**HRD Término de Referencia** **ANEXO A**

**Consultor Servicios de consultoría profesional para la adaptación de estándar internacional de ciberseguridad ISO 27001**

**Ubicación**

El Grupo BID es una comunidad de personas diversas, versátiles y apasionadas, unidas para mejorar vidas en América Latina y el Caribe. Aquellos que trabajan con nosotros encuentran un propósito y hacen lo que más les gusta en un entorno inclusivo, colaborativo, ágil y gratificante.

**Acerca de este puesto de trabajo**

Estamos buscando un/a consultor que se encargará de prestar servicios profesionales al Ministerio de Finanzas de Guatemala para la adaptación de estándar internacional de ciberseguridad de la norma ISO 27001:2022 Esencialmente, se busca garantizar la confidencialidad, integridad y disponibilidad de la información, así como gestionar de manera efectiva los riesgos asociados dentro de un ciclo de mejora continua.

Este proceso integral de consultoría abarcará el diseño, implementación, las acciones de mejora continua y el desarrollo de capacidades del personal; así mismo incluye la implementación de las acciones técnicas de configuración de software y/o hardware necesarios para el aseguramiento operativo del MINFIN y la integración de las recomendaciones legales relacionadas a las condiciones laborales vigentes. Este proceso definirá políticas y procedimientos para proteger los activos de información y aplicar controles de seguridad de la información críticos para mitigar y abordar los riesgos.

**Esto es lo que harás**

(principales responsabilidades que contribuyen a los objetivos del equipo; no incluir detalles)

- Desarrollar un plan de implementación que incluya actividades, cronograma y recursos necesarios para adoptar el ISO 27001: 2022 estableciendo hitos y entregables específicos para monitorear el progreso de la implementación.
- Definir y documentar las políticas y procedimientos específicos que cubran todos los aspectos de la seguridad de la información, alineados con la norma ISO 27001:2022, para garantizar coherencia y cumplimiento normativo.
- Validar el inventario levantado de todos los activos de información y clasificarlos según su criticidad y sensibilidad.
- Revisar, implementar y validar la efectividad de los controles de seguridad de la información específicos cumplir con la normativa, estableciendo un registro de estos para asegurar su revisión y actualización continua.
- Garantizar que solo el personal autorizado tenga acceso a información sensible según su rol y responsabilidades.
- Implementar controles específicos para la protección y privacidad de los datos personales.
- Desarrollar un plan de continuidad del negocio que incluya procedimientos para mantener y restaurar las operaciones críticas en caso de un incidente de seguridad de la información, a través de la ejecución de pruebas y simulacros para asegurar la efectividad del plan de continuidad del negocio.

- Evaluar terceros y proveedores con el fin de examinar y gestionar los riesgos asociados con terceros y proveedores que tienen acceso a la información del MINFIN con el fin de establecer requisitos de seguridad de la información.
- Desarrollar y llevar a cabo programas de capacitación para todo el personal del MINFIN para que comprendan y apliquen adecuadamente los principios y prácticas conforme a su rol, alineados con la norma ISO 27001:2022, para garantizar la correcta configuración de los controles de seguridad de la información y la gestión de riesgos.
- Las recomendaciones legales necesarias, conforme a las regulaciones laborales, para incorporar las faltas y responsabilidades legales (administrativas o penales, según corresponda) como parte del régimen de gestión de personal.
- Preparar al MINFIN para su certificación realizando una auditoría interna final para evaluar el cumplimiento de todos los requisitos de ISO 27001:2022 que incluya toda la documentación y evidencia necesaria para la auditoría de certificación externa, manteniendo un control de cambios para asegurar que la documentación esté actualizada y refleje las prácticas actuales.

## Cronograma de Entregas y Pagos

Click or tap here to enter text.

| Entregable # | Porcentaje | Fecha estimada de entrega |
|---|---|---|
| Producto 1 | 25 % | Enero 2025 |
| Producto 2 | 25 % | Mayo 2025 |
| Producto 3 | 25 % | Septiembre 2025 |
| Producto 4 | 25 % | Marzo 2026 |
| **Total** | **100 %** | - |

## Esto es lo que necesitas

- **Educación:** Máster (o título avanzado equivalente) en ciberseguridad y normativas internacional de ciberseguridad. Se valorarán certificaciones técnicas en ciberseguridad u otros campos pertinentes a las responsabilidades de la función.
- **Experiencia:** al menos seis años de experiencia progresiva liderando estrategias de ciberseguridad, auditorias y asesoramiento en normas y estándares internacionales relacionadas a la ciberseguridad, gestión de proyectos de tecnologías de información o unidades afines. Es requerido contar con experiencia comprobada trabajando en proyectos de ciberseguridad o transformación digital en el sector público (en particular, en el sector de estadísticas oficiales).
- **Idiomas:** Se requiere dominio de español y de inglés, oral y escrito. Se prefiere tener conocimientos adicionales de francés y portugués.

## Habilidades claves

**Campo técnico**

- Aprendizaje continuo
- Colaborar y compartir conocimientos
- Centrarse en los clientes
- Comunicar e influir
- Innovar y probar cosas nuevas

## Requisitos

- **Ciudadanía:** Usted es ciudadano de uno de nuestros 48 países miembros.
- **Consanguinidad:** No tiene miembros de su familia (hasta el cuarto grado de consanguinidad y segundo grado de afinidad, incluido el cónyuge) que trabajen en el BID, BID Invest o BID Lab.
- **Consideraciones en cuanto a la COVID-19:** la salud y la seguridad de nuestros empleados son nuestra principal prioridad. Como condición de empleo, el BID/BID Invest requiere que todos los nuevos empleados tengan la vacunación completa contra la COVID-19.

## Tipo de contrato y duración

- Tipo de Contrato: Consultor de Productos y Servicios Externos (PEC), suma alzada.
- Duración: 200 días en un periodo de 14 meses.

## Qué ofrecemos

El Grupo BID ofrece beneficios que responden a las diferentes necesidades y momentos de la vida de un empleado. Estos beneficios incluyen:

- Un paquete de **remuneración competitiva.**
- Una manera flexible de trabajar. Se le evaluará por entregable.

## Nuestra cultura

En el Grupo BID, trabajamos para todas las personas den lo mejor de sí y traigan a su verdadero yo al trabajo, estén dispuestas a intentar nuevos enfoques sin miedo, rindan cuentas de sus acciones y reciban una retribución por ellas.

La Diversidad, la Equidad, la Inclusión y el Sentido de Pertenencia (DEIB) son los pilares de nuestra organización. Celebramos todas las dimensiones de diversidad y animamos a que se postulen mujeres, LGBTQ+, personas con discapacidades, afrodescendientes e indígenas.

Nos cercioraremos de que a las personas con discapacidades se les brinden adaptaciones razonables para participar en el proceso de las entrevistas laborales. Si usted es un candidato calificado que tiene una discapacidad, envíenos un correo electrónico a diversity@iadb.org a fin de solicitar adaptaciones razonables para poder completar esta solicitud.

**Nuestro Equipo de Recursos Humanos revisa exhaustivamente cada solicitud.**

## Acerca del Grupo BID

El Grupo BID, compuesto por el Banco Interamericano de Desarrollo (BID), BID Invest y BID Lab, ofrece soluciones de financiamiento flexibles a sus países miembros para financiar el desarrollo económico y social a través de préstamos y subsidios a entidades públicas y privadas en América Latina y el Caribe.

## Acerca del BID

El Banco Interamericano de Desarrollo tiene como misión mejorar vidas. Fundado en 1959, el BID es una de las principales fuentes de financiamiento a largo plazo para el desarrollo económico, social e institucional de América Latina y el Caribe. El BID también realiza proyectos de investigación de vanguardia y ofrece asesoría sobre políticas, asistencia técnica y capacitación a clientes públicos y privados en toda la región.

**Síguenos:**

https://www.linkedin.com/company/inter-american-development-bank/

https://www.facebook.com/IADB.org

https://twitter.com/the_IDB

**HRD Término de Referencia** **ANEXO A**

**Consultor Servicios de consultoría profesional para Análisis de Sistemas**

**Ubicación**

El Grupo BID es una comunidad de personas diversas, versátiles y apasionadas, unidas para mejorar vidas en América Latina y el Caribe. Aquellos que trabajan con nosotros encuentran un propósito y hacen lo que más les gusta en un entorno inclusivo, colaborativo, ágil y gratificante.

**Acerca de este puesto de trabajo**

Estamos buscando un/a consultor que se encargará de realizar el análisis de los sistemas del MINFIN para determinar los datos técnicos de incidentes, vulnerabilidades potenciales de ciberseguridad, impactos potenciales a la confidencialidad y disponibilidad de los sistemas y disponibilidad de los datos.

**Esto es lo que harás**

(principales responsabilidades que contribuyen a los objetivos del equipo; no incluir detalles)

- Recopilar información acerca temas relacionados a la ciberseguridad como políticas, prácticas, medidas aplicadas, mediante revisión de documentos, entrevistas de personal del MINFIN, análisis de eventos, logs, visitas a dependencias del MINFIN, entre otros..
- Identificar y analizar posibles vulnerabilidades según la información recopilada.
- Analizar el riesgo potencial de las vulnerabilidades identificadas.
- Recomendar medidas para atender las vulnerabilidades y gestionar los riesgos.
- Al realizar lo anterior, elaborar y articular un informe consolidado.
- El informe consolidado incluirá un resumen ejecutivo, el listado de vulnerabilidades identificadas, su descripción, análisis, nivel de riesgo, y recomendaciones para su mitigación.
- Las recomendaciones serán caracterizadas también de manera que permite su priorización en un plan de trabajo, según aspectos como nivel de riesgo, costo, complejidad de implementación y el horizonte temporal recomendado para su implementación en el plazo inmediato, corto mediano o largo.
- Es posible entregar un número de informes enfocados en distintos aspectos del alcance a distintos momentos del proceso.
- Realizar una presentación de los hallazgos y recomendaciones.
- Atender comentarios del MINFIN, y del BID, y realizar ajustes al informe del proyecto; entregar el informe finalizado.
- Este alcance de proyecto consultoría no incluye apoyo en la implementación de medidas de mitigación, análisis de código, o actividades de hackeo ético.
- Las recomendaciones legales necesarias, conforme a las regulaciones laborales, para incorporar las faltas y responsabilidades legales (administrativas o penales, según corresponda) como parte del régimen de gestión de personal.
- Preparar al MINFIN para su certificación realizando una auditoría interna final para evaluar el cumplimiento de todos los requisitos de ISO 27001:2022 que incluya toda la documentación y evidencia necesaria para la auditoría de certificación externa,

manteniendo un control de cambios para asegurar que la documentación esté actualizada y refleje las prácticas actuales.

## Cronograma de Entregas y Pagos

Click or tap here to enter text.

| Entregable | Porcentaje | Fecha Estimada de Entrega |
|---|---|---|
| Plan de trabajo | 20% | Diciembre 2025 |
| Borrador del reporte de proyecto | 50% | Junio 2026 |
| Reporte final y presentación realizada | 30% | Octubre 2026 |

## Esto es lo que necesitas

- **Educación:** Doctorado, Maestría (o título avanzado equivalente) en computación, ingeniería informática, ciberseguridad o similar requerida. Se valorarán certificaciones técnicas en ciberseguridad u otros campos pertinentes a las responsabilidades de la función.
- **Experiencia:** 10 años o más de experiencia profesional y conocimiento práctico comprobado en proyectos a nivel organizacional de ciberseguridad, seguridad digital, seguridad de la información y similar.
- **Idiomas:** Se requiere dominio de español y de inglés, oral y escrito. Se prefiere tener conocimientos adicionales de francés y portugués.

## Habilidades claves

### Campo técnico

- Aprendizaje continuo
- Colaborar y compartir conocimientos
- Centrarse en los clientes
- Comunicar e influir
- Innovar y probar cosas nuevas

## Requisitos

- **Ciudadanía:** Usted es ciudadano de uno de nuestros 48 países miembros.
- **Consanguinidad:** No tiene miembros de su familia (hasta el cuarto grado de consanguinidad y segundo grado de afinidad, incluido el cónyuge) que trabajen en el BID, BID Invest o BID Lab.

- **Consideraciones en cuanto a la COVID-19:** la salud y la seguridad de nuestros empleados son nuestra principal prioridad. Como condición de empleo, el BID/BID Invest requiere que todos los nuevos empleados tengan la vacunación completa contra la COVID-19.

## Tipo de contrato y duración

- Tipo de Contrato: Consultor de Productos y Servicios Externos (PEC), suma alzada
- Duración: 200 días en un periodo de 10 meses.

## Qué ofrecemos

El Grupo BID ofrece beneficios que responden a las diferentes necesidades y momentos de la vida de un empleado. Estos beneficios incluyen:

- Un paquete de **remuneración competitiva.**
- Una manera flexible de trabajar. Se le evaluará por entregable.

## Nuestra cultura

En el Grupo BID, trabajamos para todas las personas den lo mejor de sí y traigan a su verdadero yo al trabajo, estén dispuestas a intentar nuevos enfoques sin miedo, rindan cuentas de sus acciones y reciban una retribución por ellas.

La Diversidad, la Equidad, la Inclusión y el Sentido de Pertenencia (DEIB) son los pilares de nuestra organización. Celebramos todas las dimensiones de diversidad y animamos a que se postulen mujeres, LGBTQ+, personas con discapacidades, afrodescendientes e indígenas.

Nos cercioraremos de que a las personas con discapacidades se les brinden adaptaciones razonables para participar en el proceso de las entrevistas laborales. Si usted es un candidato calificado que tiene una discapacidad, envíenos un correo electrónico a diversity@iadb.org a fin de solicitar adaptaciones razonables para poder completar esta solicitud.

**Nuestro Equipo de Recursos Humanos revisa exhaustivamente cada solicitud.**

## Acerca del Grupo BID

El Grupo BID, compuesto por el Banco Interamericano de Desarrollo (BID), BID Invest y BID Lab, ofrece soluciones de financiamiento flexibles a sus países miembros para financiar el desarrollo económico y social a través de préstamos y subsidios a entidades públicas y privadas en América Latina y el Caribe.

## Acerca del BID

El Banco Interamericano de Desarrollo tiene como misión mejorar vidas. Fundado en 1959, el BID es una de las principales fuentes de financiamiento a largo plazo para el desarrollo económico, social e institucional de América Latina y el Caribe. El BID también realiza proyectos de investigación de vanguardia y ofrece asesoría sobre políticas, asistencia técnica y capacitación a clientes públicos y privados en toda la región.

**Síguenos:**

https://www.linkedin.com/company/inter-american-development-bank/

https://www.facebook.com/IADB.org

https://twitter.com/the_IDB

**Terms of Reference**

**Cybersecurity Incident Remediation, Analysis Response & Investigation Services**

Guatemala

*GU-T1359*

*Respuesta a ciberataques y mejora de la ciberseguridad en el Ministerio de Finanzas Públicas de Guatemala*

1. Background and Justification

1.1. The increasing use of ICT in LAC is a catalyst for economic and social progress; however, it introduces inherent cybersecurity risks which must be managed on a continued basis, else citizen safety and the public trust in ICT, including consumer faith in online transactions and access to digital public services, may be negatively affected. Thus, strengthening cybersecurity is essential to safeguard citizens' rights in the digital sphere, such as privacy and property, to promote citizens' trust in digital technologies, and to support economic growth through safe digital transformation. Citizens must be assured that the digital systems they use for their personal or professional activities, as well as those that involve their personal data, possess adequate security measures to guarantee the integrity, confidentiality, and availability of their information and the services they depend on.

1.2. In this context, being prepared, and knowing where we stand, is key. The Inter-American Development Bank (IDB) carries out assessments to capture the evolving capacities of its member states to defend against the growing threats in the cyberspace. The 2020 Regional Cybersecurity Maturity Report: "Risks, Progress and the Way Forward in Latin America and the Caribbean", developed in partnership with the Organization of American States (OAS), showed that countries were in varying stages of development in their preparedness to face cybersecurity challenges, but generally still had ample room for improvement. In the case of Guatemala, its maturity in cybersecurity public policy across 53 indicators was evaluated at less than 2.0 out of 5.0 points, on average. Specifically, Guatemala has approved a National Cybersecurity Strategy in 2018, however its objectives and action plan have not yet been fully realized. In 2019, Guatemala approved a Cybercrime Law. Guatemala does not have a national-level cybersecurity agency or a critical infrastructure protection plan. In this context, the government has limited capacity to prevent, detect and respond to cyberattacks.

1.3. These underlying cybersecurity vulnerabilities occasionally result in high-profile cybersecurity attacks. In late November 2023, MINFIN announced it has suffered from a cyberattack, affecting the availability of some of its information and systems. Some of

MINFIN's main information systems include SICOIN (Sistema de Contabilidad Integrada), used to manage government payments and accounts, GuateCompras, used to manage government purchases, and Guatenominas, used to manage government salaries. The reduced availability of such systems impacted the orderly realization of the government's financial processes, and the trust in their ongoing stability.

1.4. The IDB has responded to cybersecurity challenges in LAC with several capacities building efforts, including loan operations and specific technical assistance. In Guatemala, GU-L1175 "Program for the Digital Transformation of Guatemala for Inclusive Access to Connectivity" (about to begin implementation) includes support for cybersecurity investment. Guatemala has also benefitted from regional capacity building activities such as the IDB-OAS regional cybersecurity maturity study, the IDB's National Cybersecurity Leadership course, regional and subregional events and study courses dealing with cybercrime and cybersecurity such as for investigators, customs, prisons, among others.

1.5. The IDB is in a unique position to support MINFIN's cybersecurity capacity building, given our ongoing investment and technical assistance projects, and proven record leveraging technical support from the most advanced countries in cybersecurity worldwide. For example, the government of Israel has supported capacity in cybersecurity throughout Latin America since 2016 and is currently involved providing access for the region's cybersecurity professionals to the most advanced training, knowledge, expertise and best practices worldwide (RG-T2788, RG-T4010). The contexts of Japan, Korea and Spain also portend meaningful lessons and technical support in state capacity and the co-production of cybersecurity (TT-T1137, SU-T1158, RG-T4172, RG-T3024 and RG-T3741).

## 2. Objectives

2.1. The objective of this contract is to support Ministry of Finance of Guatemala affected by the above referenced cybersecurity incident to analyze, respond and investigate their IT systems, protect those systems from the current and future potential attacks and resume normal services.

## 3. Key Activities

Consultancy activities may include multiple instances of the following kinds of professional services, as deemed necessary, planned, agreed and approved in accordance with section 4.1 during contract execution:

3.1. **Forensics:** Assist the government's IT team in determining and reporting any aspects related to the attack, such as information accessed, information exfiltrated, timeline and events of the attack.

3.2. **Remediation:** Assist the IT team in testing said systems for attacker presence and removing any persistent threats.

3.3. **Hardening review**: Following the IT systems hardening, the Government or independent consultants may review and test the recommendations' implementation by the Consulting Firm (realized through activity **Error! Reference source not found.**), potentially by follow-up calls, technical testing, or ethical hacking methods. The contracted firm will be responsible for attending remaining gaps identified by the review.

3.4. **Review and advice** regarding security policies, systems design, and contingency plans.

3.5. **Ethical hacking:** Perform ethical hacking services in case these are requested:

3.5.1. **Targets**: The Client, the Consulting Firm and the IDB will hold a dialogue to define the target systems and techniques applicable to be tested in the context of any specific Request. These may include Client Infrastructure, Applications or both:

3.5.1.1. Infrastructure: Conventional attacks on exposed IT Infrastructure with a focus on identifying and exploiting software, configuration or credential flaws.

3.5.1.2. Applications: Testing web and mobile components with a focus on obtaining access to or modifying sensitive information, or on building client-side attacks that could be used in other testing techniques (e.g., phishing).

3.5.2. **Tools**: The penetration testing will be carried out using both automated and manual tools.

3.5.3. **Methods**: The penetration testing will usually be done using "Gray Box" methods; In some cases, "White Box" or "Black Box" methods may be selected in mutual agreement.

3.6. **Monitoring:** Implement market-leading monitoring solution(s) on the IT systems, of kinds to be specified during contract execution, such as Endpoint Detection and Response (EDR), to detect possible ongoing, recurrent or future attacks. Said monitoring is required to bring systems back online and resume normal services. The contracted firm will provide the monitoring solutions and support the IT team in reviewing and handling findings detected by these solutions, for an interim period the duration of which will be agreed and approved during contract execution in accordance with section 4.1. During that period, monitoring solutions would be procured and implemented for the long term directly by the Government.

3.7. Any other professional cybersecurity services, to be agreed.

4. Contract Execution

4.1. **Planning and approval**: The Consulting Firm will develop written plan(s) to realize instances of abovementioned activities, of the types denoted in **Error! Reference source not found.** through 3.63.7, as will be required during contract execution. Each plan will specify aspects such as the activities to be carried out, responsibilities of the Consulting Firm and the Government, methodologies and tools used, specific systems in the activity's scope, the time schedule and the number of service hours charged to carry out each activity. Said plan(s) must be approved in writing by the contract supervisors prior to implementation.

4.2. **Implementation**: The Consulting Firm will perform the services according to the approved plan(s), prioritizing speed and efficiency of execution while realizing the determined objectives.

4.3. **Reporting:** The Consulting Firm will report in writing to the IDB and the Government IT team regarding the implementation of the abovementioned plans and activities, as well as on findings and recommendations to correct any deficiencies. The report shall include: an executive summary, the methodology used, activities carried out, findings grouped by levels of risk, screenshots documenting activities and findings, specific and general recommendations.

4.4. **Coordination:** The Consulting Firm will carry out the services in coordination -as relevant- with the affected government units, their IT teams, cybersecurity government agencies, and other consultants engaged by the government or by the IDB, each performing their respective roles and tasks.

4.5. **Status meetings:** Regular meetings will be held to follow-up on the execution of project activities, including representatives of the Consulting Firm, the Government, and the IDB. They are expected to be held on an as-needed frequency, initially once a week.

4.6. **Personnel:** The consulting firm would present the specific professionals who would take part in any of the activities to the Government and to the IDB, detailing their experience and credentials, and obtain approval for their participation prior to involving each and any specific professional in said activities.

5. Expected Outcome and Deliverables

5.1. Hours of cybersecurity professional services performed through activities **Error! Reference source not found.** through 3.63.77 as defined and approved.

5.2. Specific deliverables will include:
5.2.1. Short form written plan(s), delivered through activity 4.14.1;
5.2.2. Detailed reports, delivered through activity 4.3.

6. Project Schedule and Milestones

6.1. The totality of services performed shall be carried out within the approved budget and timeframe for the contract. Specific activities therein, including reporting (activity 4.3), shall be executed and reported within the number of service hours and timeframes established by the approved plans (activity 4.1).

6.2. To meet the project schedule, full and timely availability of Client IT team, independent consultants and IDB points of contact are confirmed.

7. Acceptance Criteria

7.1. The Consulting Firm shall maintain regular communication with the point of contact at the IDB and the Government IT team, in carrying out the activities and developing all deliverables described in this contract. The Consulting Firm shall obtain IDB's approval for the completion of each of the planned activities before associated payments are processed.
7.2. An IDB representative will be copied in all communications between the Consulting Firm and the Client.
7.3. All written deliverables will be presented in professional-level Spanish.
7.4. Deliverables will be provided in editable formats (i.e. Microsoft Word, PowerPoint, e-mail etc.), as well as any finalized formats.

8. Confidentiality

8.1. The Consulting Firm and its employees or agents are aware that in discharging their obligations pursuant to this Agreement, they may have access to privileged, confidential and/or proprietary information of the IDB, the Government or of another party in their possession. Under no circumstances, except with the IDB's express written permission, shall Supplier and its employees or its agents copy, reproduce, sell, assign, license, market, transfer, give or otherwise disclose to any person or organization, in any manner or form, now or after the expiration of the Agreement,

such Confidential Information or any part thereof. The Consulting Firm must handle, and if needed temporarily retain, all such information under the appropriate safeguards.

8.2. Upon request by the Bank or upon completion of the Work, Supplier will immediately return to the Bank or Government at Supplier's expense all Confidential Information, documents, or data the Supplier accessed through this engagement, and all copies thereof.

9. Supervision and Reporting

9.1. The IDB shall supervise the execution of the activities and completion of the deliverables indicated in these terms of reference and approve all payments. The points of contact at the IDB for all matters related to this contract will be Ariel Nowersztern, Senior Cybersecurity Specialist (arieln@iadb.org).

10. Schedule of payments

| Deliverable | Percentage |
|---|---|
| As per agreed number of service hours per each approved plan, on approval of deliverable 5.1 | Up to 100% |
| TOTAL | 100% |

**HRD Término de Referencia** **ANEXO A**

**Terms of Reference**

## Designing a Modern Security Operations Center (SOC) for MINFIN Guatemala

Guatemala

*GU-T1359*

*Respuesta a ciberataques y mejora de la ciberseguridad en el Ministerio de Finanzas Públicas de Guatemala*

1. Background and Justification

1.1 The increasing use of ICT in LAC is a catalyst for economic and social progress; however, it introduces inherent cybersecurity risks which must be managed on a continued basis, else citizen safety and the public trust in ICT, including consumer faith in online transactions and access to digital public services, may be negatively affected. Thus, strengthening cybersecurity is essential to safeguard citizens' rights in the digital sphere, such as privacy and property, to promote citizens' trust in digital technologies, and to support economic growth through safe digital transformation. Citizens must be assured that the digital systems they use for their personal or professional activities, as well as those that involve their personal data, possess adequate security measures to guarantee the integrity, confidentiality, and availability of their information and the services they depend on.

1.2 In this context, being prepared, and knowing where we stand, is key. The Inter-American Development Bank (IDB) carries out assessments to capture the evolving capacities of its member states to defend against the growing threats in the cyberspace. The 2020 Regional Cybersecurity Maturity Report: "Risks, Progress and the Way Forward in Latin America and the Caribbean", developed in partnership with the Organization of American States (OAS), showed that countries were in varying stages of development in their preparedness to face cybersecurity challenges, but generally still had ample room for improvement. In the case of Guatemala, its maturity in cybersecurity public policy across 53 indicators was evaluated at less than 2.0 out of 5.0 points, on average. Specifically, Guatemala has approved a National Cybersecurity Strategy in 2018, however its objectives and action plan have not yet been fully realized. In 2019, Guatemala approved a Cybercrime Law. Guatemala does not have a national-level cybersecurity agency or a critical infrastructure protection plan. In this context, the government has limited capacity to prevent, detect and respond to cyberattacks.

1.3 These underlying cybersecurity vulnerabilities occasionally result in high-profile cybersecurity attacks. In late November 2023, MINFIN announced it has suffered from a cyberattack, affecting

the availability of some of its information and systems. Some of MINFIN's main information systems include SICOIN (Sistema de Contabilidad Integrada), used to manage government payments and accounts, GuateCompras, used to manage government purchases, and Guatenominas, used to manage government salaries. The reduced availability of such systems impacted the orderly realization of the government's financial processes, and the trust in their ongoing stability.

1.4 The IDB has responded to cybersecurity challenges in LAC with a number of capacities building efforts, including loan operations and specific technical assistance. In Guatemala, GU-L1175 "Program for the Digital Transformation of Guatemala for Inclusive Access to Connectivity" (about to begin implementation) includes support for cybersecurity investment. Guatemala has also benefitted from regional capacity building activities such as the IDB-OAS regional cybersecurity maturity study, the IDB's National Cybersecurity Leadership course, regional and subregional events and study courses dealing with cybercrime and cybersecurity such as for investigators, customs, prisons, among others.

1.5 The IDB is in a unique position to support MINFIN's cybersecurity capacity building, given our ongoing investment and technical assistance projects, and proven record leveraging technical support from the most advanced countries in cybersecurity worldwide. For example, the government of Israel has supported capacity in cybersecurity throughout Latin America since 2016 and is currently involved providing access for the region's cybersecurity professionals to the most advanced training, knowledge, expertise and best practices worldwide (RG-T2788, RG-T4010). The contexts of Japan, Korea and Spain also portend meaningful lessons and technical support in state capacity and the co-production of cybersecurity (TT-T1137, SU-T1158, RG-T4172, RG-T3024 and RG-T3741).

2. Objectives

The objective of this contract is to support the MINFIN governmental Office to design a Security Operations Center (SOC) to improve MINFIN's capacity to respond to cybersecurity incidents and threats.

3. Key Activities

**3.1. Activity #1. Designing a modern Security Operations Center (SOC)** for MINFIN, including:

3.1.1. Identifying the requirements, needs, technical specifications, services and functionality attending to MINFIN's network, systems and data.

3.1.2. Designing the SOC meeting these identified aspects. The design would include business and operational processes, procedures, organizational structure,

personnel and training, technology architecture and tools including licensing considerations, metrics and levels of services, its adaptability, growth, resilience and high-availability aspects, process and schedule of establishment, training, and the operationalization of services.

3.1.3. Drafting the technical section of the terms of reference, prerequisites and evaluation criteria for contracting a specialized integrator to establish and operationalize the SOC according to the design; defining milestones and deliverables; estimating the project's detailed budget and total cost; and identifying considerations for or evaluation of potential locations for the SOC.

3.1.4. Notes:

3.1.4.1. Initial high-level objectives of the SOC project include protecting the confidentiality, integrity and availability of MINFIN's systems and data, especially those related to its critical role in the governmental sector, improving the detection of and response to cybersecurity incidents affecting MINFIN systems by implementing international best practices.

**3.2. Activity #2: Project delivery**

3.2.1. Performing a presentation of the draft project deliverables including findings, recommendations, design. These sessions will be carried out in person in Guatemala and are expected to take the form of a two- or three- day workshop.

3.2.2. Collecting feedback, incorporating any necessary adjustments to the deliverables and finalizing them. It is expected that the consulting firm will perform interviews with key stakeholders in the country, including management and Board members of MINFIN.

3.2.3. Developing local capacity building and ensuring sustainability of the analysis and recommendations are an important activity of this assignment, and thus consulting firms are encouraged to establish partnerships with other local and regional consulting firms.

4. Expected Outcome and Deliverables

- Deliverable 1 -- Project workplan and schedule.
- Deliverable 2 -- Draft report on activity #1
- Deliverable 3 -- Final report on activity #1 after carrying out activity #2

5. Project Schedule and Milestones

**5.1.** The work shall be carried out in the span of eight (8) months from the time of contract signature,

of which six (6) months would be the main project schedule and two (2) months would be reserved for administrative finalization.

**5.2.** At least two on-site visits at MINFIN's premises by the consulting team are expected, the first for gathering information about the current situation to be used for the assessment, design and recommendations activities; and the second for conducting the project delivery workshop.

6. Major Selection Criteria

**6.1.** The Consultant (potentially through one of the firms partnering to deliver this project or senior individual consultants significantly engaged in project delivery) should comply with the following requirements and qualifications.

**6.2.** Must have an established practice in Cybersecurity Consulting with a proven record and experience in advising:

6.2.1. International operators of governmental infrastructure, preferably in the finance sector.

6.2.2. Performing cybersecurity evaluation and improvement recommendations for IT systems and networks.

6.2.3. Designing, implementing or operating security operations centers.

6.2.4. The portfolio of previous reference advisory projects would preferably include similar activities, elements and methods to those required for this project.

**6.3.** Consulting Team:

6.3.1. The Lead Consultant must have at least 10 years of proven and successful experience in Cybersecurity with at least four years of experience in cybersecurity.

6.3.2. At least one significantly engaged Consultant of the team must have significant proven experience in securing IT infrastructure networks and systems.

6.3.3. At least one significantly engaged Consultant of the team must have significant proven experience in the design, implementation and/or operation of Security Operation Centers.

6.3.4. Detailed roles and responsibilities within the consulting team will be assigned to ensure comprehensive coverage of all aspects of the assessment. These includes a project leader and leads for the different major activities described above. The same person may have more than one role or responsibility in line with their professional background.

6.3.5. Relevant professional certifications, such as OSCP (Offensive Security Certified Professional) and CEH (Certified Ethical Hacker), certifications in implementing standards, Certified in Risk and Information Systems Control (CRISC), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), Certified Information

Systems Security Professional (CISSP) and specific relevant experience in with the technologies and operations of energy sector OT systems will be evaluated.

**6.4.** The proposed consulting methodology would be coherent with this project description, incorporate recognized professional standards and best practices applicable to this project scope. Methodological suggestions and project plans for improving on the steps described above, while realizing the project objectives and maintaining its deliverables, may be considered but must be approved in writing by the project supervisors.

**6.5.** Please include relevant information to evaluating the abovementioned criteria in your technical submission. Information may include, for example, the profile of your cybersecurity consulting activities, descriptions of reference consulting projects, proposed project methodology, and consultant CVs.

7. Reporting Requirements, Deliverable Acceptance Criteria and Supervision

**7.1.** Security Measures: All data collected and generated during this project will be strictly confidential, stored securely, will be transferred to the client and eliminated from the consultant's possession at the end of the project or when requested, and may not be shared, kept or reused without explicit written permission. Access to confidential data will be restricted to authorized personnel only.

**7.2.** Deliverables should be organized, paginated and designed for usability, clarity and to effectively communicate the consulting products.

**7.3.** Success will be measured by the ability to comprehensively identify and effectively exploit vulnerabilities, the comprehensiveness of the final report, and the feasibility of the recommended security enhancements.

**7.4.** Review and Sign-off: The final report will undergo a thorough review process involving both technical leads and senior management. Approval will be based on the accuracy, depth, and clarity of the findings and recommendations.

**7.5.** Language: Project communications, drafts, deliverables, and final products will be in professional level, edited English or Spanish.

**7.6.** File formats: All deliverables should be shared in editable file formats (such as Word, Excel, PowerPoint etc.), in addition to any other format included for convenience.

**7.7.** The consulting firm shall maintain regular and periodic communication with the points of contact at the IDB and MINFIN, in carrying out the activities and developing all deliverables described in

this contract. IDB and MINFIN may provide comments on deliverables to be attended before deliverables can be finalized.

**7.8.** The consulting firm shall obtain the IDB's approval of each deliverable before associated payments will be processed.

**7.9.** The IDB and shall supervise the execution of the activities and completion of the deliverables indicated in these terms of reference and approve all payments. An IDB representative will be copied in all communications between the Consulting Firm and MINFIN. The point of contact at the IDB for all matters related to this contract will be Mr. Ariel Nowersztern (arieln@iadb.org).

8. Schedule of payments

| Deliverable | Percentage |
|---|---|
| Approval of deliverable 1 | 20% |
| Approval of deliverable 3 | 40% |
| Approval of deliverable 5 | 40% |
| TOTAL | 100% |