_ S508C.pdf

27. Ciberseguridad esencial: www.cyberessentials.ncsc.gov.uk

DE LA SIGUIENTE LISTA ¿CUÁLES SON LAS 5 CAUSAS PRINCIPALES DE LOS ATAQUES OCURRIDOS?

Figura 9 Total de entrevistados, n = 288

Comprender los activos de la organización

Otro componente importante de la gestión del riesgo de ciberseguridad es la necesidad de una comprensión clara de las motivaciones y capacidades de los actores amenazados, posibles vías de ataque o explotación, así como los activos, funciones o información clave que podrían ser atacados. Un claro análisis y comprensión de las amenazas, así como de los riesgos y vulnerabilidades, es esencial para que una organización pueda priorizar la asignación de recursos presupuestarios y de otro tipo necesarios para su protección.

Cuando se preguntó "¿Qué activos cibernéticos ha identificado su organización como críticos?", El 89% de los encuestados identificó los datos como críticos, el 57% destacó el perímetro de la red de la empresa y el 41% de los sistemas de personal. Basándose en la pregunta anterior, cuando se les preguntó qué activo era el objetivo de un ciber-ataque en los últimos 12 meses, 61% de los encuestados identificó los datos, 58% el perímetro de la red de la empresa, 18% de los sistemas de personal, y 13% de la propiedad intelectual. Estos resultados son útiles, ya que pueden indicar qué tipo de información buscaban los atacantes, resaltar los activos organizacionales más vulnerables y formar una base para el desarrollo de un marco de gestión de riesgos.

¿CUÁLES RECURSOS DIGITALES DE SU ORGANIZACIÓN HA IDENTIFICADO COMO CRÍTICOS? (MARQUE TODOS LOS CORRESPONDIENTES)

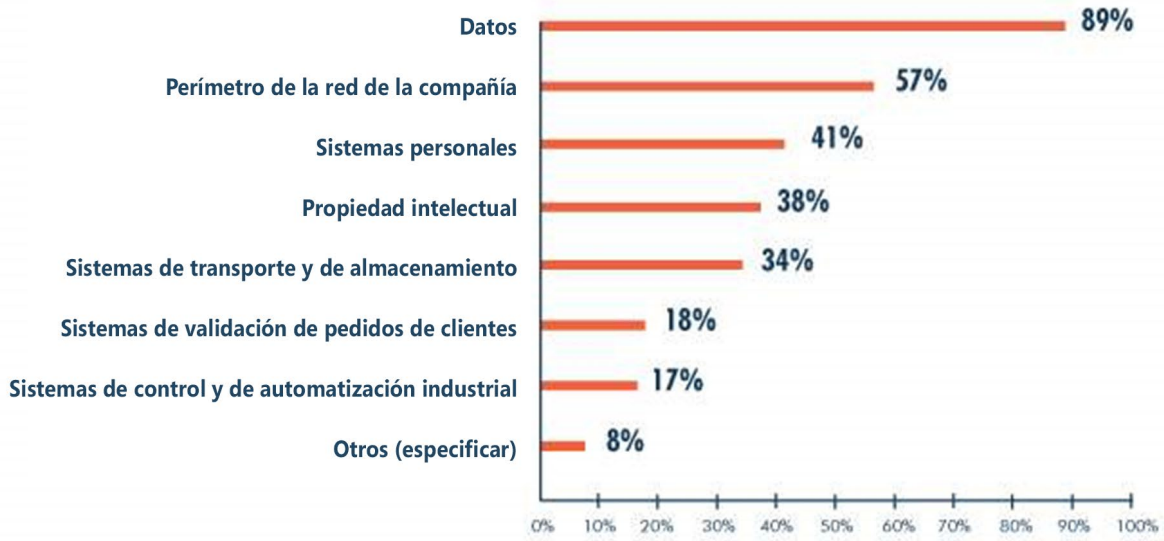


Figura 10 Total de entrevistados, n = 321

¿CUÁLES DE LOS SIGUIENTES RECURSOS DE SU ORGANIZACIÓN HAN SIDO BLANCO DE CIBER-ATAQUES EN LOS ÚLTIMOS 12 MESES? (MARQUE TODOS LOS CORRESPONDIENTES)

Figura 11 Total de entrevistados, n = 360

Medidas de ciberseguridad

Anteriormente en la encuesta nos enfocamos en la detección de incidentes; Sin embargo, otras medidas son igualmente importantes para mejorar la ciberseguridad de las organizaciones. Numerosas organizaciones han presentado ejemplos de los que podrían ser, los más frecuentes son: proteger su conexión a Internet, proteger sus dispositivos y software, controlar el acceso a sus datos y servicios, protegerse de virus y otro malware, y mantener sus dispositivos y software actualizados.[28]

Cuando se le preguntó "¿Qué tipo de medidas técnicas de ciberseguridad tiene su organización en relación con los sistemas de información de infraestructura crítica (CII) ?", la mayoría de los encuestados destacaron los firewalls de límite y las puertas de enlace de Internet (82%). Otras medidas incluyeron control de acceso (68%), protección contra malware (61%), auditorías (55%) y backup automático (50%).

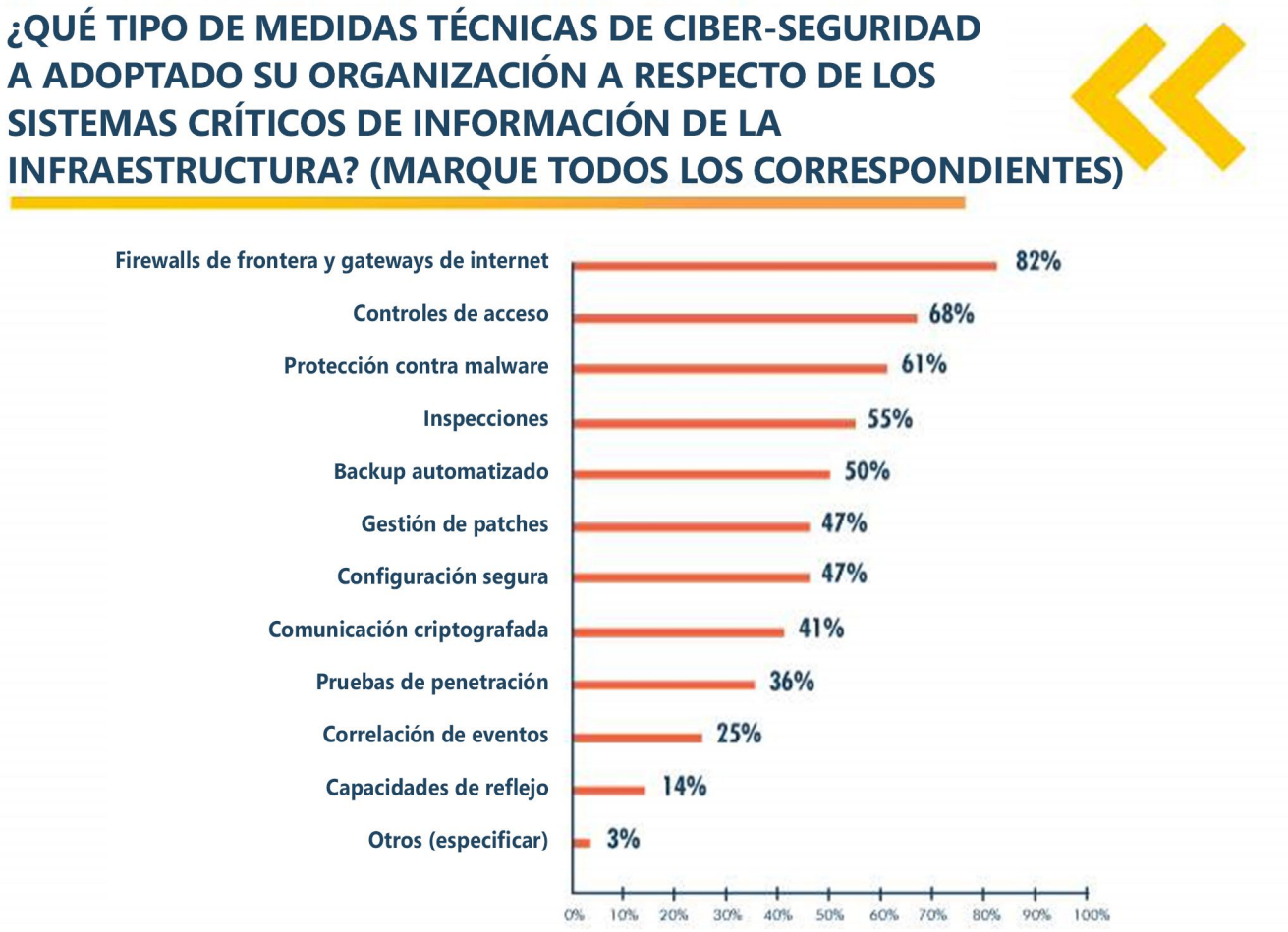


Figura 12 Total de entrevistados, n = 404

Como se indicó anteriormente en el informe, contar con marcos, directrices y procedimientos claros son consideraciones clave para el desarrollo de una política CIIP sostenible. Cuando se les preguntó: "¿Tiene su organización políticas y/o planes de seguridad cibernética?", Algunos de los aspectos más destacados fueron que el 48% de los encuestados indicó que tenían capacitación en concientización sobre ciberseguridad para los empleados, el 46% indicó que contaban con un plan de recuperación ante desastres. El 42% indicó que tenía un plan de respuesta a incidentes cibernéticos, y el 41% indicó que tenía una estrategia documentada de ciberseguridad.

28. Un ejemplo de esto es Cyber Essentials de Reino Unido www.cyberessentials.ncsc.gov.uk/ or UK government's 10 steps to cybersecurityhttps://www.ncsc.gov.uk/guidance/10-steps-cyber-security

¿SU ORGANIZACIÓN CUENTA CON POLÍTICAS Y/O PLANES DE CIBER-SEGURIDAD?

Figura 13 Total de entrevistados, n = 392

Cuando se les solicitó identificar los "estándares o marcos reconocidos" que su organización utiliza para evaluar y mitigar el riesgo cibernético, los encuestados identificados con mayor frecuencia incluyeron COBIT[29], ISO[30], IEEE[31], IEC[32], ITIL[33], OWASP[34], SANs[35] y NIST, mencionado en otra parte del documento.

En respuesta a si tienen un rol específico para abordar la seguridad cibernética, la mayoría de los encuestados indicó "sí" (62%), y solo el 38% indicó "no". Además, cuando se le preguntó qué nivel supervisa los esfuerzos de ciberseguridad dentro de su organización, el 42% indicó que su departamento de TI y el 19% el departamento de seguridad de la información, con solo el 13% identificando el C-Suite. Curiosamente, solo el 4% indicó que este papel fue eternalizado a un consultor/contratista externo. Sin embargo, esta realidad obliga a considerar a qué nivel deben abordarse los problemas de ciberseguridad. Por ejemplo, asignar esta tarea solo a TI aisla otras áreas clave dentro de una organización que deberían participar en la gestión de riesgos de sus operaciones. Por el contrario, los departamentos tradicionales de gestión de riesgos pueden no tener las habilidades requeridas.

29. Objetivos de control para información y tecnologías relacionadas (COBIT): www.isaca.org/COBIT/Documents/COBIT-5-for-Risk-Preview_res_eng_0913.pdf

30. Organización de estándares internacionales (ISO): www.iso.org

31. Instituto de Ingenieros Eléctricos y Electrónicos: www.theinstitute.ieee.org/technology-topics/cybersecurity/ieee-standards-on-cybersecurity

32. Comisión Electrotécnica Internacional: www.iec.ch/about/activities/standards.htm

33. Biblioteca de infraestructura de tecnología de la información: www.bmc.com/guides/itil-information-security-management.html

34. Proyecto abierto de seguridad de aplicaciones web: www.owasp.org/

35. www.sans.org

¿CUÁL ES EL NIVEL QUE SUPERVISA LOS ESFUERZOS DE CIBER-SEGURIDAD DE SU ORGANIZACIÓN?

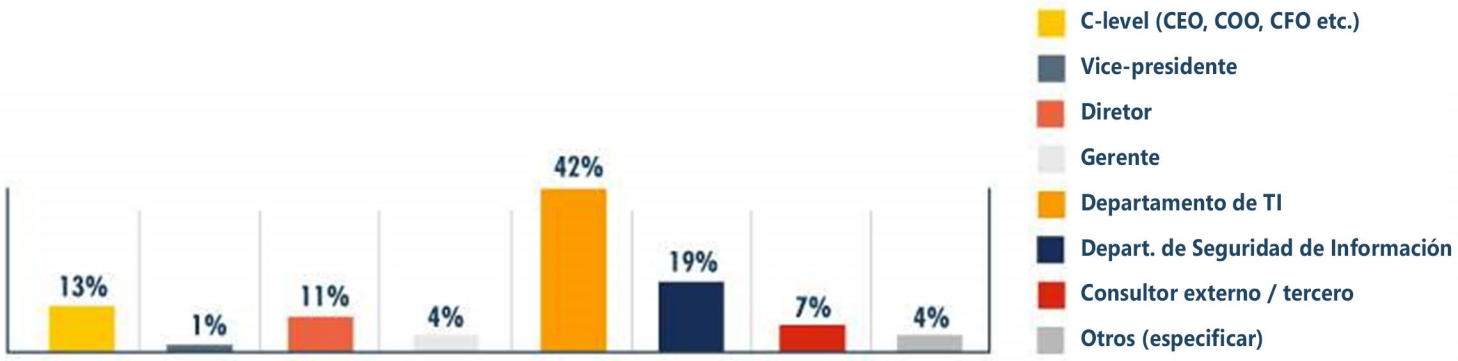


Figura 14 Total de entrevistados, n = 366

Presupuestos dedicados

La guía de gestión de riesgos resalta consistentemente la importancia de la comunicación entre las organizaciones, tanto horizontal como verticalmente. Sin embargo, la gestión del riesgo de ciberseguridad es un tema relativamente nuevo y técnico para muchos gerentes, directores y juntas directivas de empresas, por lo que pueden tener problemas con el compromiso vertical y de la organización en el tema. La comprensión de la gestión del riesgo de ciberseguridad entre las audiencias mediante el uso de un lenguaje común permite a las partes interesadas comunicarse de manera significativa sobre el panorama del riesgo, dando lugar a decisiones más informadas sobre cómo priorizar y gestionar los riesgos, y la continuidad en la estrategia de seguridad, planificación e inversiones. Si los ejecutivos pueden entender lo que los profesionales quieren lograr y revisar periódicamente el progreso en un conjunto relativamente consistente de resultados de seguridad deseados, entonces podrán comprender mejor el valor estratégico de los recursos para cumplir con los objetivos o para abordar las brechas.

Cuando se preguntó a los encuestados si existía un presupuesto específico para las medidas de seguridad cibernética, el 57% de los encuestados indicó "No". La ausencia de un presupuesto dedicado a menudo limita la capacidad de una organización de invertir en los recursos que necesita (es decir, tanto humanos como técnicos) para responder eficazmente a las amenazas cibernéticas.

Figura 15 Total de entrevistados, n = 359

Sin embargo, comparativamente, cuando se les preguntó si su presupuesto para ciberseguridad había aumentado en el último año, el 59% de los que encuestados indicó que había aumentado. Como seguimiento, se les preguntó "¿su organización mide la efectividad de su presupuesto de ciberseguridad?", El 57% indicó que sí. Este es un resultado positivo del análisis, ya que demuestra que los encuestados no solo asignan medidas de seguridad cibernética, sino que también evalúan la efectividad y hacen ajustes en consecuencia (por ejemplo, los que vieron un aumento positivo en los últimos 12 meses).

Gestión de riesgos

Muchas medidas, como las identificadas anteriormente, están orientadas a mitigar los riesgos y garantizar la resiliencia de la infraestructura crítica. La gestión de riesgos, a los efectos de esta encuesta, implica la identificación, análisis y evaluación de riesgos potenciales en un sistema o riesgos relacionados con la ciberseguridad de forma continua con el objetivo de identificar riesgos tolerables e implementar medidas de mitigación para eliminar o reducir el potencial de riesgo. Sin embargo, si bien las partes individuales de la implementación de iniciativas de gestión de riesgos podrían estar en marcha, un número mucho menor de organizaciones en esta encuesta han adoptado un enfoque integral.

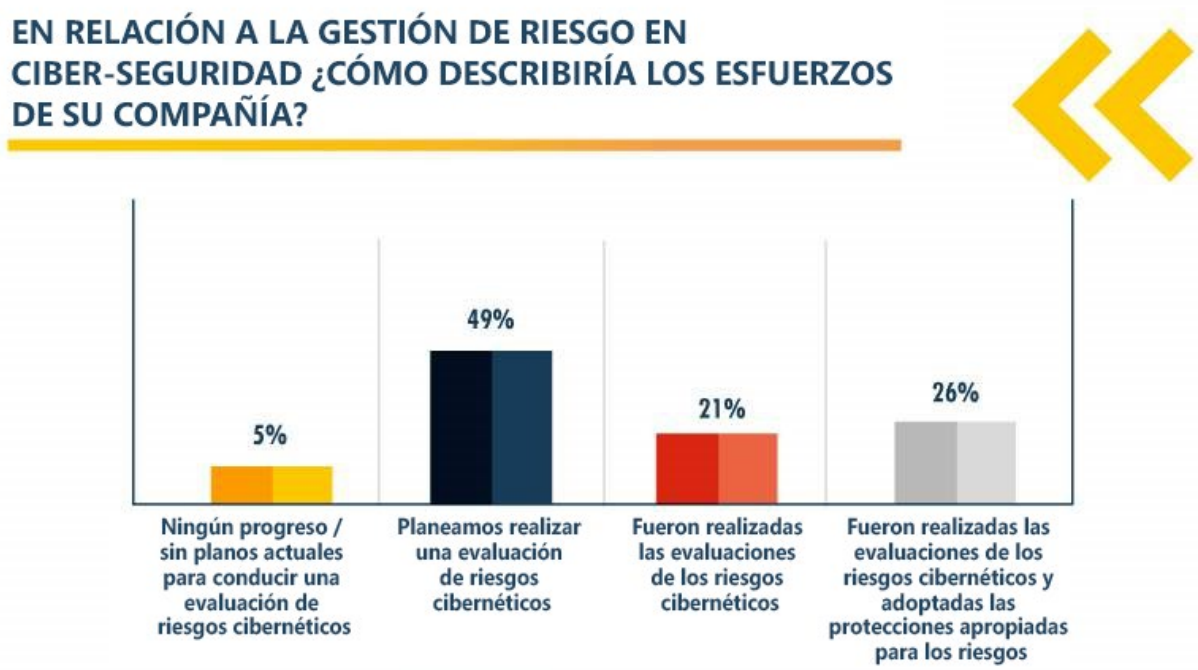


Figura 16 Total de entrevistados, n = 222

Cuando se les preguntó, "¿Su organización implementa prácticas de gestión de riesgo de ciberseguridad?", El 55% de los encuestados indicó "sí" y el 45% respondió "no". Sin embargo, en la siguiente pregunta "En relación con la gestión del riesgo de ciberseguridad, ¿cómo describiría los esfuerzos de su compañía?", Las respuestas fueron más alentadoras, el 49% de los encuestados indicó que planeaban realizar una evaluación de riesgos, el 26% indicó que se habían realizado evaluaciones y existían salvaguardas de riesgo adecuadas, el 21% indicó que se habían realizado evaluaciones cibernéticas y solo el 5% de los encuestados indicó que no se habían realizado progresos/no se habían establecido planes para llevar a cabo una evaluación de riesgos cibernéticos.

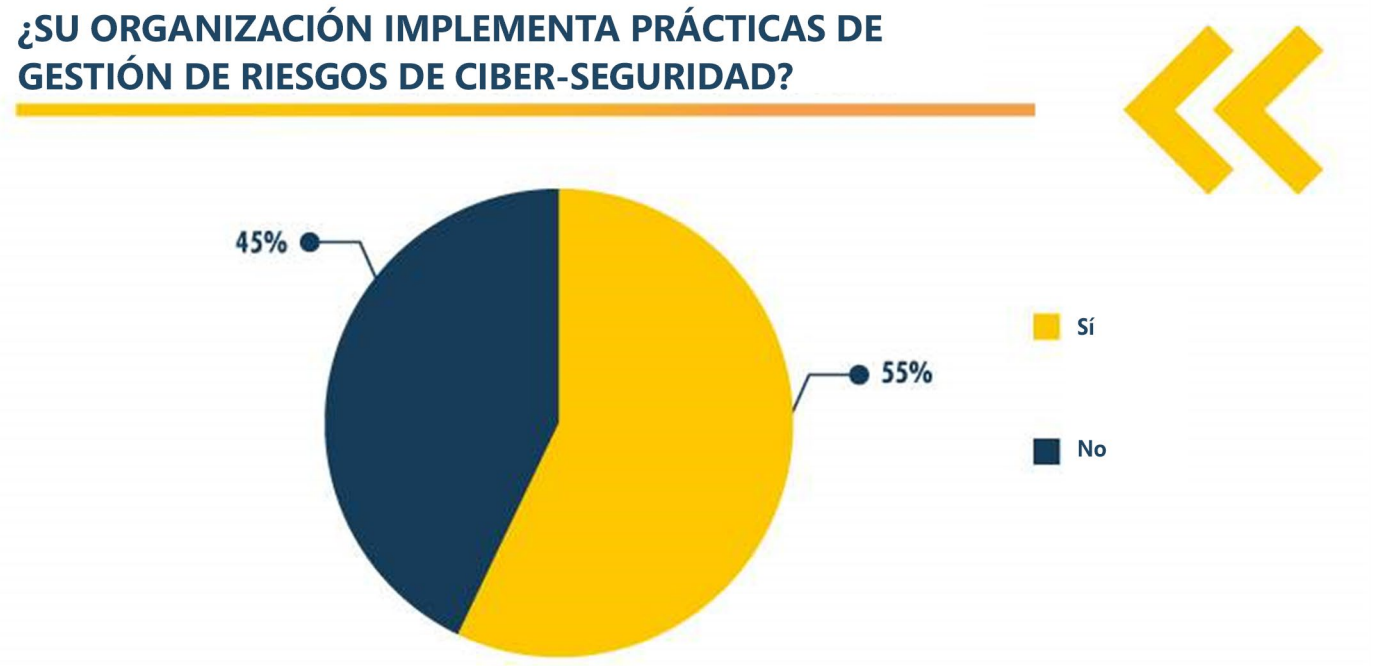


Figura 17 Total de entrevistados, n = 402

Coordinación a nivel nacional

Los gobiernos abordan la infraestructura crítica, las ciberamenazas y las evaluaciones de riesgos de forma muy diferente que el sector privado. Los políticos consideran la infraestructura crítica que se compone de sistemas y servicios monolíticos, mientras que el sector privado examina los elementos básicos dentro de su control directo y sus obligaciones contractuales para entregar servicios. Como era de esperar, los gobiernos entienden las amenazas a la infraestructura crítica a través de escenarios de alta gama que podrían comprometer la postura o la disposición de las capacidades de seguridad nacional y los activos que se necesitan para la estabilidad y la proyección de la fuerza.

A menudo se requiere un liderazgo designado dentro del gobierno para coordinar con éxito a múltiples agencias en el proceso de desarrollo de una estrategia CII. Sin embargo, en respuesta a la pregunta: ¿Su país tiene una agencia gubernamental responsable de la Protección de Infraestructura de Información Crítica?, solo el 49% de los encuestados de la región respondió "sí"[36]. Según los encuestados, las responsabilidades asignadas a esta agencia variaron, y la función más identificada fue la emisión de directrices y recomendaciones (69%), seguidas de un punto de contacto para el intercambio de información (56%).

36. Total de encuestados, n = 356

¿CUÁLES SON SUS RESPONSABILIDADES? (MARQUE TODOS LOS CORRESPONDIENTES)

Figura 18 Total de entrevistados, n = 175

Teniendo en cuenta que la mayoría de los encuestados en la pregunta anterior identificó el papel de la agencia nacional como el punto de contacto para la información, cuando se le preguntó "¿Existe una discusión/diálogo/cooperación entre el gobierno y el sector privado sobre la resiliencia cibernética de los sistemas de infraestructuras críticas (información)?, el 32% de los encuestados indicó que no estaba seguro, el 31% indicó que sí y nuestra organización participa, el 20% indicó que sí, pero su organización no participa y el 16% respondió que no.

Además, cuando se les preguntó: "¿Qué tipo de mecanismos de cooperación existen?", El 69% indicó grupos de trabajo, el 64% indicó diálogo informal y/o la cooperación, el 42% indicó alianzas público-privadas y solo el 3% indicó otras. Esto es indicativo de buenas prácticas en la región en este sentido, ya que la protección de la infraestructura crítica requiere prácticas exitosas de intercambio de información que beneficien a todas las partes interesadas.

¿QUÉ TIPOS DE MECANISMOS DE COOPERACIÓN ESTÁN DISPONIBLES? (MARQUE TODOS LOS CORRESPONDIENTES)

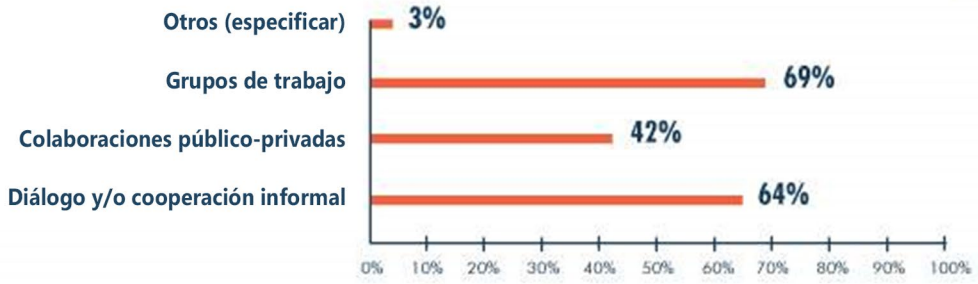


Figura 19 Total de entrevistados, n = 180

En términos de buenas prácticas a nivel nacional, cuando se les preguntó si eisten incentivos para que las CII implementen medidas de seguridad, el 78% indicó que no había incentivos vigentes, el 13% indicó que había directrices oficiales vigentes, y solo el 8% indicó que había incentivos financieros. A continuación, cuando se le preguntó, "¿Su país cuenta con una regulación específica del sector relacionada con la Protección de Infraestructuras Críticas de Información?' El 61%[37] de los encuestados respondió "no". Además, cuando se les preguntó si había algún marco de certificación (voluntario) con respecto a la seguridad cibernética en uso en su sector y su país, el 57%[38] de los que respondieron indicó "no". Finalmente, cuando se les preguntó si había algún ejercicio de ciberseguridad en su país o sector, la mayoría de los encuestados indicó que "no", con solo el 24% que indicó "sí" y el 27% que indicó "sí", pero no participamos".

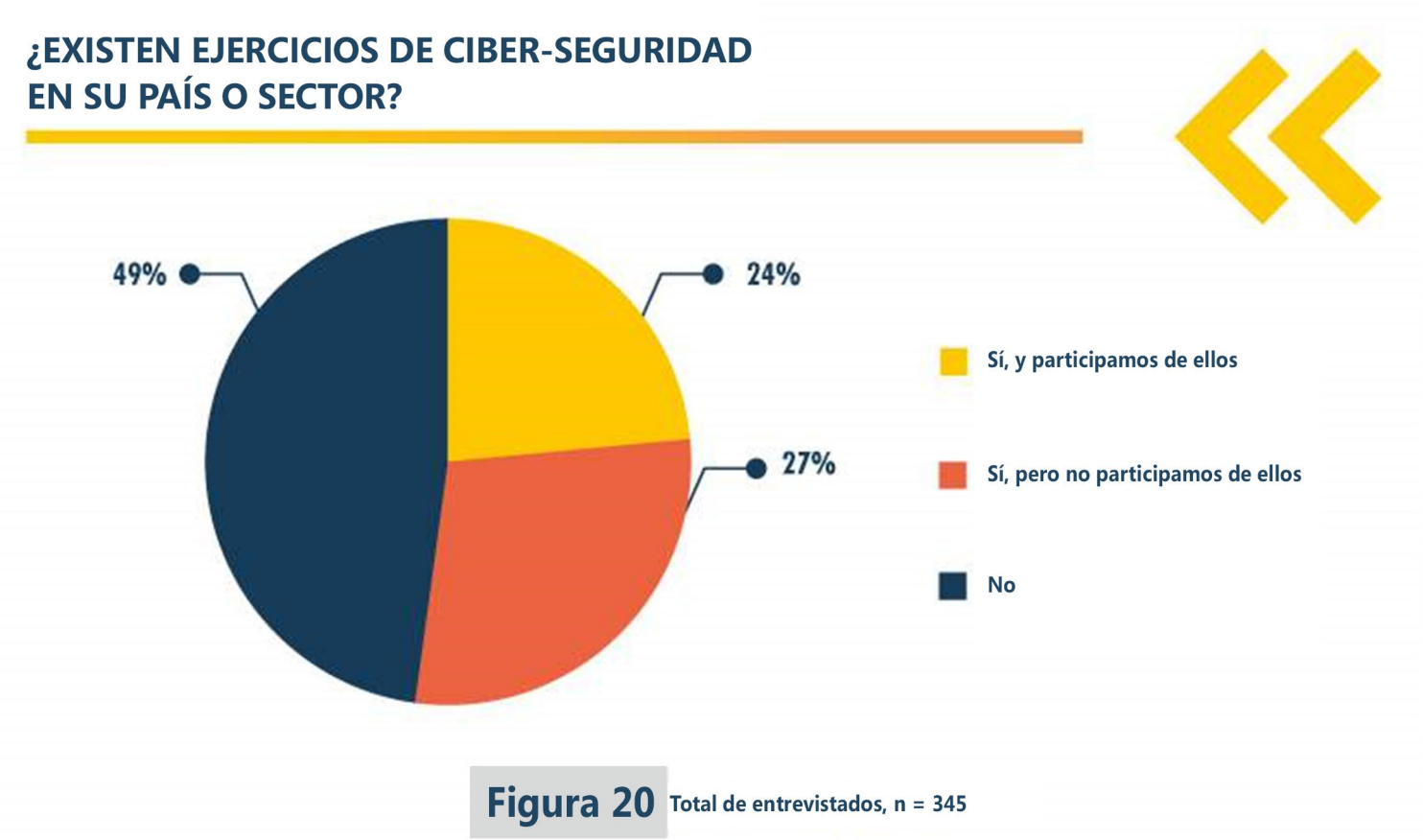


Figura 20 Total de entrevistados, n = 345

37. Total de encuestados, n = 352

38. Total de encuestados, n = 349

Parte 2

EXPERIENCIAS Y BUENAS PRÁCTICAS - ESTUDIOS DE CASO

EXPERIENCIAS Y BUENAS PRÁCTICAS - ESTUDIOS DE CASO

Lecciones aprendidas del desarrollo e implementación de la política de seguridad de la tecnología de la información (TI) en los Sistemas de Control Industrial (ICS) del Canal de Panamá

Escrito por: Raúl Millán, Supervisor Especialista en Tecnología de la Información (Seguridad), Unidad de Seguridad de Sistemas - TIGU, Vicepresidente Ejecutivo de Tecnología y Tecnología de la Información, Canal de Panamá

Resumen:

El proceso de desarrollo e implementación de una política general de seguridad de TI, destinada a ser seguida por una unidad de negocio no relacionada con TI, siempre es un desafío, debido a esta desconexión que típicamente existe entre TI y la empresa. En el caso del Canal de Panamá, el "negocio" se define como cualquier cosa que tenga una relación directa con un barco que transita por las aguas del Canal. Esto sitúa al sector de TI aún más lejos del "negocio", clasificándolo como una unidad de soporte, a pesar de que las operaciones del Canal dependen continuamente de los sistemas de TI, en forma de ICS (Sistemas de control industrial).

Origen:

En 2014, el Canal de Panamá reconoció la importancia de las unidades de negocios generadoras de ingresos y los riesgos asociados con el uso de ICS. Como resultado, se acordó que se necesitaba una política de seguridad de TI para proporcionar contexto y directrices a las unidades de negocios marítimas, de agua y energía, en particular, a todos los grandes usuarios de ICS en sus operaciones diarias.

Estas tres unidades tienen diferentes objetivos comerciales, todos alineados con la generación de ingresos. La unidad de operaciones marítimas está a cargo de todo lo relacionado con los tránsitos de buques. La unidad de energía tiene la tarea de generar la electricidad requerida para operar las operaciones marítimas del Canal, así como de gestionar su producción, lo que incluye vender cualquier exceso de capacidad al mercado nacional de energía. La unidad de negocios de agua tiene la responsabilidad de gestionar el suministro de agua, que incluye el agua necesaria para el tránsito marítimo, así como el agua utilizada para el consumo humano. Esto se hace vendiendo agua dulce de los lagos al Instituto Nacional del Agua (IDAAN) o procesando el agua a través de una de las instalaciones de procesamiento de agua que posee y opera el Canal.

Si bien estas tres unidades actualmente representan las principales actividades generadoras de ingresos del Canal, se planean más para el futuro para garantizar una gestión rentable del mismo. Ejecutar las operaciones diarias sin una guía clara para asegurar sus sistemas de TI simplemente no es una opción.

Análisis:

El requisito de desarrollar una política de seguridad informática que se aplique a las unidades de negocios generadoras de ingresos que diseñen, implementen y operen sistemas de control industrial dentro del Canal de Panamá, fue un hallazgo contenido en una auditoría interna; aunque la necesidad de una política de este tipo había sido identificada mucho tiempo antes de que el requerimiento fuera formalizado por los auditores.

El principal problema que la política trató de abordar es la falta de claridad en lo que respecta a los diferentes roles y responsabilidades relacionadas con el funcionamiento del entorno de ICS. Desde el punto de vista de TI no hubo claridad con respecto a los requisitos técnicos (no participación en el proceso de compra), ninguna capacitación estratégica (poca participación en la transferencia de conocimiento), falta de control del diseño (los diseños generalmente no consideran los controles básicos de seguridad de TI), y las expectativas de apoyo injustas de la unidad de negocios (se considera que TI es responsable y responsable del soporte). Desde la perspectiva empresarial, la TI solo se consideró como un proveedor de soporte, aunque no siempre sabía lo que la unidad de negocio había elegido implementar.

En este escenario, se ha creado una zona gris de roles y responsabilidades desconocidas en la que ninguna de las dos áreas, TI y Operaciones, se siente responsable del mantenimiento, las operaciones y la seguridad del ISC. El objetivo principal de la política de seguridad de ICS es comprender tanto el sector de TI como el de operaciones, cuando se trata de roles y responsabilidades, controles de seguridad de TI y modelos de diseño para ICS, por ejemplo, Purdue Enterprise Reference Architecture (PERA)[39]. Sigue una estructura estándar para documentos de esta naturaleza y abarca:

1. Definiciones
2. Política
3. Excepciones
4. Roles y responsabilidades
5. Implementación

La sección de definiciones incluye numerosos términos relacionados con ICS, como Tecnología de Operaciones (TO), Control de supervisión y adquisición de datos (SCADA), Sistemas de control distribuido (DCS), Unidad terminal remota (RTU), Controlador lógico programable (PLC), Interfaz humano-máquina (HMI) y el modelo de referencia PERA mencionado anteriormente.

El contenido de la política define lo que está permitido y prohibido con respecto a:

1. El acceso físico a las áreas donde se utiliza ICS, declarando principalmente que los medios para restringir el acceso a tales instalaciones debería existir.
2. Acceso lógico a los recursos de ICS, describiendo los requisitos típicos de control de TI (segmentación de red física, firewalls, IPS, autenticación, registro y lista blanca de dispositivos).
3. La documentación y la capacitación también se incluyen como responsabilidades deben ser asignadas. Específicamente, la política establece que la documentación relacionada con el ICS debe considerarse confidencial y debe ser protegida de acuerdo con la política actual para este tipo de información. Además, la capacitación en ciberseguridad es obligatoria para todas las operaciones y personal de apoyo relacionado con ICS.

39. www.en.wikipedia.org/wiki/Purdue_Enterprise_Reference_Architecture

La política también abordó las siguientes áreas más específicamente:

A. Prohibiciones:
1. Acceso remoto
2. USB, discos duros externos, cámaras y teléfonos inteligentes
3. Redes inalámbricas y puntos de acceso wifi

B. Responsabilidades asignadas a la unidad operacional (propietario del sistema):
1. Inventario: realizando un seguimiento de todos los activos de TI autorizados.
2. Documentación
3. Planificación de la continuidad del negocio
4. Control de cambio de configuración

C. Responsabilidades asignadas a la unidad de seguridad de TI:
1. Incidentes de seguridad de TI y gestión de vulnerabilidades
2. Operaciones de control de seguridad (firewalls, IPS, seguridad endpoint, control de acceso a la red y otros)
3. Capacitación de ciberseguridad
4. Diseño de interconexión de red

Más específicamente, en lo que se refiere a las actividades de soporte de TI, se acordó que estas deberían ser ejecutadas por personal de TI específicamente asignado a través de acuerdos formales[40] de nivel operacional con las unidades de negocios. Este enfoque estableció claramente la expectativa de lo que el "negocio" debía implementar, así como también el "servicio" que iban a recibir de TI.

Es evidente a partir de la descripción de la política que se atiene a los principios básicos y no entra en detalles sobre cómo implementar los diferentes controles, aunque describe las responsabilidades de cada jugador. Esto podría ser una desviación de la política de TI típica, pero dado que su objetivo era abordar el área gris creada por la falta de comprensión de los diferentes roles y responsabilidades, parecía la mejor manera de iniciar el diálogo entre TI y operaciones, en relación con la seguridad de ICS.

40. www.en.wikipedia.org/wiki/Operational-level_agreement

Lecciones aprendidas:

La lección más importante que se identificó fue la constatación del orden en el que se desarrolló la política fue contraproducente. Rápidamente quedó claro que los roles y responsabilidades deberían haberse definido y comprendido antes de que se redactase la política. Aunque hemos tomado esta decisión a propósito, este enfoque no se recomienda para el desarrollo de ninguna política de TI. Su principal riesgo radica en el hecho de que si la política se vuelve obsoleta antes de que se establezcan los roles definidos, las diferentes unidades de negocios podrían no estar tan dispuestas a absorber las responsabilidades percibidas como "nuevas obligaciones".

En cambio, primero debería establecerse un comité directivo de TI. Dicho comité puede definir los roles y las responsabilidades necesarios, además de ser un lugar para debatir los controles técnicos. Su valor particular radica en garantizar que los datos específicos de la seguridad TO sean discutidos y acordados con las unidades de negocio que poseen el ICS. Debe ser una entidad permanente y no debe confundirse con los comités directivos de seguridad de TI generalmente encontrados dentro de las organizaciones. Esto se debe a que el objetivo principal de la TO siempre será la disponibilidad, mientras que los objetivos generales de seguridad de TI tienden a ser guiados por la confidencialidad y la integridad. Por lo tanto, se recomienda llegar a un acuerdo antes de desarrollar una política de cualquier tipo.
Asegurarse de que las definiciones sean claras antes de escribir la política, ya que está comenzando en este camino tempranamente. La adopción temprana ayudará a evitar una prisa por cumplir con las auditorías y regulaciones internas o externas, dependiendo de la industria. El principal objetivo de seguridad de TI debería ser lograr la garantía y no solo el cumplimiento. Si se apresura el desarrollo de la política, el resultado podría ser un documento centrado en el cumplimiento, en lugar de proteger los sistemas contra ataques.

Una lección inevitable fue que se debía disponer de tiempo suficiente para celebrar reuniones presenciales para asegurar la adquisición y poder explicar los motivos que impulsaron el desarrollo de la política. Los fundamentos, así como los roles y responsabilidades, deben estar documentados y claros para todos los involucrados en el diseño, operación y soporte de estos sistemas.

Otra lección importante fue que la cooperación de los compañeros en la comunidad de seguridad de TI que enfrentan desafíos similares puede ser particularmente útil. En el caso del Canal de Panamá, se han utilizado los recursos que estaban disponibles como resultado del desarrollo de la Estrategia Nacional de Ciberseguridad, que definía a los diversos actores de la infraestructura. Además, hoy, el Canal de Panamá está cooperando con el Instituto de Acueductos y Alcantarillados Nacionales (IDAAN) para apoyarlos en el desarrollo de su propia política de seguridad informática de ICS, y para obtener comentarios sobre nuestro propio enfoque. En conclusión, las lecciones derivadas de la implementación de nuestra política de seguridad de TI se pueden resumir de la siguiente manera:

1. Establecer un comité directivo antes de desarrollar la política;
2. Definir los objetivos de la política al inicio;
3. Participar en reuniones presenciales en unidades de negocios de manera regular;
4. Una Estrategia Nacional de Ciberseguridad puede ayudar a facilitar el proceso; y
5. la cooperación con los compañeros es un paso crítico para el éxito.

La ciberseguridad es vital para proteger la infraestructura crítica

Autor: Kaja Ciglic,
Director, Política y Estrategia de Ciberseguridad del Gobierno de Microsoft

Extracción

La naturaleza esencial de los sectores críticos de infraestructura hace que su protección sea una preocupación importante para la política nacional. Sin embargo, la protección de los entornos de infraestructura crítica conectados requiere un nuevo enfoque, sustancialmente diferente de las prácticas establecidas utilizadas para los riesgos de seguridad tradicionales y fuera de línea.

La tecnología es cada vez más importante para las oportunidades sociales y económicas del mundo actual. Esto también es válido para la infraestructura crítica nacional. Estas entidades adoptan la conectividad digital y la aprovechan para reducir los costos, aumentar la productividad y la eficiencia, mejorar la prestación de servicios y, en última instancia, permitir una mayor oportunidad económica. Desde los servicios financieros hasta el reposo de emergencia, desde la renovación energética hasta el suministro de agua, los sectores de infraestructura crítica están utilizando la tecnología para tener un impacto fundamental y mejorar continuamente nuestra calidad de vida.
La naturaleza esencial de las funciones y servicios de los sectores de infraestructura crítica hace que su protección sea una importante prioridad de política nacional. Sin embargo, proteger los entornos de infraestructura crítica conectados requiere una acción reguladora individual. Las complejidades de comprender y gestionar el riesgo en entornos conectados solo pueden ser navegadas a través de una coordinación y colaboración sin precedentes entre el gobierno, los propietarios y operadores de infraestructuras críticas y los proveedores de tecnología.

¿La ciberseguridad necesita incorporar la gestión de riesgos?

El enfoque de Microsoft en seguridad cibernética abarca más de cuatro décadas. Tomamos decisiones estratégicas para avanzar en la seguridad de nuestros productos y servicios, incluida una inversión anual de U$S 1 mil millones en investigación y desarrollo en este espacio. También recurrimos a nuestra experiencia para proporcionar regularmente orientación y capacitación a los clientes para protegerse a sí mismos y asociarse con gobiernos a nivel mundial para compartir las mejores prácticas que les ayuden a cumplir sus obligaciones exclusivas con sus ciudadanos en el ciberespacio.

La orientación que Microsoft proporciona con mayor frecuencia, independientemente de si se trata de organizaciones del sector público o privado, es que cualquier enfoque de ciberseguridad debe basarse en una gestión de riesgos priorizada. Todas las organizaciones, incluida la infraestructura crítica designada, deben equilibrar las inversiones en ciberseguridad con aquellas que respaldan otras funciones de la organización, como el desarrollo comercial y productos o servicios nuevos o mejorados. Ninguna organización tiene un presupuesto de seguridad ilimitado y todas las actividades implican cierto grado de riesgo.

Por consiguiente, los marcos de políticas que las naciones adoptan con el objetivo de aumentar la protección de infraestructura crítica deben basarse en la gestión de riesgos priorizada. Deberían permitir que las organizaciones identifiquen y evalúen sus riesgos más importantes de ciberseguridad, centrándose en las vulnerabilidades, las amenazas internas y externas y las posibles consecuencias de la explotación de las vulnerabilidades. Además, deberían permitir a las organizaciones determinar cómo gestionar el riesgo que han identificado, incluso al aceptarlomitigarlo, transferirlo o evitarlo.

¿Cuáles son las líneas de base de seguridad efectivas?

Las líneas de base de seguridad efectivas y eficientes tienden a adoptar los siguientes enfoques:

- Reunir y utilizar diversos conocimientos a través de un proceso de desarrollo abierto, colaborativo e iterativo.
- Aprovechar las mejores prácticas existentes
- Ayudar a gstionar la ciberseguridad destacando la gestión de riesgos priorizada
- Facilitar la toma de decisiones al aumentar la comprensión de la gestión de ciberseguridad tanto dentro como entre las organizaciones
- Permitir la innovación centrándose en los resultados de seguridad deseados en lugar de requisitos normativos.

Los gobiernos pueden hacerlo de manera más efectiva utilizando marcos de políticas que establecen puntos de referencia de seguridad para sectores críticos. Estos pueden tomar forma de orientación voluntaria, junto con incentivos (por ejemplo, requisitos de adquisición o subsidios fiscales); o ser implementado a través de un requisito reglamentario obligatorio, particularmente cuando surge una necesidad elevada de seguridad del entorno de riesgo. Independientemente del enfoque, el uso de líneas de base de seguridad intersectoriales generará un comportamiento positivo más allá de las organizaciones directamente impactadas, obligando o incentivando a los proveedores a implementar las mismas actividades de referencia también[41].

Mejores prácticas de las líneas de base de seguridad: Marco de ciberseguridad del NIST

El Marco para Mejorar la Ciberseguridad de Infraestructuras Críticas, desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos, es un ejemplo de una línea de base de seguridad que ha demostrado ser eficaz y por lo tanto ha logrado una mayor adopción, tanto dentro como fuera de los Estados Unidos. Su utilidad puede atribuirse, al menos en parte, a la naturaleza de su proceso de desarrollo. El marco fue desarrollado en estrecha colaboración con la industria, en diferentes sectores y tamaños, en un proceso abierto, iterativo y consultivo.

El marco de ciberseguridad del NIST fue iniciado por la orden ejecutiva 13636, publicada en 12 de febrero de 2013 y desarrollada durante varios meses con la ayuda de consultores, workshops y conversaciones informales para mejorar la ciberseguridad de infraestructuras críticas, que tuvieron lugar en todo Estados Unidos. El Marco continúa evolucionando y actualizándose, ya que a través de la implementación, las partes interesadas descubren los desafíos o áreas a las que podría expandirse para ayudarles a gestionar su entorno de riesgo de ciberseguridad.

En Europa, el gobierno italiano adoptó en 2015 su propio marco de ciberseguridad, que se centra en las pequeñas y medianas empresas. En Europa, el gobierno italiano adoptó en 2015 su propio marco de ciberseguridad, que se centra en las pequeñas y medianas empresas. El documento italiano se basa en gran medida en el marco de seguridad cibernética del NIST. Del mismo modo, la Comisión Australiana de Valores e Inversiones (ASIC) emitió en 2015 su informe de resiliencia cibernética: La verificación de integridad (REP 429), que alentó a las empresas a considerar el uso del Marco de seguridad cibernética del NIST para evaluar y mitigar sus riesgos cibernéticos.

La aceptación del marco probablemente continuará. La reciente Orden Ejecutiva Presidencial sobre el Fortalecimiento de la Ciberseguridad de las Redes Federales e Infraestructuras Críticas exige el uso del marco en todas las agencias del gobierno de los Estados Unidos. Además, la Organización Internacional de Normalización (ISO) ha aprobado recientemente un trabajo sobre un informe técnico sobre "Ciberseguridad y normas ISO e IEC", que busca adaptar el marco al entorno internacional, en parte incorporando muchas más normas ISO/IEC en su estructura y referencias informativas. Alentamos a los gobiernos de las Américas a participar en ese proceso.

41. -Marco para Mejorar la Ciberseguridad de Infraestructuras Críticas NIST: www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

-La Orden Ejecutiva 13636 sobre Mejoramiento de Ciberseguridad de Infraestructuras Críticas: www.obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

-Marco de ciberseguridad italiano: www.cybersecurityframework.it/en

Informe 429 sobre Ciber-resiliencia - Verificación de integridad: www.download.asic.gov.au/media/3062900/rep429-published-19-march-2015-1.pdf

- Orden ejecutiva presidencial sobre el fortalecimiento de la ciberseguridad de las redes federales e infraestructuras críticas: www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

Las líneas de base de seguridad son un componente central de la protección eficaz de infraestructuras críticas

Las líneas de base de seguridad son un conjunto fundamental de políticas, resultados, actividades, prácticas y controles destinados a ayudar a gestionar el riesgo de seguridad cibernética. Por lo general, cubren una amplia gama de objetivos de políticas de gestión de riesgos, como la protección contra amenazas cibernéticas o la detección y respuesta a incidentes. También pueden incluir resultados deseados más específicos (por ejemplo, conocer sus riesgos organizacionales), actividades o prácticas de seguridad (por ejemplo, realizar una evaluación de riesgos, documentar, revisar y difundir los resultados, y actualizar la evaluación regularmente) y controles de seguridad (por ej. las políticas de seguridad están definidas, aprobadas por la administración, publicadas y comunicadas a los empleados y a terceros).

Las líneas de base de seguridad son particularmente útiles para mejorar la ciberseguridad, ya que deben abarcar una serie de riesgos que suelen aplicarse en ciertos entornos, incluyendo sectores más críticos. La mayoría de los riesgos que enfrentan los gobiernos y las empresas son similares, por lo que la mayoría de las actividades "básicas" o de gestión de riesgos también son similares. Por ejemplo, todas las organizaciones deben pensar en revisar y actualizar regularmente las evaluaciones de riesgos, administrar cómo se accede a los recursos para evitar usuarios o comportamientos no autorizados, y planificar y mitigar el impacto de los incidentes. Si bien las líneas de base de seguridad deben ser aplicables en todos los sectores, permitiendo la comprensión común y la práctica constante en las organizaciones interdependientes, también pueden complementarse con prácticas o estándares que respondan a las amenazas o vulnerabilidades específicas del sector.

Cuando las líneas de base de seguridad se centran en los resultados, permiten a las organizaciones adaptarse a los cambios en la tecnología y al panorama de las amenazas. Mientras que los enfoques prescriptivos imponen el uso de tecnologías o controles particulares (por ejemplo, el uso de autenticación de dos factores), los enfoques centrados en los resultados permiten a las organizaciones determinar qué tecnologías, controles u otras actividades les permitirán cumplir, o incluso superar, un conjunto de resultados de seguridad deseados (por ej., controlar el acceso lógico a los recursos). A medida que las tecnologías y las arquitecturas evolucionan, esas organizaciones pueden implementar nuevos servicios y capacidades, incluyendo mejores servicios de seguridad o capacidades que respondan a las nuevas amenazas, con mayor agilidad. t

Aprovechar las mejores prácticas internacionales salvaguarda los recursos limitados

Una diferencia importante en gestionar la seguridad de las infraestructuras físicas y la gestión de la ciberseguridad de las infraestructuras críticas conectadas a Internet es la incapacidad de los gobiernos para limitar sus esfuerzos a los confines de sus fronteras nacionales. Es imprudente pensar en amenazas de ciberseguridad como amenazas exclusivamente nacionales. Desde el sector bancario hasta la red energética, los sectores de infraestructura crítica de hoy en día están interconectados y operan a nivel internacional. Aprovechar las mejores prácticas de ciberseguridad internacional establecidas, como las líneas de base de seguridad, puede garantizar que las organizaciones y actividades globales interconectadas o incluso interdependientes sean respaldadas o incluso fortalecidas por enfoques coherentes para la gestión de riesgo de ciberseguridad.

El proceso de crear un conjunto de prácticas de gestión de riesgos desde cero también requiere muchos recursos. En vista de la escasez mundial de profesionales de ciberseguridad, esto puede ser especialmente desafiante. El uso de métodos probados y verdaderos proporciona a los gobiernos una base sólida de prácticas y resultados más inmediatos. También asegura que se apliquen recursos suficientes a la gestión de la seguridad y el riesgo en lugar de desviarlos hacia el cumplimiento.

Lograr la resiliencia cibernética requiere un compromiso continuo

La protección crítica de la información a veces se ve de manera limitada, centrándose únicamente en el desarrollo de políticas y capacidades técnicas básicas requeridas para la protección, detección y respuesta a los ciberataques. Sin embargo, aunque una implementación efectiva de estos aumentará la seguridad de la infraestructura en un punto particular en el tiempo, no es suficiente. La protección de infraestructura crítica no puede ni debe verse como un estado final, sino como un proceso continuo de gestión de riesgos para mejorar la ciberseguridad y la resiliencia.

La capacidad de recuperación cibernética se puede entender mejor como las capacidades de una organización para la preparación, respuesta y reinvención frente a una amenaza cibernética. Efectivamente, esto incluye procesos que permiten la estabilidad, aseguran la recuperación y ayudan a restablecer los servicios rápidamente. Es distinto de la ciberseguridad, ya que esta última se centra especialmente en la protección de la confidencialidad, la integridad y la disponibilidad de datos, sistemas e infraestructura de TIC, como se destacó anteriormente. La resiliencia cibernética, por otra parte, es la capacidad de un sistema de TIC para continuar operando según lo previsto, incluso si la ciberseguridad está fallando o ha fallado.

Como resultado, lograr la resiliencia cibernética requiere una preparación integral para eventos que no solo están en línea, sino que también pueden incluir un ataque físico, un desastre natural, una falla técnica, un error humano o cualquier combinación de los mismos. También requiere un cambio en la tradicional forma de pensar en protección de infraestructuras críticas para manejar con éxito los riesgos e incidentes a través de la respuesta operativa, diseñada para el aprendizaje continuo y la reinvención.

El enfoque en la continuidad de la gestión de riesgos es fundamental en este sentido. Observar la protección de infraestructura crítica a través de este ángulo permite a las organizaciones planificar y gestionar mejor el ciclo de vida de ciberseguridad, responder a las amenazas a medida que evolucionan, internalizar las lecciones aprendidas y compartirlas con las diferentes partes interesadas operativas dentro de la organización afectada, así como con comunidades de políticas y seguridad fuera de la organización real que podrían beneficiarse de ella.

Componentes clave de la resiliencia cibernética

- Preparación.
  Para planear la preparación a largo plazo, una organización debe identificar activos, evaluar y administrar el riesgo de infraestructura, desarrollar capacidades para responder y recuperarse de interrupciones e invertir en investigación, educación y prácticas que contribuyan a los objetivos de ciberresiliencia a largo plazo.

- Respuesta.
  Al utilizar los planes y estrategias establecidos durante la fase de preparación, las entidades resilientes continúan funcionando durante una crisis y se recuperan rápidamente. Una respuesta resiliente también es adaptativa y flexible: innovar durante una crisis es un elemento clave de la resiliencia.

- Reinvención.
  Aprender y mejorar los planes y estrategias existentes es un sello distintivo de la resiliencia cibernética. Después de una crisis, el análisis es clave: identificar qué fue efectivo y dónde la respuesta fue problemática; desarrollando un plan de mejora; y luego implementándolo. Es importante pensar más allá de las ganancias a corto plazo.

Las alianzas público-privadas permiten una respuesta rápida

La protección eficaz de la infraestructura crítica debe basarse en alianzas privadas-privadas y también público-privadas. Los gobiernos, los propietarios y operadores de infraestructuras críticas y los proveedores de TIC deben asociarse entre sectores y fronteras para poder gestionar mejor los riesgos. Los beneficios de la acción colectiva en ciberseguridad son evidentes. El intercambio de información es un ejemplo del valor potencial de la respuesta colectiva a las amenazas cibernéticas. Cuando se comparte información sobre atacantes y métodos de ataque, las organizaciones están mejor preparadas para frustrarlas. Por lo tanto, sería útil que los gobiernos consideraran la implementación de marcos e incentivos que alentarían a las organizaciones de infraestructura críticas a participar en esta actividad.

Sin embargo, las alianzas público-privadas pueden ser efectivas más allá del intercambio básico de información sobre amenazas procesables. A través de grupos de trabajo o comités consultivos, los gobiernos pueden reunir a diferentes partes interesadas para mejorar la seguridad de sus servicios críticos. Sus áreas de enfoque podrían incluir: llegar a un acuerdo sobre líneas de base comunes de ciberseguridad, establecer estructuras de coordinación eficaces y procesos y protocolos de intercambio de información, identificando e intercambiaando ideas, enfoques y mejores prácticas para mejorar la seguridad, así como mejorar la coordinación internacional.

Estos esfuerzos no siempre tienen que llevarse a cabo en estructuras formales. Para aprovechar e integrar diversos conocimientos, los gobiernos también deben enfocarse en ser abiertos y colaborativos, creando así una oportunidad para el intercambio de experiencias, perspectivas e ideas. Por ejemplo, cuando se trata de desarrollo de políticas, encontramos que las políticas de seguridad cibernética se benefician de un proceso iterativo, que busca refinar los requisitos a lo largo del tiempo y brinda amplias oportunidades para comentarios sobre los proyectos de planes.

A nivel mundial, decenas de países están desarrollando o desarrollando directrices, normas y estándares de ciberseguridad que buscan mejorar la ciberseguridad de su infraestructura crítica. Los puntos de referencia de seguridad, los marcos de intercambio de información y las alianzas público-privadas son fundamentales para la mayoría de ellos. Esperamos que esta publicación ayude a orientar el desarrollo de políticas de ciberseguridad en las Américas de una manera que no solo resulte en la mejora de la seguridad y la capacidad de recuperación de la infraestructura crítica, sino también en la oportunidad social continua y el crecimiento económico. Microsoft está listo para apoyar esos esfuerzos.

Ciberseguridad industrial y el desafío de la cooperación entre TI y TO en la industria petrolera

Autor: Hernán Vázquez,
Gerente de TI de ARPEL

Extracto

Hoy nos enfrentamos a numerosos desafíos técnicos planteados por la creciente importancia del mundo digital en la industria petrolera y de gas. Además, la transformación digital ha dado lugar a cambios organizacionales, así como a diferentes responsabilidades relacionadas con el cumplimiento regulatorio. Además, la transformación digital ha dado lugar a cambios organizacionales, así como a diferentes responsabilidades relacionadas con el cumplimiento reglamentario.

El uso integral y en tiempo real de la información generada por equipos de negocios y equipos de campo y/o planta, por ejemplo en campos petroleros digitales, es cada vez más importante para las empresas de dicho sector. Como en todas partes, ha surgido la necesidad de que la Asociación Regional de Empresas del Sector del Petróleo, Gas y Biocombustibles en América Latina y el Caribe (ARPEL) y sus miembros integren los mundos de tecnología de la información (TI) y tecnología operacional (TO). Además, identificamos una clara necesidad de un espacio para construir un entendimiento mutuo, intercambiar experiencias y mejores prácticas, y abordar juntos los desafíos de la ciberseguridad.

La membresía de ARPEL actualmente representa más del 90% de las actividades upstream y downstream en América Latina y el Caribe, e incluye compañías operativas nacionales e internacionales, proveedores de tecnología, bienes y servicios para la cadena de valor e instituciones nacionales e internacionales del sector. Nuestros miembros enfrentan diferentes realidades, que se hicieron evidentes durante las reuniones organizadas por la Asociación en los últimos dos años, sin embargo, también hemos sido capaces de observar la existencia de problemas comunes, como los relacionados con la convergencia entre las áreas de TI y TO.

El mundo TO a menudo incluye maquinaria especializada, como sistemas de control industrial. Algunos ejemplos son el equipo de perforación y refinación para la industria petrolera y de gas, grandes redes de sistemas eléctricos y sensores utilizados en el sector de energía y servicios públicos. Estos sistemas típicamente físicos ahora integran sensores inteligentes que pueden ayudar al personal de operaciones a aumentar su eficiencia, ahorrar dinero y tomar mejores decisiones comerciales. De hecho, cuando los datos de los sensores remotos se ponen a disposición de una empresa en particular, se convierte en una herramienta poderosa para garantizar que las decisiones sean más efectivas y garanticen la diferenciación competitiva. Por lo tanto, en lugar de considerar TO y TI como dos redes individuales, los profesionales a cargo de estas áreas (directores de información (CIO), jefes de tecnología (CTO) y jefes de seguridad de información (CISO) se están dando cuenta de que estas dos áreas deben converger, lo que a su vez introduce nuevos desafíos y oportunidades.

El Grupo de Trabajo de Ciberseguridad Industrial de nuestra Asociación decidió abordar este importante desafío mediante la organización de eventos, talleres, seminarios y seminarios web. Esto nos llevó a concluir que se necesita un mayor trabajo conjunto, involucrando tanto a los profesionales de TO como a los de TI, por ejemplo, realizando análisis y desarrollando estrategias de seguridad de la infraestructura. Además, creemos que es clave para todos los países de la región adoptar un marco reglamentario formal en este campo para garantizar que puedan gestionar este riesgo adecuadamente. También se destacó la importancia de incorporar la ciberseguridad en las agendas de la alta gerencia de las compañías.

Como ejemplo de dicha actividad, una de nuestras empresas miembro creó un comité interdisciplinario de seguridad cibernética formado por los principales puntos de contacto de las distintas empresas verticales, personal de los sistemas de información e unidades de seguridad de la información. Este comité publicó el primer estándar de ciberseguridad industrial en la empresa, comenzando así en el camino hacia la integración de las áreas de TI y TO. En el proceso aprovecharon las sinergias colaborativas de estas áreas y desarrollaron reglas especiales para cada grupo empresarial. La participación autónoma y activa de la unidad de seguridad de la información en la gobernanza de la seguridad es vital para la integración de las diversas áreas de negocios dentro de la gestión de sistemas de información.

Además de otros factores importantes, la integración de unidades de TI y TO impulsa y justifica la necesidad de una gestión de seguridad de la información que sea autónoma y separada de la unidad de sistemas de información. De hecho, dada la creciente importancia del tema, es esencial que las empresas destinen más fondos para la ciberseguridad, entendiendo que esta es una inversión a largo plazo en la mitigación de riesgos para la empresa. Esto es cada vez más cierto para las grandes corporaciones.

El Foro Económico Mundial[42] enumera los riesgos cibernéticos como uno de los riesgos más importantes a nivel mundial. Del mismo modo, el Grupo Allianz coloca el riesgo cibernético en el top 10 de los principales riesgos actuales. Es importante destacar que el riesgo cibernético ha crecido en importancia de acuerdo con este índice: saltando de la posición 13 en 2013 a 3 en 2017[43]. Estos datos son una prueba más de que es extremadamente importante para la alta gerencia corporativa apoyar la capacitación del personal de seguridad cibernética, participar en el desarrollo de programas de concientización, alentar el establecimiento de equipos de respuesta de emergencia y asegurar el monitoreo periódico de la infraestructura y los sistemas.

Muchos de los problemas descritos anteriormente fueron abordados en un estudio llevado a cabo en Argentina por el Centro de Ciberseguridad Industrial de España[44]. Investigó a 18 empresas de diferentes sectores y fue lanzado en 2016 en un seminario organizado por ARPEL, la OEA y los Ministerios de Relaciones Exteriores y Culto de la República de Argentina. Los principales hallazgos incluyen:

- Para el 42% de los encuestados, el sector de TI era responsable de la ciberseguridad;
- El nivel de capacitación fue aceptable en TI, aunque fue bajo en otras áreas, tales como recursos inhumanos, control de calidad, adquisición y seguridad.
- El 41% de los encuestados realizó un análisis formal de riesgos de ciberseguridad;
- Los nuevos proyectos generalmente incluían requisitos de ciberseguridad, pero tendían a ser básicos o se delegaban al proveedor.
- Más del 50% de los encuestados no contaba con un proceso de gestión de incidentes;
- El estudio también reveló que el sector privado desconoce en gran medida las iniciativas del sector público.

Además de los hallazgos mencionados anteriormente, es apropiado suponer que existen más lagunas en términos de conocimiento y conocimiento de amenazas, capacitación, análisis de riesgos y gestión de incidentes. Sin embargo, incluso con eso en mente, los estándares, la comprensión, las mejores prácticas y las herramientas ya están disponibles y pueden ayudar a reducir la probabilidad de un ataque cibernético. Los ataques cibernéticos son una amenaza manejable, y la clave para estar preparado radica en poder implementar dichos estándares y buenas prácticas correctamente.

En ARPEL, seguiremos colaborando con nuestras empresas miembros, instituciones miembros y agencias nacionales e internacionales con el objetivo de reducir las brechas existentes y lograr la excelencia operativa y de gestión en un tema tan importante como la ciberseguridad.

42. Foro Económico Mundial, Informe Global de Riesgos (2018): www.weforum.org/agenda/2018/01/our-exposure-to-cyberattacks-is-growing-we-need-to-become-cyber-risk-ready/

43. Barómetro de riesgos de Allianz; Principales riesgos comerciales (2017): www.agcs.allianz.com/assets/PDFs/Reports/Allianz_Risk_Barometer_2017_EN.pdf

44. Centro Industrial de Ciberseguridad de España: www.cci-es.org/web/cci/home

Crear una conciencia global de Protección de Infraestructuras Críticas de Información: la Conferencia Anual de Meridian: más de una década de experiencia

Autor: Peter Burnett,
Proceso Meridian

Extracto

Esta presentación proporciona una breve discusión sobre la importancia del papel de la CIIP y Meridian para promover esa conciencia en todo el mundo. Plantea paralelismos con el proceso de Londres y distingue a CIIP de la ciberseguridad

Origen

En 2005, muy pocas personas habían oído hablar de ciberseguridad. Mucha gente pensaba que su infraestructura crítica (si es que reconocían ese concepto) podría estar protegida por vallas, guardias, sistemas de control de acceso, etc. De hecho, algunos de los elementos más importantes de nuestras infraestructuras críticas ya eran muy dependientes de las TIC en la época, especialmente en los sectores de finanzas, energía y, por supuesto, telecomunicaciones. Solíamos hablar sobre ataques electrónicos, seguridad informática, seguridad de la información, pero cuando estos conceptos se aplicaban a la protección de infraestructura crítica, se conocían como Protección de Infraestructuras Críticas de la Información (CII).

Cinco años más tarde se hizo evidente para muchos países que había una gran cantidad de cuestiones de seguridad importantes relacionados con el uso de las TIC en muchos aspectos de nuestras vidas, y el término que surgió para cubrirlos fue la ciberseguridad. Fue entonces cuando el Secretario de Relaciones Exteriores del Reino Unido estableció la serie de conferencias de alto nivel conocidas inicialmente como "El Proceso de Londres", pero ahora mejor conocidas como la Conferencia Mundial sobre el Espacio Cibernético (GCCS). Esa serie de eventos a nivel ministerial estimuló a los gobiernos de muchos países a descubrir más sobre la ciberseguridad y a reconocer su importancia. Se convirtió en una práctica aceptada que los países deberían crear estrategias nacionales de ciberseguridad (NCSS) para abordar los aspectos de seguridad cibernética del desarrollo económico, la defensa y la privacidad, por nombrar solo algunas cuestiones.

Sensibilización

No cabe duda de que el GCCS ha hecho un gran trabajo al transformar la ciberseguridad de un tema técnico a uno político, lo que aumenta su importancia en las agendas gubernamentales. Organizado por la India en noviembre de 2017,[45]el GCCS 2017 propuso promover un ciberespacio inclusivo con un enfoque en políticas y marcos de inclusión, sostenibilidad, desarrollo, seguridad, libertad, tecnología y alianzas para defender la democracia digital y promover el diálogo entre las partes interesadas.

Esta actividad de alto nivel también ha alentado a muchos gobiernos y organizaciones a abordar la desigualdad entre los países en términos de su madurez de seguridad cibernética y a participar en la creación de capacidad de ciberseguridad. La OEA es un excelente ejemplo de dicha organización y han contribuido enormemente a aumentar la conciencia y la capacidad de ciberseguridad en muchos países de las Américas y el Caribe. También ha sido un partidario muy valioso de Meridian, particularmente cuando la conferencia anual de Meridian se llevó a cabo en la región de la OEA. Puede haber varias razones por las cuales la OEA apoya a Meridian, pero una de las razones es el papel que Meridian ha desarrollado en términos de creación de capacidad de ciberseguridad.

Mucho antes de que la primera conferencia de Meridian fuera organizada por la agencia CIIP del Reino Unido, el Centro Nacional de Coordinación de Seguridad de Infraestructura (NISCC) en Greenwich, Londres en 2005, habían desarrollado algunas ideas clave dentro del NISCC:

1. Los gobiernos se dieron cuenta de que sabían muy poco sobre cómo proteger realmente su CII. En consecuencia, el concepto de intercambio de información confiable evolucionó, donde el gobierno y operadores industriales de CII compartirían su información, experiencias e ideas, de manera confidencial, para ayudar a protegerse contra amenazas. Este es ahora un concepto y una práctica bien establecidos, pero igual de importante y difícil de lograr.

2. La segunda constatación fue que, a diferencia de la protección de la infraestructura crítica que había sido una actividad en gran parte nacional, CIIP debe abordarse a nivel internacional. Esto se debe a que las CII casi siempre están interconectadas a través de las fronteras y, por lo tanto, interesa a cada país ayudar a proteger las CII de otros países. Una CII vulnerable en un país puede crear una ruta de ataque a otras CII, como un eslabón débil en una cadena. Además, el advenimiento del ciberespacio significa que cada país tiene ahora una frontera digital con cualquier otro país en el ciberespacio.

Por supuesto, hay muchas razones para conversar con otros países sobre el CIIP, por ejemplo: para compartir información sobre desarrollos y mejores prácticas en respuesta, ejercicios, políticas, estrategias, investigación, legislación, etc. y, por supuesto, desarrollos en tecnología. Meridian ha proporcionado un foro para esto en su conferencia anual durante 13 años, y estos eventos están diseñados específicamente para fomentar el intercambio y la discusión de ideas, prácticas y puntos de vista en un ambiente informal no político y confidencial. También brinda oportunidades para que los delegados establezcan y desarrollen vínculos de confianza con sus contrapartes en otros países. Estas conexiones personales pueden resultar inestimables cuando se trata de contingencias y amenazas emergentes, especialmente cuando se desarrollan en el nivel de las políticas, lo que ejemplifica a los delegados de Meridian y los miembros de la comunidad de Meridian.

Esta es un área donde Meridian difiere de GCCS, aunque hay una serie de paralismos entre las dos series de conferencias y los procesos de acompañamiento. Los delegados de Meridian suelen ser altos funcionarios de políticas gubernamentales, no los delegados de nivel ministerial que son delegados en GCCS.

45. Experiencias y buenas prácticas: estudios de caso

aunque los miembros de Meridian a menudo asisten a GCCS en apoyo. Las conferencias de Meridian son eventos mucho más pequeños y reservados, con un máximo de 100 delegados en total, y no más de 3 por país, no las vastas delegaciones que pueblan GCCS. Esto ayuda a todos los delegados de Meridian a desarrollar vínculos de confianza.

La otra gran diferencia es que Meridian se enfoca en la CIIP y no intenta abordar un campo mucho más amplio de ciberseguridad. Esto permite un enfoque mucho más claro, sin la distracción o la desviación en cuestión de elementos de ciberseguridad. En un principio se había supuesto que la CIIP simplemente se incluiría en la ciberseguridad, cuando ésta se convirtiera en un tema de moda en las agendas gubernamentales. En la práctica, sin embargo, todavía hay un fuerte interés discreto en las CIIP entre las naciones desarrolladas, donde a menudo se puede considerar el elemento más importante de la ciberseguridad. Esto se debe a que si la CII de una nación no está protegida, entonces todos los demás aspectos del entorno en línea están en peligro, al igual que la seguridad de esa nación.

La existencia continua de un foro respetado a nivel mundial dedicado a la CIIP subraya la importancia del tema. El hecho de que Meridian continúe floreciendo en su 13° año es aún más notable ya que sigue siendo un foro exclusivo del gobierno, con el fin de preservar su atmósfera confidencial. Eso significa que Meridian no cuenta con patrocinio ni apoyo de la industria y, por lo tanto, cuenta con recursos mínimos, y no cuenta con una secretaría, excepto un coordinador a tiempo parcial. No obstante, siempre ha habido una larga lista de países que desean ser anfitriones de la conferencia anual, y desde 2015 ha recibido el apoyo de GFCE en la forma de la Iniciativa CIIP GFCE-Meridian, así como contribuciones clave de gobiernos específicos, como Suecia,
Reino Unido y Holanda.

Meridian ha seguido deliberadamente una política de rotación en diferentes regiones siempre que posible. Esto significa que ha sido hospedado 3 veces en las Américas. En 2009, fue organizado por EE.UU., en 2013 por Argentina y en 2016 por México, y es probable que regrese pronto a las Américas.

Uno de los grandes beneficios de hospedar a Meridian es que eleva el perfil de CIIP en la agenda gubernamental del país anfitrión. Esto se debe a que la agencia anfitriona invitará a delegados de otras agencias, estimulando un debate sobre qué agencias tienen un rol en la CIIP y cómo pueden trabajar todas juntas. Esta fue una observación única cuando Meridian se organizó en Buenos Aires, pero también ha sido válida para muchos otros países anfitriones. La organización de Meridian ayuda a construir vínculos dentro de esa región, y puede impulsar los esfuerzos del país anfitrión para mostrar liderazgo en el tema. La necesidad crucial de vínculo internacional hace que la organización de Meridian sea una forma extremadamente valiosa para establecer contactos a nivel de trabajo sobre cuestiones de CIIP con países vecinos, así como entre otros 60 países de la comunidad de Meridian.

Meridian ahora también tiene otras actividades específicas de desarrollo de capacidades, apoyando el desarrollo continuo de CIIP en todos los países. Estos incluyen el antiguo directorio de contactos de Meridian CIIP, la Guía de buenas prácticas de CIIP más reciente, así como un nuevo "Programa de complicidad" en desarrollo y un paquete de capacitación de CIIP actualmente en desarrollo. La mejor manera de obtener más información sobre estos desarrollos y convertirse en miembro de la Comunidad Meridian (si su país aún no se ha unido) es accediendo a **www.meridianprocess.org.**

APÉNDICE
Recursos adicionales

Varios organismos, como el Foro Global sobre Conocimientos Cibernéticos, el Instituto Nacional Estadounidense de Estándares y Tecnología, así como compañías como Microsoft, han desarrollado directrices para apoyar el desarrollo y la implementación de estrategias y enfoques de CIIP, así como marcos asociados para evaluar y gestionar el riesgo en relación con la CII. Estos pueden aplicarse tanto en el sector público como en el privado:

- GFCE (2016): La Guía de Buenas Prácticas de GFCE-MERIDIAN sobre Infraestructuras Críticas de la Información Protección para los responsables de las políticas gubernamentales;[46];
*Instituto Nacional de Estándares y Tecnología (NSIT) Marco para mejorar la ciberseguridad de las infraestructuras críticas (Versión 1.1 Proyecto 2) 42)[47];
- Microsoft (n.d.): Un marco para la Gestión de Riesgos de Infraestructuras Críticas de la Información[48];

Si bien la primera guía cubre el desarrollo de una estrategia CIIP desde una perspectiva de política, las dos siguientes ofrecen recomendaciones específicas relacionadas con la implementación de iniciativas CIIP. En particular, brindan orientación sobre cómo evaluar y gestionar los riesgos de ciberseguridad. El documento final proporciona recomendaciones específicas sobre cómo desarrollar e implementar requisitos de seguridad básicos para garantizar que las organizaciones puedan permanecer seguras. Además, las organizaciones específicas del sector que cuentan como infraestructuras críticas, tanto públicas como privadas, han desarrollado una guía de gestión de riesgos para sus industrias verticales. Estos incluyen, por ejemplo, el Comité de Protección de Infraestructuras Críticas de North American Electric Reliability Corporation[49], el Intercambio de Información de la Industria Química/Consejo Americano de Química[50], y el Consejo de Estabilidad Financiera[51].

Finalmente, la Organización Internacional de Normalización (ISO) proporciona varias pautas, que incluyen: La norma ISO 27032, que proporciona una guía para mejorar la ciberseguridad y abarca las prácticas de seguridad básicas; la norma ISO 27001, que apoya el establecimiento de un Sistema de Gestión de Seguridad de la Información (ISMS) en una organización; e ISO 27005, que destaca las mejores prácticas para el desarrollo de una metodología de gestión de riesgos[52]

46. La Guía de Buenas Prácticas de GFCE-MERIDIAN sobre Infraestructuras Críticas de la Información para los responsables de la formulación de políticas gubernamentales;
www.meridianprocess.org/siteassets/meridian/gfce-meridian-gpg-to-ciip.pdf

47. Marco para Mejorar la Ciberseguridad de Infraestructuras Críticas NIST:
www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_without-markup.pdf

48. Microsoft, un Marco para la Gestión de Riesgos de Infraestructuras Críticas de la Información;
www.uery.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc7

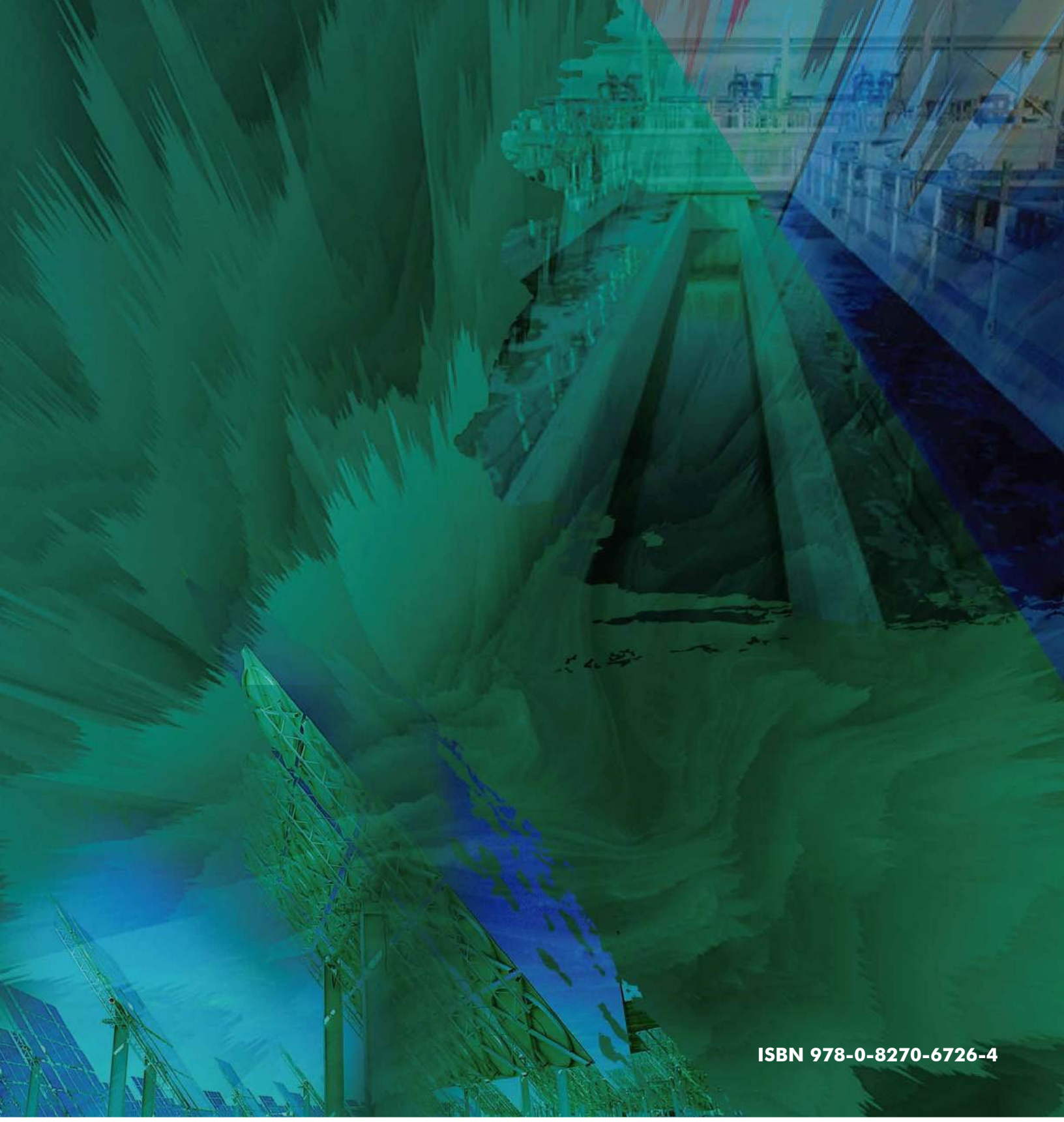
49. Infraestructura crítica de North American Electric Reliability Corporation:
www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

50. Intercambio de datos de la industria química/Consejo estadounidense de química:
www.chemitc.americanchemistry.com/RCSC-NIST-Framework-Guidance-Jan-2016.pdf

51. Consejo de Estabilidad Financiera
www.fsb.org/wp-content/uploads/P131017-2.pdf

52. ISO. (2011). ISO/IEC 27005:2011: Gestión de riesgos de seguridad de la información: www.iso.org/standard/56742.html; ISO. (2012). ISO / IEC 27032: 2012: Pautas para la ciberseguridad: www.iso.org/standard/44375.html;
ISO. (2013). ISO/IEC 27000: Sistemas de gestión de seguridad de la información: www.iso.org/isoiec-27001-information-security.html

PROTECCIÓN DE LA INFRAESTRUCTURA CRÍTICA EN AMÉRICA LATINA Y EL CARIBE 2018



ISBN 978-0-8270-6726-4

OAS More rights for more people

Microsoft