

## **TÉRMINOS DE REFERENCIA**

### *Consultoría para análisis de brechas de habilidades digitales en las empresas para riesgos de ciberseguridad*

#### **1. Antecedentes y Justificación**

- 1.1.** Debido a la pandemia, las economías de la región sufrieron cierres y paralizaciones, interrumpiendo el flujo de actividades productivas y de consumo lo que se tradujo en contracciones en la oferta y la demanda. Esta sucesión de fricciones afectó la relación entre empresas y consumidores e interrumpió las CGV al suspender las transacciones entre proveedores, productores y servicios relacionados. Las empresas se vieron obligadas a responder en múltiples frentes simultáneamente: mientras trabajaban para proteger la seguridad de sus empleados, también necesitaban salvaguardar su viabilidad operativa, cada vez bajo un estrés más significativo debido a un gran impacto en las CGV.
- 1.2.** Las consecuencias de la interrupción de la CGV se han hecho evidentes por la pandemia y otros eventos globales, como la guerra en Ucrania, incluidos los atacantes cibernéticos. En efecto, los proveedores externos de una empresa pueden poner en riesgo toda la cadena de suministro. Gartner informa que en 2019 solo el 21% de los líderes de la cadena de suministro creen que su red de proveedores es "altamente resistente" a los ataques cibernéticos. Asimismo, de acuerdo a una encuesta realizada por el grupo NCC en 2022 a cerca de 1.400 tomadores de decisiones de seguridad cibernética en 12 economías avanzadas, encontró que solo el 32% estaba "muy seguro" de poder responder de manera rápida y efectiva a un ataque a la cadena de suministro. Las empresas en una cadena de suministro son tan fuertes como su eslabón más débil, pero pueden mejorar esta situación asegurándose de que cada eslabón (empresa) a lo largo de su cadena de suministro esté protegido contra amenazas cibernéticas McAlmont (2022).
- 1.3.** Lo anterior también aplica al sector público, donde los países necesitan mejor equipamiento para combatir la creciente sofisticación de los atacantes cibernéticos. Por ejemplo, en abril de 2022, el gobierno de Costa Rica confirmó haber sido víctima del ransomware Conti, el cual afectó, en su mayoría, al Ministerio de Hacienda y a entidades como la Costarricense y la Caja Costarricense del Seguro Social. Debido a esta situación, el gobierno se vio obligado a deshabilitar varios servicios informáticos y a declarar Estado de Emergencia Nacional (Maundrill, 2022). Por su parte, de acuerdo con IBM Security X-Force Threat Intelligence Index 2023, Colombia es el segundo país de la región que más ciberataques se reportaron en 2022, detrás de Brasil. Entre enero y octubre de 2022, se reportaron más de 50.000 denuncias por ciberataques en Colombia, según cifras del Centro Cibernético de la Policía Nacional. Además, más de 30 empresas informaron que fueron objeto de hackeos, entre ellas EPS Sanitas que administra la salud a más de cinco millones de colombianos. El último informe semestral del panorama global de amenazas de FortiGuard Labs resalta que Panamá recibió 1.400 millones de intentos de ciberataques en 2022. Para el caso de El Salvador, 206.000 empresas fueron víctimas de ataques cibernéticos en 2021.
- 1.4.** Los ataques cibernéticos se dirigen cada vez más a las pequeñas y medianas empresas (PYMES), normalmente los eslabones más débiles de una cadena, lo cual puede ser devastador desde el punto de vista financiero (OCDE, 2021). En efecto, cerca del 70% de las pymes de la región afirman haber experimentado recientemente problemas de ciberseguridad (referencia), por lo que resulta fundamental comprender mejor los riesgos y las posibles estrategias y buenas prácticas para que las PYMES operen de manera más segura.

## **2. Objetivos**

- 2.1.** El objetivo de esta consultoría es analizar las brechas de habilidades digitales en las empresas para riesgos de ciberseguridad en Costa Rica, Panamá y Colombia. Los objetivos específicos son: (i) identificar el grado de escasez de habilidades digitales necesarias para proporcionar a las empresas y la infraestructura pública crítica suficiente seguridad cibernética, y (ii) identificar las capacidades de las PYME de los países para hacer frente a los riesgos de ciberseguridad.

## **3. Alcance de los Servicios**

- 3.1.** Se contratará a una firma consultora, por un periodo de 6 meses. La firma deberá contar con un Coordinador del Proyecto para garantizar una implementación efectiva de los objetivos establecidos en la consultoría
- 3.2.** La firma deberá tener experiencia y conocimiento en la definición, búsqueda y análisis de metodologías y parámetros de operación de análisis institucional enfocado al sector privado.
- 3.3.** La firma deberá contar con un equipo con experiencia y conocimiento en la formulación de estudios para temas digitales, específicamente ciberseguridad.
- 3.4.** Contar con experiencia positiva mínima de 3 años desarrollando estudios, metodologías y realizando estudios relevantes a esta consultoría.

## **4. Actividades Clave**

Para el desarrollo de la consultoría la firma consultora deberá llevar a cabo al menos las siguientes actividades para lograr los objetivos del trabajo encomendado, sin perjuicio de que se incorporen otras actividades puntuales, previa aprobación del equipo contraparte, en conformidad al desarrollo del proyecto:

- 4.1.** Revisar las capacidades institucionales del sector privado con relación a la ciberseguridad.
- 4.2.** Identificar el grado de escasez de habilidades digitales necesarias para proporcionar a las empresas y la infraestructura pública crítica suficiente seguridad cibernética.
- 4.3.** Analizar e identificar las capacidades de las PYME de los países para hacer frente a los riesgos de ciberseguridad
- 4.4.** Recomendar una propuesta de fortalecimiento de capacidades para el cierre de brechas digitales y de ciberseguridad.
- 4.5.** Analizar las necesidades de las empresas, los sectores y los sub-sectores que caracterizan el ecosistema regional para atender las amenazas en ciberseguridad, y proponer instrumentos que desde el sector público se pueden implementar para brindar apoyo.
- 4.6.** Proponer los requerimientos mínimos que debería tener un plan de respuesta a incidentes de seguridad para PyMEs, mismos que serán utilizados como insumo para elaborar términos de referencia de una consultoría específica que diseñe dicho plan

## **5. Resultados y Productos Esperados**

La consultoría deberá entregar como productos finales los siguientes:

- 5.1. Producto 1:** Plan de trabajo detallado, con indicación de plazos y entidades a ser involucradas.
- 5.2. Producto 2:** Informe con: (i) revisión de grado de escasez de habilidades digitales necesarias para proporcionar a las empresas y la infraestructura pública crítica suficiente seguridad cibernética; y (ii) análisis de capacidades de las PYME de los países para hacer frente a los riesgos de ciberseguridad.

- 5.3. Producto 3:** Informe con las recomendaciones para el fortalecimiento de capacidades de las empresas en temas de ciber seguridad y requerimientos mínimos para un plan de respuesta a incidentes de ciberseguridad.

## **6. Calendario del Proyecto e Hitos**

Actividades y productos	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6
Producto 1	X					
Producto 2			X			
Producto 3						X

## **7. Requisitos de los Informes**

- 7.1.** Todo informe debe ser sometido al Banco en un archivo electrónico. El informe debe incluir una carátula, resumen, documento principal, y todos los anexos.
- 7.2.** Los informes deben ser presentados en idioma español.

## **8. Criterios de aceptación**

- 8.1.** La empresa contratada deberá hacer entrega formal de cada producto solicitado de acuerdo con el plan de trabajo y cronograma aprobado por la coordinación de este estudio.
- 8.2.** Para el desarrollo de cada uno de los productos deben sostenerse reuniones con las contrapartes técnicas de esta contratación, para analizar el avance de cada producto, acordar posibles ajustes o abordaje de contingencias, siendo esto un requisito fundamental para la aprobación de los productos.
- 8.3.** Si se solicitan ajustes a los informes como correcciones o complementos al contenido entregado, las nuevas versiones deberán incorporar esos comentarios. Mientras esto no ocurra, las versiones entregadas se entenderán preliminares y no aprobadas para pago.
- 8.4.** Los informes deberán recoger las observaciones del BID. Los informes deberán ser remitidos al Jefe de Equipo la Cooperación Técnica

## **9. Supervisión e Informes**

- 9.1.** El liderazgo y coordinación de esta consultoría estará a cargo del Especialista Líder en Competitividad, Tecnología e Innovación (CTI/CPN). El líder y coordinador de esta consultoría dará visto bueno en aceptación de cada uno de los productos y entregables mencionados anteriormente con el fin de realizar cada desembolso a la firma consultora. La comunicación que hará oficial la aceptación de cada entregable será por medio de correo electrónico.
- 9.2.** El proveedor del servicio procurará mantener reuniones periódicas de coordinación con las contrapartes. Estas reuniones podrán ser virtuales y el formato será definido de común acuerdo al inicio del estudio y podrá ser revisado conforme avance la consultoría.
- 9.3.** Los productos deberán ser enviados al BID para su revisión y comentarios. Una vez incluidos los comentarios, y para procurar que los productos finales sean de utilidad para los países beneficiarios.

## **10. Calendario de Pagos**

- 10.1.** Las condiciones de pago se basarán en los hitos o entregables del proyecto. El Banco no espera hacer pagos por adelantado en virtud de contratos de consultoría a menos que se requiera una cantidad significativa de viajes.

**10.2.** La Tasa de Cambios Oficial del BID indicada en el SDP se aplicará para las conversiones necesarias de los pagos en moneda local.

Plan de Pagos	
Entregables	%
1. Productos 1	20%
2. Producto 2	40%
3. Producto 3	40%
<b>TOTAL</b>	<b>100%</b>

## **TÉRMINOS DE REFERENCIA**

### *Consultoría para programa de capacitación en Ciberseguridad para PyMEs*

#### **1. Antecedentes y Justificación**

- 1.1.** Debido a la pandemia, las economías de la región sufrieron cierres y paralizaciones, interrumpiendo el flujo de actividades productivas y de consumo lo que se tradujo en contracciones en la oferta y la demanda. Esta sucesión de fricciones afectó la relación entre empresas y consumidores e interrumpió las CGV al suspender las transacciones entre proveedores, productores y servicios relacionados. Las empresas se vieron obligadas a responder en múltiples frentes simultáneamente: mientras trabajaban para proteger la seguridad de sus empleados, también necesitaban salvaguardar su viabilidad operativa, cada vez bajo un estrés más significativo debido a un gran impacto en las CGV.
- 1.2.** Las consecuencias de la interrupción de la CGV se han hecho evidentes por la pandemia y otros eventos globales, como la guerra en Ucrania, incluidos los atacantes cibernéticos. En efecto, los proveedores externos de una empresa pueden poner en riesgo toda la cadena de suministro. Gartner informa que en 2019 solo el 21% de los líderes de la cadena de suministro creen que su red de proveedores es "altamente resistente" a los ataques cibernéticos. Asimismo, de acuerdo a una encuesta realizada por el grupo NCC en 2022 a cerca de 1.400 tomadores de decisiones de seguridad cibernética en 12 economías avanzadas, encontró que solo el 32% estaba "muy seguro" de poder responder de manera rápida y efectiva a un ataque a la cadena de suministro. Las empresas en una cadena de suministro son tan fuertes como su eslabón más débil, pero pueden mejorar esta situación asegurándose de que cada eslabón (empresa) a lo largo de su cadena de suministro esté protegido contra amenazas cibernéticas McAlmont (2022).
- 1.3.** Lo anterior también aplica al sector público, donde los países necesitan mejor equipamiento para combatir la creciente sofisticación de los atacantes cibernéticos. Por ejemplo, en abril de 2022, el gobierno de Costa Rica confirmó haber sido víctima del ransomware Conti, el cual afectó, en su mayoría, al Ministerio de Hacienda y a entidades como la Costarricense y la Caja Costarricense del Seguro Social. Debido a esta situación, el gobierno se vio obligado a deshabilitar varios servicios informáticos y a declarar Estado de Emergencia Nacional (Maundrill, 2022). Por su parte, de acuerdo con IBM Security X-Force Threat Intelligence Index 2023, Colombia es el segundo país de la región que más ciberataques se reportaron en 2022, detrás de Brasil. Entre enero y octubre de 2022, se reportaron más de 50.000 denuncias por ciberataques en Colombia, según cifras del Centro Cibernético de la Policía Nacional. Además, más de 30 empresas informaron que fueron objeto de hackeos, entre ellas EPS Sanitas que administra la salud a más de cinco millones de colombianos. El último informe semestral del panorama global de amenazas de FortiGuard Labs resalta que Panamá recibió 1.400 millones de intentos de ciberataques en 2022. Para el caso de El Salvador, 206.000 empresas fueron víctimas de ataques cibernéticos en 2021.
- 1.4.** Los ataques cibernéticos se dirigen cada vez más a las pequeñas y medianas empresas (PYMES), normalmente los eslabones más débiles de una cadena, lo cual puede ser devastador desde el punto de vista financiero (OCDE, 2021). En efecto, cerca del 70% de las pymes de la región afirman haber experimentado recientemente problemas de ciberseguridad (referencia), por lo que resulta fundamental comprender mejor los riesgos y las posibles estrategias y buenas prácticas para que las PYMES operen de manera más segura.

## **2. Objetivos**

- 2.1.** El objetivo de esta consultoría es apoyar a implementar un programa de asesoría técnica para el desarrollo de capacidades empresariales y transferencia de conocimiento en procesos de digitalización y transformación digital, específicamente en ciberseguridad para PYMES de la región.

## **3. Alcance de los Servicios**

- 3.1.** Se contratará a una firma consultora, por un periodo de 12 meses. La firma deberá contar con un Coordinador del Proyecto para garantizar una implementación efectiva de los objetivos establecidos en la consultoría.
- 3.2.** El equipo de la firma deberá tener experiencia y conocimiento en la implementación de programas o concursos de innovación. Se valorarán las experiencias que tengan que ver con asesoría técnica y/o concursos dirigidos a PYMES en temas relacionados con la digitalización y la transformación digital, con especial énfasis en ciberseguridad.
- 3.3.** La firma debe contar con las personas expertas profesionales necesarias para cumplir a cabalidad con los objetivos y entregables del programa propuesto y debe indicar quién es la persona que lidera el programa. Deberán ser personas profesionales y tener las competencias y habilidades teóricas y prácticas comprobables y requeridas para impartir los procesos de desarrollo de capacidades y el acompañamiento/asesoría técnica propuestos, en relación con el contenido temático definido y su rol en el desarrollo del programa. Estas personas pueden ser personal de planta o subcontratadas.
- 3.4.** Todo el recurso humano deberá tener disponibilidad inmediata para atender la demanda de trabajo que se requiera y así garantizar la realización y cumplimiento de los servicios con calidad y profesionalismo.
- 3.5.** La firma debe contar con una experiencia positiva mínima de 3 años desarrollando y brindando procesos formativos y de asesoría empresariales y debe contar con la capacidad (física, tecnológica y de personal) suficiente para atender la cantidad de personas que se requieren. El personal involucrado en el proceso debe contar con una experiencia mínima de 2 años, relacionada con los temas que vaya a desarrollar.
- 3.6.** La firma será la responsable de realizar el diseño, desarrollo y ejecución de todas las actividades del Programa, en sus procesos (asesoría técnica), según los contenidos temáticos propuestos.
- 3.7.** El equipo de la firma deberá trabajar de manera coordinada con el equipo del BID durante la ejecución del proyecto y deberá mantener una reunión de seguimiento y avances al menos una vez cada 15 días durante el periodo de ejecución.

## **4. Actividades Clave**

Para el desarrollo de la consultoría la firma consultora deberá llevar a cabo al menos las siguientes actividades para lograr los objetivos del trabajo encomendado, sin perjuicio de que se incorporen otras actividades puntuales, previa aprobación del equipo contraparte, en conformidad al desarrollo del proyecto:

### **4.1. Estrategia Comunicacional y búsqueda de beneficiarios:**

- a. Preparar y presentar el Plan de Trabajo, con metodología y su respectivo cronograma de actividades y plazos de entrega de los productos.
- b. Diseño de la estrategia comunicacional, desarrollo del naming, KV y landing page, así como la difusión, lanzamiento y convocatoria del proyecto en redes y prensa. El presupuesto debe incluir pautas en redes sociales y producción de materiales para la difusión. Si la firma consultora no cuenta con un equipo de comunicación debe

subcontratar este servicio.

- c. Desarrollo del proceso de postulación y selección de las empresas. El equipo evaluador estará conformado por integrantes de la firma y el equipo designado del BID. Se espera seleccionar al menos a 200 PYMES. Los criterios de selección de las empresas serán definidos por el BID, en donde se elaborará un listado con los criterios de elegibilidad bien detallados para la selección y admisión de empresas.

#### **4.2. Asesoría técnica de expertos digitales:**

- a. Una vez se cuente con un conjunto de PYMES seleccionadas, la firma consultora gestionará el plan de la prestación de asistencia técnica directa a las empresas para la implementación de acciones de digitalización y transformación digital, específicamente en ciberseguridad.
- b. Entiéndase como servicios de asesoría técnica los procesos de implementación de un plan de cierre de brechas definido en un diagnóstico (puede referenciarse a la estrategia diseñada en programas anteriores) y que requiere asistencia técnica inicial del ente proveedor. Sesiones de asesoramiento y colaboración sobre un tema específico que permiten el desarrollo de habilidades y la transferencia de conocimientos especializados a la empresa para el uso, incorporación, reparación y/o mantenimiento de maquinaria, equipo y/o software que logren hacer más eficiente los procesos de la empresa e incrementar su productividad en temas relacionados con comercio electrónico.

#### **4.3. Sistematización de los resultados**

- a. La firma deberá recopilar y sistematizar los datos del proyecto que servirán de base para la evaluación del programa ejecutado.
- b. Deberá formular aprendizajes y recomendaciones para futuras iniciativas.
- c. Elaborar el material comunicacional para la difusión de los resultados del proyecto.
- d. La firma deberá colaborar con los consultores (externos) a cargo del proceso de la evaluación de la intervención apoyada por el programa. La participación de los consultores encargados de la evaluación se dará desde las fases iniciales y podrán intervenir en cualquier momento del proceso. Al respecto, se podrán impartir encuestas u otras herramientas a las empresas participantes como parte del proceso de evaluación de conocimientos y alcances obtenidos de los beneficiarios. El diseño de estas herramientas será realizado por los consultores expertos en evaluación, con participación de la firma consultora en la fase de diseño y recogida de información. Los resultados serán compartidos con el BID para el proceso posterior de evaluación.

### **5. Resultados y Productos Esperados**

La consultoría deberá entregar como productos finales los siguientes:

- 5.1. Producto 1:** Plan de trabajo que incorpore los principales hitos y actividades a ser desarrolladas para el cumplimiento de los objetivos propuestos, indicando el cronograma y modalidad de las asesorías técnicas en comercio electrónico a las PYMES.
- 5.2. Producto 2:** Informe de avances que incluya la lista de cumplimiento de entregables para cada PYME a ser beneficiadas con el proyecto.
- 5.3. Producto 3:** Informe final del proyecto, que incluya documentación que demuestre la prestación efectiva de la asistencia técnica a las PYMES, una evaluación de satisfacción de las mismas, además de una sistematización de aprendizajes, conclusiones y recomendaciones para poder escalar el Programa en el futuro.

## 6. Calendario del Proyecto e Hitos

Actividades y productos	Mes 1	Mes 3	Mes 6	Mes 9	Mes 12
Producto 1	X				
Producto 2			X		
Producto 3					X

## 7. Requisitos de los Informes

- 7.1. Todo informe debe ser sometido al Banco en un archivo electrónico. El informe debe incluir una carátula, resumen, documento principal, y todos los anexos.
- 7.2. Los informes deben ser presentados en idioma español.

## 8. Criterios de aceptación

- 8.1. La empresa contratada deberá hacer entrega formal de cada producto solicitado de acuerdo con el plan de trabajo y cronograma aprobado por la coordinación de este estudio.
- 8.2. Para el desarrollo de cada uno de los productos deben sostenerse reuniones con las contrapartes técnicas de esta contratación, para analizar el avance de cada producto, acordar posibles ajustes o abordaje de contingencias, siendo esto un requisito fundamental para la aprobación de los productos.
- 8.3. Si se solicitan ajustes a los informes como correcciones o complementos al contenido entregado, las nuevas versiones deberán incorporar esos comentarios. Mientras esto no ocurra, las versiones entregadas se entenderán preliminares y no aprobadas para pago.
- 8.4. Los informes deberán recoger las observaciones del BID. Los informes deberán ser remitidos al Jefe de Equipo la Cooperación Técnica

## 9. Supervisión e Informes

- 9.1. El liderazgo y coordinación de esta consultoría estará a cargo del Especialista Líder en Competitividad, Tecnología e Innovación (CTI/CPN). El líder y coordinador de esta consultoría dará visto bueno en aceptación de cada uno de los productos y entregables mencionados anteriormente con el fin de realizar cada desembolso a la firma consultora. La comunicación que hará oficial la aceptación de cada entregable será por medio de correo electrónico.
- 9.2. El proveedor del servicio procurará mantener reuniones periódicas de coordinación con las contrapartes. Estas reuniones podrán ser virtuales y el formato será definido de común acuerdo al inicio del estudio y podrá ser revisado conforme avance la consultoría.
- 9.3. Los productos deberán ser enviados al BID para su revisión y comentarios. Una vez incluidos los comentarios, y para procurar que los productos finales sean de utilidad para los países beneficiarios.

## 10. Calendario de Pagos

- 10.1. Las condiciones de pago se basarán en los hitos o entregables del proyecto. El Banco no espera hacer pagos por adelantado en virtud de contratos de consultoría a menos que se requiera una cantidad significativa de viajes.
- 10.2. La Tasa de Cambios Oficial del BID indicada en el SDP se aplicará para las conversiones necesarias de los pagos en moneda local.



Plan de Pagos	
Entregables	%
4. Productos 1	20%
5. Producto 2	60%
6. Producto 3	20%
<b>TOTAL</b>	<b>100%</b>