INICIATIVA DE SEGURIDAD CIBERNÉTICA DE LA OEA

Foro Global sobre Experticia Cibernética (GFCE)

Organización de los Estados Americanos | Más derechos para más gente

GFCE Global Forum on Cyber Expertise

CONTENIDOS

INICIATIVA DE SEGURIDAD CIBERNÉTICA DE LA OEA

La Organización de Estados Americanos (OEA) ha estado trabajando para fortalecer las capacidades de seguridad cibernética entre los Estados Miembros de la OEA desde principios de la década de 2000. Con los años, se ha convertido en un líder regional en asistencia a los países para fortalecer la capacidad técnica y de seguridad cibernética, al nivel de políticas, para garantizar un ciberespacio seguro y resiliente. El programa de seguridad cibernética de la OEA apoya las iniciativas sobre la base de un análisis en profundidad y en la comprensión de la magnitud de las amenazas cibernéticas en un país dado, además de las capacidades nacionales existentes para hacerle frente a esas amenazas. Además, la OEA promueve la participación de los asociados y las partes interesadas de diferentes sectores, asegurando que el gobierno, el sector privado y la sociedad civil participen directamente en la formulación de políticas de seguridad cibernética.

MARCO DE SEGURIDAD CIBERNÉTICA REGIONAL DE LA OEA

En 2004, la OEA se convirtió en el primer organismo regional en adoptar una estrategia de Seguridad Cibernética a través de la aprobación unánime de "La Estrategia Integral de Seguridad Cibernética Interamericana", que le establece un mandato a la Secretaría General de la OEA en el sentido de ayudar a los Estados Miembros en la creación y el fortalecimiento de sus capacidades de seguridad cibernética. Reconociendo la naturaleza cambiante de las amenazas de seguridad cibernética, los Estados Miembros de la OEA renovaron su compromiso con la seguridad cibernética mediante la adopción, en 2012, de la declaración sobre "Fortalecimiento de la Seguridad Cibernética en las Américas" (2012) y, más recientemente, la "Declaración sobre la Protección de la Infraestructura Crítica ante las Amenazas Emergentes" (2015). Estos instrumentos son fundamentales para la promoción de políticas de seguridad cibernética políticamente cohesivas en las Américas.

LO QUE LES OFRECEMOS A NUESTROS ESTADOS MIEMBROS

La Iniciativa de Seguridad Cibernética de la OEA aborda temas de seguridad cibernética con base en un enfoque flexible y dinámico, en el que se ajustan las políticas de seguridad cibernética y la provisión de capacitación técnica de acuerdo a las nuevas tendencias y necesidades emergentes. Con los años, el Programa de Seguridad Cibernética de la OEA ha evolucionado para afrontar los desafíos mediante un enfoque multifacético y personalizado, con el establecimiento de un plan de acción que se puede adecuar para adaptarse mejor a las necesidades específicas de un país.

1. DESARROLLO DE LA ESTRATEGIA NACIONAL DE SEGURIDAD CIBERNÉTICA

El enfoque del Programa de Seguridad Cibernética de la OEA en este área consiste en facilitar la organización de mesas redondas nacionales con la participación de interesados clave en seguridad cibernética nacionales, incluyendo representantes del gobierno, el sector privado, la sociedad civil y la academia. Facilitadas por expertos de la OEA, las sesiones primero buscan familiarizar a los participantes con el propósito de las estrategias nacionales de seguridad cibernética y darles a conocer la función y componentes de una serie de estrategias que están en vigor en todo el mundo. Tras los debates de mesa redonda, la OEA recopila y organiza la información recopilada y le presenta un proyecto de estrategia integral al punto de contacto del Estado Miembro, quien luego lo distribuye a la comunidad de seguridad cibernética nacional en general. Enseguida comienza un proceso de retroalimentación y revisión facilitado por la OEA, que continúa hasta que se cumplen las necesidades de los Estados Miembros, el documento se considera definitivo y se les presenta a las autoridades competentes para su aprobación.

La OEA ha ayudado a Colombia (2011), Panamá (2012), Trinidad y Tobago (2013) y Jamaica (enero de 2015) en el desarrollo y adopción de marcos nacionales de política de seguridad cibernética. La OEA también se encuentra trabajando con Dominica, Surinam, Costa Rica y Perú, en el desarrollo de sus respectivas estrategias de seguridad cibernética nacional.

2. CAPACITACIONES Y TALLERES DE SEGURIDAD CIBERNÉTICA

Con base en las necesidades y solicitudes específicas de cada país, la OEA ofrece capacitaciones dirigidas a funcionarios con responsabilidades directas, ya sea un supervisor o un técnico, para asegurar o coordinar la seguridad cibernética nacional. Estas acciones formativas están centradas en un amplio público de actores de seguridad cibernética, incluidos agentes del orden, personal técnico y de respuesta a incidentes, partes interesadas del sector privado, responsables de políticas, entre otros.

En promedio, el Programa de Seguridad Cibernética de la OEA ofrece formación a más de 1.200 funcionarios por año. La formación técnica a los funcionarios ha demostrado ser un medio de gran éxito para la mejora de la seguridad cibernética a nivel nacional y regional, y para la creación de confianza y redes entre los participantes. El Programa de Seguridad Cibernética de la OEA ha ofrecido capacitación en sistemas industriales avanzados de control, diplomacia internacional en seguridad cibernética, protección de infraestructuras críticas, ISO 27001 Sistema de Gestión de la Seguridad de la Información, prácticas de investigación, análisis forense, respuesta a incidentes, desarrollo y gestión de CSIRT, y otros temas relacionados con la seguridad cibernética.

3. DESARROLLO CSIRT Y RED HEMISFÉRICA

El establecimiento y desarrollo de Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT nacionales) son la máxima prioridad de la OEA, que promueve y ofrece asistencia técnica a estos fines. El Programa de Seguridad Cibernética de la OEA también ha estado desarrollando una red hemisférica virtual de CSIRT, que busca facilitar la comunicación y el intercambio de información en tiempo real entre los CSIRT en las Américas, así como garantizar que cada país tenga un punto de contacto oficial designado para cuestiones de respuesta a incidentes cibernéticos.

La OEA promovió y apoyó la creación de varios CSIRT, cuyo número se elevó de 4 a 18 en la última década. La OEA se está uniendo a la Iniciativa de Madurez de CSIRT del GFCE. Además, el Programa de Seguridad Cibernética está desarrollando actualmente una Guía de Mejores Prácticas de CSIRT.

4. EJERCICIOS DE GESTIÓN DE CRISIS

Mediante la utilización de un laboratorio cibernético móvil de tecnología de punta, la OEA lleva a cabo ejercicios de gestión de crisis de seguridad cibernética diseñados a la medida de las necesidades de los Estados Miembros. Este laboratorio le permite a la OEA realizar ejercicios en cualquier lugar, independientemente de la calidad de la infraestructura o el nivel de conectividad, superando así las limitaciones potenciales que podrían obstaculizar la implantación exitosa de tal ejercicio.

El laboratorio cibernético móvil se ha utilizado en 8 ejercicios de gestión de crisis nacionales y 2 regionales desde 2012. Estos ejercicios reúnen a una gran variedad de partes interesadas nacionales y CSIRT internacionales para mejorar la coordinación y comunicación en el manejo de incidentes de seguridad cibernética.

5. SENSIBILIZACIÓN

Se está empleando un enfoque doble para las campañas de sensibilización de seguridad cibernética: por un lado, la provisión de productos tangibles (por ejemplo, conferencias, videos, carteles) y por el otro, la asistencia a países en el desarrollo de una campaña nacional de concienciación sobre la seguridad cibernética. La OEA también se ha asociado con una serie de organizaciones de la sociedad civil especializadas en llegar a los usuarios finales y en la creación de conciencia para ayudar a Estados Miembros en el desarrollo de sus campañas.

El Programa de Seguridad Cibernética de la OEA está desarrollando un conjunto de herramientas de sensibilización de seguridad cibernética (una especie de guía de cómo adelantarla) para ayudar a países en la formulación de sus propias campañas de concienciación en seguridad cibernética centradas en los usuarios finales de Internet. Nuestros socios incluyen el Anti-Phishing Working Group (APWG) y la Convención de mensajería STOP.THINK.CONNECT., entre otras organizaciones de la sociedad civil.

6. MISIONES DE ASISTENCIA TÉCNICA EN SEGURIDAD IBERNÉTICA

El Programa de Seguridad Cibernética de la OEA responde a las solicitudes de los países, en función de una atención por estado, mediante el desarrollo y la realización de misiones de asistencia técnica, a la medida, diseñadas para abordar las preocupaciones específicas de seguridad cibernética. Estos pueden tomar una variedad de formatos, dependiendo de las facetas de seguridad cibernética particular que quiera abordar un Estado Miembro. Algunas misiones de asistencia técnica toman la forma de grupos de trabajo con expertos en seguridad cibernética; otras son de asistencia basada en emergencia.

Solo en 2014, la OEA realizó misiones de asistencia técnica en más de 10 países. Por ejemplo, en 2014 el Gobierno de Colombia le solicitó a la OEA organizar una Comisión Internacional de Expertos para evaluar el estado actual del país en materia de seguridad cibernética. La evaluación incluyó visitas al sitio, revisiones de políticas, marcos legales e institucionales y terminó con la entrega de recomendaciones, por parte de los peritos, a ministros y otros altos funcionarios de alto nivel del gobierno colombiano. En otro caso, la OEA trasladó a un equipo de expertos en respuesta a incidentes a Jamaica para apoyar la gestión de incidentes de seguridad cibernética. Lo anterior incluyó la colaboración de la Red Hemisférica de CSIRT de la OEA.

7. ACCESO A EXPERTICIA EN SEGURIDAD CIBERNÉTICA

La asociación del Programa de Seguridad Cibernética de la OEA con una serie de expertos internacionales en seguridad cibernética les facilita el acceso a los Estados Miembros a la experticia acreditada y reconocida, a nivel internacional, en diferentes campos de la seguridad de la información. A través de estas asociaciones, los Estados Miembros de la OEA reciben asistencia sin costo alguno en la formulación, implementación y revisión técnica de sus políticas de seguridad cibernética, y tienen acceso a una amplia gama de mejores prácticas, experiencias y actividades de capacitación técnica sobre temas de seguridad cibernética.

La OEA ofrece acceso a expertos en seguridad cibernética a través de alianzas con empresas del sector privado (por ejemplo, Microsoft, Trend Micro y Symantec), la academia (por ejemplo, Universidad de Oxford), y organizaciones sin fines de lucro, como el Foro Económico Mundial (FEM), el Registro de Direcciones de Internet para América Latina y Caribe (LACNIC), y la Corporación para la Asignación de Nombres y Números en Internet (ICANN). Estas asociaciones han dado resultados fructíferos y tangibles, como la producción de informes oficiales y la organización de varias iniciativas conjuntas (por ejemplo, actividades de formación, talleres, mesas redondas).

8. SEGURIDAD CIBERNÉTICA Y GOBIERNO EN LÍNEA PARA UNA EFICAZ GESTIÓN PÚBLICA

Sobre la base de la cooperación horizontal, alianzas estratégicas y el uso eficiente de la Tecnología de la Información y la Comunicación (TIC) a nivel nacional y local, el programa de gobierno en línea de la OEA es el centro de intercambio de información de las Américas para la promoción de la gobernanza electrónica en el hemisferio a través de iniciativas como la Iniciativa Latinoamericana por los Datos Abiertos (ILDA), la Plataforma de Formación en Línea (Campus virtual de la OEA), MuNet (municipios transparentes y eficientes), la Red de Autoridades de Gobierno electrónico de América Latina y el Caribe (Red Gealc), la Red Interamericana de Compras Gubernamentales (RICG) y la iniciativa de Catastro. El Programa de Seguridad Cibernética de la OEA trabaja en estrecha colaboración con el Programa de Gobierno electrónico de la OEA en la promoción de iniciativas de seguridad cibernética en las Américas.

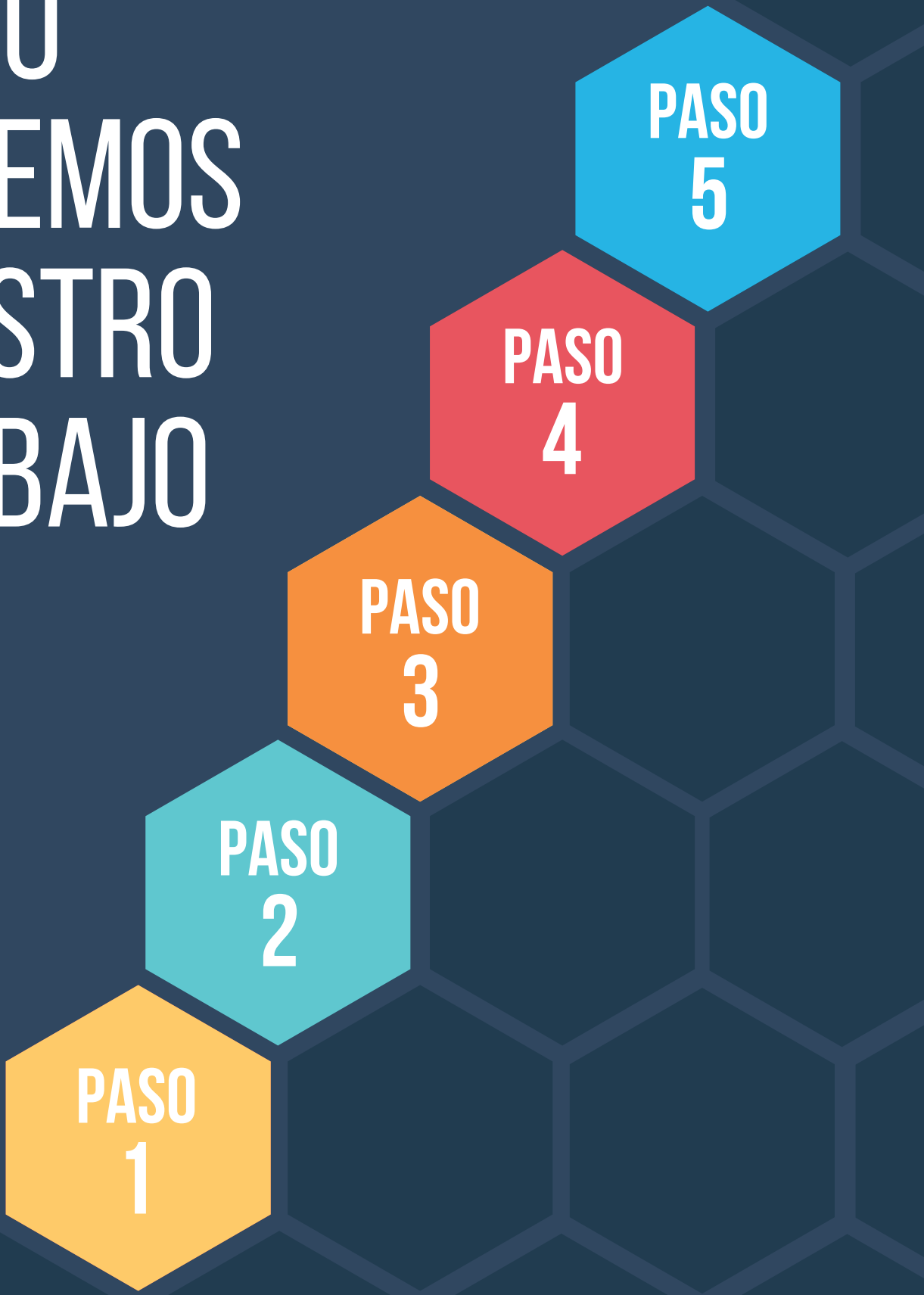
El Programa de Gobierno electrónico es el punto focal para el desarrollo de capacidades, el diálogo y la política de Gobierno electrónico, sirve como la Secretaría Técnica de la Red Gealc, cuenta con más de 20 cursos en línea diferentes disponibles; ha impartido formación a más de 14.000 funcionarios públicos, incluyendo la organización de 15 talleres de gobierno electrónico (dirigido a más de 550 alcaldes y representantes municipales). También ha apoyado la modernización del catastro en el Caribe, específicamente en Antigua y Barbuda y Saint Kitts y Nevis bajo un modelo de asociación con el sector privado.

9. IDENTIFICACIÓN Y ADOPCIÓN DE NORMAS TÉCNICAS PARA UNA ARQUITECTURA SEGURA DE INTERNET

Una estrategia eficaz de seguridad cibernética deberá reconocer que la seguridad de la red de sistemas de información que comprenden la Internet requiere una alianza entre el gobierno y la industria. Las capacidades de seguridad en productos informáticos son cruciales para la seguridad de la red en general, y deben desarrollarse de una manera que promueva la integración de capacidades de seguridad aceptables en la arquitectura general de la red.

Para lograr tales soluciones integradas de seguridad cibernética, con base tecnológica, la seguridad de la red debe estar diseñada en torno a las normas internacionales desarrolladas en un proceso abierto. El desarrollo de normas para la arquitectura de seguridad en Internet requerirá un proceso de múltiples pasos para asegurar que se logre el suficiente acuerdo, planificación y aceptación entre las diversas entidades gubernamentales y privadas que deberán cumplir un papel en la promulgación de dichas normas.

CÓMO HACEMOS NUESTRO TRABAJO



PASO UNO: SOLICITUD DEL ESTADO MIEMBRO

La Organización de Estados Americanos (OEA) ofrece asistencia técnica diseñada a la medida y entrega iniciativas de creación de capacitación en seguridad cibernética a petición de los Estados Miembros. La solicitud de asistencia se puede hacer a través del punto de contacto nacional del Estado Miembro, o por medio de un simple correo electrónico dirigido a la Secretaría General de la OEA (cybersecurity@oas.org).

Los Estados Miembros también están invitados a completar nuestro "Formulario de Solicitud de Asistencia Técnica" (Anexo A), que está orientado hacia la obtención de una información más específica acerca de la asistencia solicitada (necesidad o preocupación específica, institución solicitante, beneficiarios, plazo esperado y disponibilidad de recursos). Representa un punto de partida para la identificación conjunta, cuando sea posible, de los recursos y conocimientos suficientes para satisfacer las necesidades de seguridad cibernética actual y futura de las instituciones solicitantes.

PASO DOS: CONSIDERACIÓN DE LA SOLICITUD POR PARTE DE LA OEA

La Secretaría General de la OEA estudia detenidamente cada solicitud de asistencia técnica, teniendo en cuenta la información presentada por el Estado Miembro, así como la disponibilidad de personal, programa de trabajo actual, y recursos financieros y en especie para llevar a cabo la iniciativa propuesta.

Junto con los representantes del gobierno del país, la OEA evalúa las necesidades de seguridad cibernética y, con base en estos resultados, se elaboran planes de acción para fortalecer las capacidades de seguridad cibernética en el país.

Si la Secretaría General de la OEA no tiene los recursos financieros suficientes disponibles para suministrar el apoyo solicitado, puede diseñar, en consulta con el Estado Miembro solicitante, una propuesta de financiación que se presentará a varios donantes. La OEA también puede utilizar la plataforma que ofrece el Foro Mundial sobre la Experticia Cibernética (GFCE) para evaluar el interés de donantes potenciales en el apoyo a la iniciativa.

PASO TRES: DISEÑO

Con el fin de identificar y entender los desafíos específicos de un país, la OEA inicia el proceso de diseño mediante la realización de un análisis de la situación. Esto puede implicar visitas en el lugar con funcionarios gubernamentales y otros interesados en seguridad cibernética nacionales pertinentes, incluidos los representantes de la sociedad civil, la academia y el sector privado. El proceso de diseño puede también incluir la organización de mesas redondas y discusiones moderadas de grupos de trabajo, la realización de encuestas, y la recopilación de otra información necesaria para preparar un marco más detallado para la implementación de la iniciativa.

Gracias a las alianzas desarrolladas a lo largo de los años, la OEA trabaja en estrecha colaboración con una variedad de expertos e instituciones especializadas en diferentes áreas de la seguridad cibernética en la región y en todo el mundo, en el diseño e implementación de sus iniciativas de apoyo.

PASO CUATRO: IMPLEMENTACIÓN

Una vez que la OEA y los principales interesados de los países están de acuerdo con un diseño, puede comenzar la fase de implementación con la ejecución de las actividades del proyecto. A lo largo de la fase de ejecución, la OEA supervisa la entrega de la iniciativa a través de la recolección regular de información. Se pueden hacer ajustes a la iniciativa sobre la base de estos resultados, o a petición del gobierno del Estado Miembro.

El proceso de implementación por lo general se lleva a cabo con el apoyo del grupo de expertos de la OEA y actores técnicos y de políticas de una amplia gama de sectores dentro del Estado Miembro.

PASO CINCO: MISIÓN DE SEGUIMIENTO E INFORME GFCE

Cuando ha finalizado la fase de implementación, la OEA organiza misiones de seguimiento para asegurarse de que los países están adoptando un compromiso a largo plazo y de forma continua con los proyectos de seguridad cibernética en el país. Las misiones de seguimiento son esenciales para identificar el avance de los Estados Miembros en la creación de capacidad de seguridad cibernética, y para estudiar la posibilidad de dar un paso adelante hacia la consecución de objetivos más avanzados. También pueden llevarse a cabo evaluaciones externas, con la participación de todos los actores involucrados, a fin de valorar los resultados obtenidos por el proyecto/iniciativa.

En la reunión anual del GFCE, la Secretaría General de la OEA presentará un informe sobre los proyectos y actividades realizadas en las Américas. Este informe describirá los resultados obtenidos y los retos aún por resolver.

ANEXO
-A-

FORMULARIO DE SOLICITUD DE ASISTENCIA TÉCNICA

Este formulario debe ser diligenciado por los Estados Miembros de la OEA interesados en solicitarle a la Secretaría General asistencia en las iniciativas de creación de capacidad en diversas áreas de la seguridad cibernética.

ESTADO MIEMBRO Y INSTITUCIÓN SOLICITANTE

País: _____

Nombre de la institución que requiere apoyo: _____

Departamento/Área: _____

Persona de contacto dentro de la institución: _____

Correo electrónico: _____

Número telefónico: _____

DESCRIPCIÓN DE LA NECESIDAD

Describa en pocas palabras u oraciones la preocupación/necesidad de seguridad cibernética que afronta su país/institución.

APOYO SOLICITADO

Explique cómo puede ayudarle la Secretaría General de la OEA y/o sus socios a solucionar esta preocupación/necesidad. Usted puede hacerlo mediante la selección con una marca de verificación de uno o más de los siguientes servicios y/o mediante la descripción del tipo de apoyo solicitado en el cuadro de texto que le sigue. Si hay más de un área de interés para su país/institución, indique el orden de prioridad, siendo 1 el más importante.

Misión de Asistencia Técnica:

- ☐ Evaluación general de las necesidades
- ☐ Suministro de experticia en un área determinada (indique los detalles a continuación)
- ☐ Desarrollo o modernización de CSIRT
- ☐ Desarrollo de la Estrategia de Seguridad Cibernética Nacional
- ☐ Seguridad Cibernética y Gobierno Electrónico
- ☐ Ejercicio de Gestión de Crisis
- ☐ Campaña de sensibilización pública
- ☐ Capacitaciones (indique los detalles a continuación)
- ☐ Otros (s)

Los posibles temas incluyen, pero no se limitan a: la protección de la infraestructura crítica, gestión de seguridad de la información, prácticas de investigación, análisis forense, respuesta a incidentes, gestión de CSIRT, etc.

Sírvanse proporcionar información detallada sobre el apoyo solicitado:

BENEFICIARIOS

¿Quién espera usted que se beneficiará directamente del apoyo propuesto?

ASOCIADOS NACIONALES

¿Qué otras instituciones han participado o necesitan participar (por ejemplo, otras entidades gubernamentales, el sector privado o partes interesadas de la sociedad civil)?

CRONOGRAMA

¿Cuándo le gustaría recibir el apoyo propuesto? (por ejemplo, el cuarto trimestre de 20XX)

RECURSOS

¿Hay recursos financieros y/o en especie actualmente disponibles dentro de su institución para cumplir con la mencionada necesidad? ¿Ha contactado a algunas agencias donantes?

INFORMACIÓN DE CONTACTO GFCE

PROGRAMA DE SEGURIDAD CIBERNÉTICA DE LA OEA

Tel. +1 202.370.4674
Correo electrónico: cybersecurity@oas.org
Sitio web: www.oas.org/cyber

Organización de los Estados Americanos | Más derechos para más gente

PROGRAMA DE SEGURIDAD CIBERNÉTICA DE LA OEA

Comisión Interamericana contra el Terrorismo
Secretaría de Seguridad Multidimensional

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS

1889 F Street N.W.
Washington, D.C. 20006
P. 202 370 4674
F. 202 458 3857
cybersecurity@oas.org

WWW.OAS.ORG/CYBER