

## ABSTRACTO DE COOPERACIÓN TÉCNICA

### I. Información Básica del Proyecto

▪ País/Región:	ECUADOR/CAN - Grupo Andino
▪ Nombre de la CT:	Fortalecimiento de Servicios Tecnológicos y Seguridad Informática del Ministerio de Relaciones Exteriores y Movilidad Humana (MREMH)
▪ Número de CT:	EC-T1399
▪ Jefe de Equipo/Miembros:	García Mejía, Mauricio (IFD/ICS) Líder Del Equipo; Porrua Vigón, Miguel Ángel (IFD/ICS) Jefe Alternativo del Equipo de Proyecto; Nowersztern, Ariel (IFD/ICS); TOBAR ARIAS, ELSA KATHERINE (CAN/CEC); Catano Guzman, Mariana (IFD/ICS); Hidrovo, Marcela Vanessa Velazquez, Gumersindo G. (VPC/FMP); Verissimo Da Silva, Carolina; Azevedo, Andrea Pereira (LEG/SGO)
▪ Taxonomía:	Apoyo al Cliente
▪ Número y nombre de la operación que apoyará la CT:	N/A
▪ Fecha del Abstracto de CT:	27 Apr 2018
▪ Beneficiario:	República del Ecuador
▪ Agencia Ejecutora:	Ministerio De Relaciones Exteriores
▪ Financiamiento solicitado del BID:	\$ 200,000.00
▪ Contrapartida Local:	\$ 0.00
▪ Periodo de Desembolso:	30 months
▪ Tipos de consultores:	Individuos; Empresas
▪ Unidad Responsable de Preparación:	División de Innovación para Servir al Ciudadano
▪ Unidad Responsable de Desembolso:	Representación Ecuador
▪ CT incluida en la Estrategia de País (s/n):	No
▪ CT incluida en CPD (s/n):	No
▪ Alineación a la Actualización de la Estrategia Institucional 2010-2020:	Capacidad institucional y estado de derecho

### II. Objetivos y Justificación de la CT

- 2.1 El Objetivo General que persigue esta CT es fortalecer la Seguridad Informática de las Misiones Diplomáticas del Ecuador en el Mundo, a través de (i) el diseño de un SGSI y plan continuidad del negocio; y (ii) la implementación de Redes Privadas Virtuales (VPN), y a fin de contribuir al cumplimiento a la normativa legal vigente y mitigar los riesgos de seguridad informática a los que actualmente está expuesto el MREMH en la prestación de sus servicios virtuales a través del ESIGEX.
- 2.2 El problema principal que pretende resolver esta CT son las deficiencias en la seguridad informática de las misiones diplomáticas del Ecuador en el Mundo. Según una evaluación internacional hecha por el BID, Ecuador se encuentra en nivel inicial o formativo en 47 de 49 dimensiones de madurez de ciberseguridad. Ecuador no cuenta con una estrategia nacional de ciberseguridad ni con manejo centralizado de la ciberseguridad a nivel gubernamental. Según una evaluación internacional hecha por el ITU, Ecuador se encuentra en la posición 66 de 193 entre los países a nivel mundial. Según indicado en un reporte del MREMH, las misiones diplomáticas cuentan actualmente con bajos controles existentes de la EGSi, no cuentan con comunicación encriptada con Quito, ni con protección contra amenazas a nivel de las redes o a nivel de las computadoras. Esta situación está desalineada con prácticas básicas de protección informática, sobre todo en caso de una organización nacional sensible y con varios sitios dispersos. En este sentido, se han reportado numerosos incidentes de

seguridad informática en las misiones diplomáticas, como secuestro y robo de información, divulgación no autorizada, mal funcionamiento del hardware, software, red, etc. Por falta de herramientas de detección, se estima que la mayoría de los ataques cibernéticos intentados no se detectan por el MREMH.

- 2.3 Los análisis preliminares de riesgos indican que estos incidentes no han sido gestionados adecuadamente debido los siguientes factores causales: (i) gestión desintegrada de la seguridad informática, con deficitaria aplicación de controles y gestión de riesgos, así como falta de redundancias; y (ii) carencia de canales de comunicación seguros entre el MREMH y las más de 100 misiones diplomáticas del Ecuador en el mundo.
- 2.4 El MREMH se considera una entidad sensible del gobierno ecuatoriano. El MREMH publica en internet servicios y aplicaciones web tanto de uso interno y externo las cuales han sido desarrolladas de forma heterogénea, sin controles de seguridad adaptados a las amenazas y vulnerabilidades actuales. En este sentido, el aplicativo más crítico es el Sistema de Gestión del Servicio Exterior (ESIGEX) que es además el aplicativo core del Ministerio, el cual se utiliza remotamente sin que cuente con la seguridad adecuada para su funcionamiento.
- 2.5 El Fortalecimiento de la Seguridad Informática de las Misiones Diplomáticas del Ecuador en el mundo constituye un proyecto de importancia y trascendencia debido a que: (i) Contribuye al cumplimiento de los objetivos estratégicos del MREMH de lograr que los servicios que brinda el MREMH sean de calidad, eficientes y accesibles para todos los ciudadanos, incrementar la protección de los Ecuatorianos en el exterior y la calidad, eficiencia y accesibilidad de los servicios que brinda MREMH, en el Ecuador y en el exterior; (ii) Apoya significativamente en el cumplimiento de la normativa legal vigente en temas de seguridad informática; (iii) mitiga riesgos a los que están expuestos los sistemas informáticos de uso interno y exclusivo del MREMH, publicados en el Internet. (iv) contribuye al fortalecimiento del Sistema de Gestión de Seguridad de la Información (SGSI) institucional; (v) es la solución más integral y con menor impacto operativo y técnico, debido a que implica el reemplazo ni construcción de nuevos sistemas informáticos; y (vi) constituye un referente de gestión de seguridad informática para otras entidades del estado.

### **III. Descripción de las Actividades y Resultados**

- 3.1 **Componente 1.- Fortalecimiento del Sistema de Seguridad de la Información.** El objetivo de este componente es apoyar el desarrollo de un sistema de seguridad de información que permite gestionar adecuadamente los riesgos de seguridad de la información del MREMH. Para ello, se financiarán las siguientes actividades: (i) Diseño del sistema de gestión de seguridad de la información, que incluye el levantamiento del estado actual de seguridad de la información, definición del alcance (partes o procesos de la organización que van a ser incluidos, los procesos críticos, que es lo que se quiere proteger y por dónde empezar), revisión y establecimiento de políticas de seguridad, organización de la seguridad, activos de Seguridad de la Información, análisis de riesgos, definición y aplicación de controles (EGSI/27002:2013) y software de gestión del SGSI; y (ii) Diseño del plan de continuidad del negocio, que incluirá levantamiento del estado actual, definición del alcance, análisis de la organización, estrategia de continuidad, pruebas, mantenimiento, revisión y estrategias de concientización. Como resultado de este componente, se contará con procedimientos, instructivos y guías de los productos desarrollados para la gestión de seguridad de la información en el MREMH.
- 3.2 **Componente 2.- Fortalecimiento de la seguridad de los canales de comunicación entre el MREMH y las misiones diplomáticas.** El objetivo de este componente es apoyar la implementación de algunos componentes del sistema de seguridad de la información desarrollado en el componente anterior. Para ello, el componente financiará

las siguientes actividades: (i) Equipamiento para implementación de VPN's entre la planta central de Quito y las misiones diplomáticas alrededor del mundo; y (ii) capacitación y certificación del personal del MREMH en competencias críticas para la seguridad de la información, tales como Certificación ISO 27001 Implementador; Certificación ISO 22301 Implementador; Certified Ethical Hacker CEH; Mikrotik MTCNA, entre otros. Como resultado de este componente, se espera contar con 102 Misiones Diplomáticas conectadas y gestionadas a través de los canales de VPN, así como con personal certificado.

#### IV. Presupuesto

##### Presupuesto Indicativo

Actividad/Componente	BID/Financiamiento por Fondo	Contrapartida Local	Financiamiento Total
Componente 1.- Fortalecimiento del Sistema de Seguridad de la Información.	\$ 83,000.00	\$ 0.00	\$ 83,000.00
Fortalecimiento de la seguridad de los canales de comunicación entre el MREMH y las misiones diplomáticas	\$ 117,000.00	\$ 0.00	\$ 117,000.00
Total	\$ 200,000.00	\$ 0.00	\$ 200,000.00

#### V. Agencia Ejecutora y Estructura de Ejecución

- 5.1 La CT será ejecutada por el Ministerio de Relaciones Exteriores y Movilidad Humana (MREMH), que es el rector de la política internacional y es responsable de la gestión y coordinación de esta, la integración latinoamericana y la movilidad humana. La unidad responsable de la ejecución de la CT será el Coordinación General de Tecnologías de la Información y Comunicación (CGTIC), a través de la Dirección de Infraestructura, Operaciones y Seguridad de TI (DIOSTI), que cuenta con 18 funcionarios con título de tercer nivel y experiencia en redes y telecomunicaciones, incluyendo un área de Gestión de Evaluación y Seguridad Informática. La CGTIC será responsable de los aspectos administrativos incluyendo: La presentación al Banco del plan de ejecución del proyecto, Informes trimestrales de avance del proyecto, Supervisión y Monitoreo de las actividades relacionadas al proyecto, Velar por el cumplimiento de lo estipulado en el convenio de CT y en los procedimientos y políticas del BID, Evaluación final del proyecto. La DIOSTI se encargará de la ejecución técnica incluyendo: Ejecución técnica del proyecto conforme al plan presentado por la CGTIC, Gestión de Riesgos técnicos inherentes al proyecto, Reporte mensual de avances.
- 5.2 Debido a la naturaleza del proyecto se designará un funcionario de carrera, perteneciente a la DIOSTI del Área de Gestión y Evaluación de Seguridad, como gerente del proyecto quien será responsable de Coordinar la ejecución administrativa y técnica del proyecto. Los desembolsos seguirán las normas y procedimientos del Banco, para lo cual se entregarán anticipos financieros en función de una proyección de gastos de seis meses.
- 5.3 La adquisición de bienes del programa se realizará de conformidad con las Políticas para Adquisición de Bienes y Obras financiados por el BID respectivamente, de acuerdo con lo establecido en el convenio de la CT y el Plan de Adquisiciones. El seguimiento del proyecto se realizará a través de informes semestrales de progreso y reuniones trimestrales de seguimiento del avance físico y financiero entre la CGTIC y el equipo del Banco, con el fin de coordinar acciones y actividades que aseguren su buena ejecución y el logro de sus metas y objetivos. El Jefe de Equipo del Proyecto del Banco,

con apoyo de la oficina del Banco en Ecuador (CAN/CEC), supervisará el proyecto. El MREMH, a través de la CGTIC, reportará al Banco el avance y seguimiento a la ejecución del proyecto incluyendo: Detalle de las actividades, productos y resultados alcanzados; Evaluación del avance de los indicadores de información financiera; evaluación de la ejecución física (incluyendo identificación de obstáculos encontrados y medidas de mitigación tomadas) y lecciones aprendidas; la actualización del plan operativo anual, del plan de adquisiciones/contrataciones y del cronograma de utilización de los recursos para el semestre siguiente.

## **VI. Riesgos Importantes**

- 6.1 Se estima que el proyecto podría tener los siguientes riesgos: 1. La Disponibilidad de tiempo de los funcionarios para las capacitaciones 2. Debido a la dispersión geográfica, diferencia horaria y otros factores los trabajos podrían no estar bien coordinados o las autoridades locales desinformadas. 3. Debido a los procesos administrativos internos de la institución, no se disponga a tiempo de los técnicos en los 102 sitios de la implementación. 4. Que el comportamiento de la solución no sea el esperado debido a la diversidad de factores que influyen en la comunicación a largas distancia, la legislación y la disponibilidad de tecnología de cada país.

## **VII. Salvaguardias Ambientales**

- 7.1 La clasificación ESG para esta operación es "indefinida".