

TÉRMINOS DE REFERENCIA

Consultoría para el diseño del plan de acción para la implementación del CSIRT.gov.br y ejecución de un proyecto piloto.

1. Antecedentes y Justificación

El COVID-19 ha acelerado la transformación digital de nuestras sociedades, y la ciberseguridad ha pasado a ocupar un lugar central entre las preocupaciones del mundo. Según un estudio realizado por Enterprise Insight en 2020¹, el 78% de los líderes de TI considera que sus organizaciones no cuentan con las medidas apropiadas de ciberseguridad. A su vez, de acuerdo al Global Risk Report² del Foro Económico Mundial la ciberseguridad se ubica entre los cinco riesgos más importantes que enfrentan las empresas.

La digitalización del sector público brasileño lograda recientemente trae un importante desafío: Desarrollar capacidades en Ciberseguridad. Si bien el gobierno federal cuenta con una estrategia nacional de ciberseguridad aprobada en 2020 y se posiciona sobre la media de madurez de la región, según el estudio de Madurez en Ciberseguridad³ realizado por el BID y la OEA en 2020, subsisten desafíos de coordinación, operacionales y de talento humano. Esta situación se replica también, pero de forma más severa, a nivel de los gobiernos estaduais, en un contexto de cada vez mayores ataques que vienen generando interrupciones en la entrega de servicios clave como salud o justicia. Brasil formaba parte del Top 10 Global Threat Rank y ocupaba la posición 70 de 175 países en el ranking del Índice Global de Ciberseguridad.

La Secretaria de Gobierno Digital (SGD) del Ministerio de Economía, en su rol de órgano central de administración de los recursos de tecnología del Gobierno Federal, ofrece la plataforma de servicios compartidos de la administración federal y define las mejores prácticas en el uso de TIC. Entre estas actividades, dicha secretaría se encuentra trabajando en el desarrollo de sus capacidades mediante la creación de un Centro de Respuesta a Incidentes de Ciberseguridad (CSIRT) y un Centro de Excelencia en Ciberseguridad.

2. Objetivos

El objetivo de esta consultoría es realizar un diagnóstico de la situación actual de la gestión de incidentes de la SGD; diseñar y dimensionar un roadmap de implementación de un CSIRT para los servicios de gobierno digital según el análisis realizado; e implementar un plan piloto de dicho CSIRT

¹ <https://finance.yahoo.com/news/78-lack-confidence-company-cybersecurity-153000182.html?guccounter=1>

² http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

³ <https://www.iadb.org/ciberseguridad2020>

3. Actividades Clave

Las principales actividades que se estima el contractual deberá realizar son:

- (i) Elaborar un análisis de la situación actual de la SGD para identificar las principales necesidades en términos de detección y respuesta a incidentes de ciberseguridad, teniendo en cuenta las demás iniciativas existentes en el gobierno y realizar una estimación del dimensionamiento requerido del CSIRT.
- (ii) Elaborar un diseño del CSIRT, incluyendo: Objetivos, servicios recomendados, infraestructura necesaria, la integración con terceras partes, capacitación recomendada y presupuestos estimados basados en el análisis de la actividad (i).
- (iii) Desarrollo de un plan de acción para la implementación del CSIRT diseñado, explicitando: las principales necesidades, la propuesta de diseño, cronograma de implementación y estimación presupuestal.
- (iv) Implementación de un proyecto piloto del CSIRT implantando herramientas de software libre para la gestión de incidentes, recolección y análisis de logs de 3 sistemas, plataforma para threat intelligence y diseño del procedimiento de respuesta a incidentes.

4. Resultados y Productos Esperados

La firma presentará 4 entregables:

- (a) Informe de relevamiento correspondiente a la actividad (i) al mes de ser contratada;
- (b) Diseño del CSIRT correspondiente a la actividad (ii) a los 4 meses de ser contratada;
- c) Desarrollo de un plan de acción, correspondiente a la actividad 3 (iii) a los 8 meses de ser contratada ;
- d) Proyecto piloto implementado, correspondiente con la actividad 4 (iv) a los 4 meses de ser contratada

5. Requisitos de los Informes

Los informes deben ser validados previamente a su aceptación por parte del Banco en coordinación con el cliente. Los mismos deben estar en idioma Portugués o Inglés.

6. Requisitos de la firma

Las firmas consultoras interesadas deberán proporcionar información que indique que están calificadas para suministrar los servicios (folletos, descripción de trabajos similares, experiencia en condiciones similares, disponibilidad de personal que tenga los conocimientos pertinentes, etc.). En particular deberán demostrar experiencia en consultorías de ciberseguridad, experiencia en protección de infraestructuras críticas y políticas públicas. Las firmas consultoras elegibles se pueden asociar como un emprendimiento conjunto o en un acuerdo de sub-consultoría para mejorar sus calificaciones. Dicha asociación o emprendimiento conjunto nombrará a una de las firmas como representante.

7. Calendario de Pagos

- 7.1. 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. El Banco desea recibir la propuesta de costos más competitiva para los servicios descritos en el presente documento.
- 7.2. 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	
<i>Entregables</i>	%
Entregable a)	20%
Entregable b)	20%
Entregable c)	20%
Entregable d)	40%
TOTAL	100%

TÉRMINOS DE REFERENCIA

Consultoría para el diseño del plan de acción para la implementación un Centro de Excelencia en Ciberseguridad

1. Antecedentes y Justificación

El COVID-19 ha acelerado la transformación digital de nuestras sociedades, y la ciberseguridad ha pasado a ocupar un lugar central entre las preocupaciones del mundo. Según un estudio realizado por Enterprise Insight en 2020⁴, el 78% de los líderes de TI considera que sus organizaciones no cuentan con las medidas apropiadas de ciberseguridad. A su vez, de acuerdo al Global Risk Report⁵ del Foro Económico Mundial la ciberseguridad se ubica entre los cinco riesgos más importantes que enfrentan las empresas.

La digitalización del sector público brasileño lograda recientemente trae un importante desafío: Desarrollar capacidades en Ciberseguridad. Si bien el gobierno federal cuenta con una estrategia nacional de ciberseguridad aprobada en 2020 y se posiciona sobre la media de madurez de la región, según el estudio de Madurez en Ciberseguridad⁶ realizado por el BID y la OEA en 2020, subsisten desafíos de coordinación, operacionales y de talento humano. Esta situación se replica también, pero de forma más severa, a nivel de los gobiernos estaduais, en un contexto de cada vez mayores ataques que vienen generando disrupciones en la entrega de servicios clave como salud o justicia. Brasil formaba parte del Top 10 Global Threat Rank y ocupaba la posición 70 de 175 países en el ranking del Índice Global de Ciberseguridad.

La Secretaria de Gobierno Digital (SGD) del Ministerio de Economía, en su rol de órgano central de administración de los recursos de tecnología del Gobierno Federal, ofrece la plataforma de servicios compartidos de la administración federal y define las mejores prácticas en el uso de TIC. Entre estas actividades, dicha secretaría se encuentra trabajando en el desarrollo de sus capacidades mediante la creación de un Centro de Respuesta a Incidentes de Ciberseguridad (CSIRT) y un Centro de Excelencia en Ciberseguridad.

2. Objetivos

El objetivo de esta consultoría es realizar un diagnóstico de la situación actual en desarrollo de conocimiento en ciberseguridad de la SGD; diseñar y dimensionar un roadmap de implementación de un Centro de Excelencia en Ciberseguridad según el análisis realizado. Esta consultoría debe estar sincronizada con su equivalente relativa al diseño y dimensionamiento del roadmap para el CSIRT.gob.br de la misma secretaría.

⁴ <https://finance.yahoo.com/news/78-lack-confidence-company-cybersecurity-153000182.html?guccounter=1>

⁵ http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

⁶ <https://www.iadb.org/ciberseguridad2020>

3. Actividades Clave

Las principales actividades que se estima el contractual deberá realizar son:

- (i) Elaborar un análisis de la situación actual de la SGD para identificar las principales necesidades en términos de desarrollo de conocimiento, capital humano y capacitación en materia de ciberseguridad.
- (ii) Elaborar un diseño de un Centro de Excelencia en Ciberseguridad, incluyendo: Objetivos, estructura organizacional, servicios, estructura de oferta educativa, infraestructura necesaria, la articulación con terceras partes, y presupuestos estimados basados en el análisis de la actividad (i).
- (iii) Desarrollo de un plan de acción para la implementación del Centro de Excelencia en Ciberseguridad diseñado, explicitando: las principales necesidades, la propuesta de diseño, cronograma de implementación y estimación presupuestal.

4. Resultados y Productos Esperados

La firma presentará 4 entregables:

- (a) Informe de relevamiento correspondiente a la actividad (i) al mes de ser contratada;
- (b) Diseño del Centro de Excelencia correspondiente a la actividad (ii) a los 4 meses de ser contratada;
- (c) Desarrollo de un plan de acción, correspondiente a la actividad 3 (iii) a los 18 meses de ser contratada.

5. Requisitos de los Informes

Los informes deben ser validados previamente a su aceptación por parte del Banco en coordinación con el cliente. Los mismos deben estar en idioma Portugués o Inglés.

6. Requisitos de la firma

Las firmas consultoras interesadas deberán proporcionar información que indique que están calificadas para suministrar los servicios (folletos, descripción de trabajos similares, experiencia en condiciones similares, disponibilidad de personal que tenga los conocimientos pertinentes, etc.). En particular deberán demostrar experiencia en consultorías de ciberseguridad, experiencia en protección de infraestructuras críticas y políticas públicas. Las firmas consultoras elegibles se pueden asociar como un emprendimiento conjunto o en un acuerdo de sub-consultoría para mejorar sus calificaciones. Dicha asociación o emprendimiento conjunto nombrará a una de las firmas como representante.

7. Calendario de Pagos

- 7.1. 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. El Banco desea recibir la propuesta de costos más competitiva para los servicios descritos en el presente documento.
- 7.2. 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	
<i>Entregables</i>	%
Entregable a)	20%
Entregable b)	40%
Entregable c)	40%
TOTAL	100%

TÉRMINOS DE REFERENCIA

Consultoría para el dictado de capacitación en ciberseguridad y nuevas tecnologías.

1. Antecedentes y Justificación

El COVID-19 ha acelerado la transformación digital de nuestras sociedades, y la ciberseguridad ha pasado a ocupar un lugar central entre las preocupaciones del mundo. Según un estudio realizado por Enterprise Insight en 2020⁷, el 78% de los líderes de TI considera que sus organizaciones no cuentan con las medidas apropiadas de ciberseguridad. A su vez, de acuerdo al Global Risk Report⁸ del Foro Económico Mundial la ciberseguridad se ubica entre los cinco riesgos más importantes que enfrentan las empresas.

La digitalización del sector público brasileño lograda recientemente trae un importante desafío: Desarrollar capacidades en Ciberseguridad. Si bien el gobierno federal cuenta con una estrategia nacional de ciberseguridad aprobada en 2020 y se posiciona sobre la media de madurez de la región, según el estudio de Madurez en Ciberseguridad⁹ realizado por el BID y la OEA en 2020, subsisten desafíos de coordinación, operacionales y de talento humano. Esta situación se replica también, pero de forma más severa, a nivel de los gobiernos estatales, en un contexto de cada vez mayores ataques que vienen generando interrupciones en la entrega de servicios clave como salud o justicia. Brasil formaba parte del Top 10 Global Threat Rank y ocupaba la posición 70 de 175 países en el ranking del Índice Global de Ciberseguridad.

La Secretaria de Gobierno Digital (SGD) del Ministerio de Economía, en su rol de órgano central de administración de los recursos de tecnología del Gobierno Federal, ofrece la plataforma de servicios compartidos de la administración federal y define las mejores prácticas en el uso de TIC. Entre estas actividades, dicha secretaría se encuentra trabajando en el desarrollo de sus capacidades mediante la creación de un Centro de Respuesta a Incidentes de Ciberseguridad (CSIRT) y un Centro de Excelencia en Ciberseguridad.

2. Objetivos

El objetivo de esta consultoría es el dictado de capacitación en ciberseguridad y nuevas tecnologías que permita desarrollar capacidades en el personal técnico y mandos medios de la SGD y órganos vinculados a sistemas críticos de Gobierno Digital. Estas capacitaciones deben incluir actividades prácticas, tanto técnicas como ejercicios de table-top cuando corresponda.

3. Actividades Clave

Las principales actividades que se estima el contractual deberá realizar son:

⁷ <https://finance.yahoo.com/news/78-lack-confidence-company-cybersecurity-153000182.html?guccounter=1>

⁸ http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

⁹ <https://www.iadb.org/ciberseguridad2020>

- (i) dictado de la capacitación en ciberseguridad para técnico para las certificaciones: CTIA, CSA, ECIH, CHFI;
- (ii) dictado de capacitación en ciberseguridad para mandos medios y gerentes;
- (iii) dictado de capacitación en Blockchain e Inteligencia Artificial para técnicos.
- (iv) disponibilización on-line cursos y webinars de sensibilización en ciberseguridad para usuarios.

4. Resultados y Productos Esperados

La firma presentará 4 entregables:

- (a) capacitación dictada, correspondiente a la actividad (i) a los 2 meses de ser contratada;
- (b) capacitación dictada, correspondiente a la actividad (ii) a los 3 meses de ser contratada;
- (c) capacitación dictada, correspondiente a la actividad 3 (iii) a los 12 meses de ser contratada;
- (d) cursos y webinars online disponibles, correspondientes a la actividad 4 (iv) a los 24 meses de ser contratada.

5. Requisitos de los Informes

Los informes deben ser validados previamente a su aceptación por parte del Banco en coordinación con el cliente. Los mismos deben estar en idioma Portugués o Inglés.

6. Requisitos de la firma

Las firmas consultoras interesadas deberán proporcionar información que indique que están calificadas para suministrar los servicios (folletos, descripción de trabajos similares, experiencia en condiciones similares, disponibilidad de personal que tenga los conocimientos pertinentes, etc.). En particular deberán demostrar experiencia en consultorías de ciberseguridad, experiencia en protección de infraestructuras críticas y políticas públicas. Las firmas consultoras elegibles se pueden asociar como un emprendimiento conjunto o en un acuerdo de sub-consultoría para mejorar sus calificaciones. Dicha asociación o emprendimiento conjunto nombrará a una de las firmas como representante.

7. Calendario de Pagos

- 7.1.** 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. El Banco desea recibir la propuesta de costos más competitiva para los servicios descritos en el presente documento.

7.2. 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	
<i>Entregables</i>	%
Entregable a)	25%
Entregable b)	25%
Entregable c)	25%
Entregable d)	25%
TOTAL	100%