CONTRATACIÓN DEL SERVICIO DE CAPACITACION DENOMINADO CURSO "SEGURIDAD DE LA INFORMACIÓN, GESTIÓN DE INCIDENTES Y CIBERSEGURIDAD" PARA LOS SERVIDORES DEL OSCE

1. ÁREA USUARIA

Unidad de Recursos Humanos de la Oficina de Administración del Organismo Supervisor de las Contrataciones del Estado-OSCE.

2. DENOMINACIÓN DE LA CONTRATACIÓN

CONTRATACIÓN DEL SERVICIO DE CAPACITACION DENOMINADO CURSO "SEGURIDAD DE LA INFORMACIÓN, GESTIÓN DE INCIDENTES Y CIBERSEGURIDAD" PARA LOS SERVIDORES DEL OSCE.

3. FINALIDAD PÚBLICA

Capacitar de manera transversal a los servidores del OSCE a fin de que puedan adquirir conocimientos y habilidades necesarios para abordar los desafíos de la seguridad de la información, la gestión de incidentes y la ciberseguridad en un entorno digital logrando prevenir, detectar, y responder ante incidentes de seguridad informática, asegurando la protección de datos y sistemas críticos.

4. OBJETIVO DE LA CONTRATACIÓN

El curso tiene por objetivo que, los servidores civiles del OSCE participantes, al término del mismo, logren adquirir conocimientos teóricos y prácticos esenciales en el ámbito de la seguridad de la información, la gestión de incidentes y la ciberseguridad, para que puedan identificar, prevenir y responder a amenazas y vulnerabilidades en los sistemas informáticos de sus organizaciones.

5. ACTIVIDAD DEL POI

C0015 - EJECUCIÓN DEL PLAN DE DESARROLLO DE PERSONAS (PDP)

6. ALCANCES Y DESCRIPCIÓN DE SERVICIO

ITEM	CANTIDAD	UNIDAD DE MEDIDA	DESCRIPCIÓN
1	1	Servicio	CONTRATACIÓN DEL SERVICIO DE CAPACITACION DENOMINADO "SEGURIDAD DE LA INFORMACIÓN, GESTIÓN DE INCIDENTES Y CIBERSEGURIDAD" PARA LOS SERVIDORES DEL OSCE.

6.1Actividades a desarrollar por el proveedor:

a) Desarrollar seis (06) sesiones de capacitación de dos (02) horas cronológicas y treinta (30) minutos por sesión y una (01) sesión de una (01) hora cronológica.

b) Brindar asistencia técnica sobre el uso de la plataforma virtual de capacitación.

c) Entregar los materiales necesarios para el desarrollo de las sesiones.

d) Elaborar el registro de asistencia de los servidores de la entidad que participan en el curso y notas obtenidas.

e) Realizar el envío del reporte de asistencia al día siguiente de realizada cada sesión del curso.

f) Controlar la asistencia de todos los participantes en cada sesión.

g) Tomar la evaluación final en la última sesión de clases.

h) Deberá emitir la constancia y/o certificado de los participantes que obtengan nota aprobatoria cumpliendo con los siguientes requisitos:

• Que hayan asistido por lo menos a cinco (05) de las siete (07) sesiones de la capacitación (la inasistencia deberá ser justificada a la institución educativa).

• Que hayan obtenido la calificación mínima de doce (12) sobre veinte (20) en la evaluación final del curso.

6.2Temario:

CURSO "SEGURIDAD DE LA INFORMACIÓN, GESTIÓN DE INCIDENTES Y CIBERSEGURIDAD"		
Sesión 01	**Módulo 1: Introducción a la Seguridad de la Información y Ciberseguridad** - Definición y objetivos de la seguridad de la información. - Principios básicos: Confidencialidad, Integridad y Disponibilidad (CIA). - Tipos de amenazas y vulnerabilidades. - Conceptos básicos de ciberseguridad: ataques, actores maliciosos y motivaciones. - La evolución de la ciberseguridad en el contexto actual.	2 horas 30 minutos
Sesión 02	**Módulo 2: Normativas y Estándares de Seguridad** - ISO 27001: Sistema de gestión de seguridad de la información. - NIST y su aplicación en la ciberseguridad. - GDPR y normativas de protección de datos. - Requisitos de cumplimiento en la seguridad de la información. - Implementación de controles de seguridad según normativas internacionales.	2 horas 30 minutos
Sesión 03	**Módulo 3: Gestión de Incidentes de Seguridad Informática** - Definición de incidentes de seguridad y su clasificación. - Ciclo de vida de un incidente de seguridad. - Identificación y clasificación de incidentes de seguridad. - Herramientas y técnicas para la detección de incidentes.	2 horas 30 minutos
Sesión 04	**Módulo 3: Gestión de Incidentes de Seguridad Informática** - Respuesta ante incidentes: protocolos y estrategias de mitigación. - Ejercicios prácticos de gestión de incidentes (simulación). - Recuperación y análisis post-incidente.	2 horas 30 minutos
Sesión 05	**Módulo 4: Técnicas y Herramientas de Ciberseguridad** - Firewalls, IDS/IPS (Sistemas de detección y prevención de intrusos). - Cifrado de datos y autenticación. - Análisis de vulnerabilidades y herramientas de escaneo de redes. - Antivirus, antimalware y técnicas de defensa contra software malicioso.	2 horas 30 minutos

	- Simulaciones de ciberataques: análisis y respuesta ante amenazas (ejercicios prácticos).	
Sesión 06	**Módulo 5: Tendencias Emergentes y Futuro de la Ciberseguridad** - Desafíos emergentes en ciberseguridad: IoT, IA, computación en la nube. - Ciberseguridad en entornos de trabajo híbridos y remotos. - Técnicas de ciberdefensa avanzadas.	2 horas 30 minutos
Sesión 07	**Módulo 5: Tendencias Emergentes y Futuro de la Ciberseguridad** - La ciberseguridad en la era de la inteligencia artificial y el machine learning. - Estrategias de defensa proactivas y predictivas. **Evaluación del curso**	1 hora

6.3 Cantidad de Servidores a Capacitar:

La cantidad se servidores de capacitar son cien (100) servidores del OSCE.

6.4Horario:

- Las siete (07) sesiones se desarrollarán los lunes, miércoles y jueves de 7:00 pm a 9:30 pm, y la fecha de inicio será pactada luego de las coordinaciones previas entre la Gestora de capacitación de la entidad y el proveedor.
- Horas cronológicas: 16 horas cronológicas
- Horas lectivas certificadas: 21 horas
- Número de Sesiones: 7 sesiones

6.5Manejo de fondos públicos

- Dentro de las actividades a realizar por el prestador del servicio, NO están inmersas el manejo de fondos públicos; por lo que NO deberá presentar su DDJJ de Bienes, Ingresos y Rentas.

6.6Declaración Jurada de Intereses

- De acuerdo a lo señalado en el objeto de contratación y actividades descritas, el prestador del servicio NO se constituye como sujeto obligado para presentar la Declaración Jurada de Intereses, de acuerdo a lo señalado en el artículo 3 de la Ley N° 31227.

6.7Consultoría

- De acuerdo a lo señalado en el objeto de contratación y actividades descritas, el servicio a contratar NO corresponde a un contrato de consultoría y por lo tanto NO procede su inclusión en el Sistema de Registro para el Control de Contratos de Consultoría del Estado-SIRICC.

7. REQUISITOS DEL PROVEEDOR Y/O PERSONAL PROPUESTO

Persona jurídica con por lo menos tres (03) años de experiencia en dictado de cursos.

7.1 Experiencia del Proveedor

El proveedor acreditara que haya desarrollado al menos dos (02) capacitaciones (curso, taller, seminario, congreso y/o especialización) y/o asistencia técnica en temas de Seguridad de la Información, gestión de incidentes y/o ciberseguridad.

7.2 Experiencia del Personal Clave

- Experiencia general mínima de seis (6) años en entidades públicas y/o privadas.
- Experiencia específica en temas afines al curso mínima de cinco (5) años en el Sector Público y/o Privado.
- Experiencia en docencia de 4 años mínimo, haber dictado como mínimo 4 cursos relacionados al tema del curso solicitado, en los últimos 4 años en universidades, institutos, entidades del estado y/o centros de formación.

7.3 Formación Académica

Profesional titulado en Ingeniería de Sistemas, Ingeniería informática, Ingeniería Industrial y/o afines con especialidad o posgrado en Seguridad de la Información o temas relacionados.

7.4 Capacitación

En ISO 27001 Implementador Líder o Auditor Líder, Certified Network Security Administrator, Certified Security Specialist, Ciberseguridad y/o Seguridad de la información (mínimo 180 horas lectivas acumuladas).

7.5 Otros

- No estar impedido de contratar con el Estado.
- Contar con Registro Nacional de Proveedores (RNP) vigente.
- Contar con RUC activo y habido.
- El proveedor deberá contar con una plataforma virtual con la capacidad necesaria para el desarrollo del curso.

8. LUGAR Y PLAZO DE PRESTACIÓN DEL SERVICIO

8.1 **Lugar:** La prestación del servicio se llevará a cabo de manera virtual a través de la plataforma que disponga el proveedor del servicio.

8.2 **Plazo:** Hasta treinta (30) días calendario, contados a partir del día siguiente de la notificación de la orden del servicio.

9. ENTREGABLES

El proveedor deberá entregar un Informe final de la actividad desarrollada (que incluya constancias, asistencia y nota obtenida por cada participante) dirigido a la Unidad de Recursos Humanos, como máximo hasta doce (12) días calendario posteriores a la última sesión del curso.

El proveedor deberá emitir las constancias y/o certificados de los participantes que obtengan nota aprobatoria cumpliendo con los requisitos señalados en el numeral 6.1. del presente documento.

El proveedor deberá entregar las constancias y/o certificados virtuales, con firma digital registrada, o físicos con firma manual (la entrega física se realizará en la Sede Central del OSCE previa coordinación).

10. LUGAR DE PRESENTACION DE LOS ENTREGABLES

El entregable debe ser presentado, a través de la Mesa de partes presencial o mesa de partes Digital del OSCE, disponible en https://apps.osce.gob.pe/mesa-partes-digital/, dirigido a la Unidad de Recursos Humanos. El horario para la recepción virtual de documentos será de lunes a viernes hasta las 23:59 horas

11. CONFORMIDAD DE SERVICIO

La conformidad del servicio estará a cargo de la Unidad de Recursos.

Dicha conformidad se otorgará en un plazo que no exceda de los siete (07) días calendario, contados desde el día siguiente de recibido el entregable.

12. FORMA DE PAGO

Pago Único al 100%, previa conformidad y presentación del comprobante de pago.

El pago se realizará con abono en la cuenta "Código de Cuenta Interbancaria" (CCI) del contratista, como máximo, hasta los diez (10) días calendario posteriores a la emisión de la conformidad del servicio respectiva y presentación del comprobante de pago.

13. PENALIDADES APLICABLES:

13.1 Penalidad por mora:
Se aplicará al contratista la penalidad establecida en el artículo 162 del Reglamento de la Ley de Contrataciones del Estado.

13.2 Otras Penalidades: No aplica

14. CONFIDENCIALIDAD Y PROPIEDAD INTELECTUAL

La información y material producido bajo los términos de este servicio, tales como escritos, medios magnéticos, digitales, y demás documentación generados por el servicio, pasará a propiedad del OSCE. El/La proveedor deberá mantener la confidencialidad y reserva absoluta en el manejo de la información y documentación a la que se tenga acceso relacionada a la prestación.

15. RESPONSABILIDAD POR VICIOS OCULTOS

El contratista es el responsable por la calidad ofrecida y por los vicios ocultos del servicio ofertado por un plazo no menor de un año, contado a partir de la conformidad otorgada por la Entidad.

16. CLAUSULA DE CUMPLIMIENTO (LEY DE PREVENCION Y MITIGACION DEL CONFLICTO DE INTERESES EN EL ACCESO Y SALIDA DE PERSONAL DEL SERVICIO PUBLICO, LEY N° 31564).

Son causales de resolución de contrato la presentación con información inexacta o falsa de la Declaración Jurada de Prohibiciones e Incompatibilidades a que se hace referencia

en la Ley de prevención y mitigación del conflicto de intereses en el acceso y salida de personal del servicio público. Asimismo, en caso se incumpla con los impedimentos señalados en el artículo 5 de dicha ley se aplicará la inhabilitación por cinco años para contratar o prestar servicios al Estado, bajo cualquier modalidad.

17. COMPROMISO ANTISOBORNO:

- El contratista declara conocer los compromisos antisoborno del OSCE, el cual se estable en su Política del Sistema Integrado de Gestión y se encuentra disponible en el portal web del OSCE:

  https://www.gob.pe/institucion/osce/campa%C3%B1as/1861-politica-del-sistemaintegrado-de-gestion-del-osce

- El contratista declara no haber, directa o indirectamente, ofrecido, negociado o efectuado pago o, en general, entregado beneficio o incentivo ilegal en relaciónal servicio a prestarse bien a proporcionarse. En línea con ello, se compromete a actual en todo momento con integridad, a abstenerse de ofrecer, dar o prometer, regalo u objeto alguno a cambio de cualquier beneficio, percibido de manera directa o indirecta; a cualquier miembro del Consejo Directivo, funcionarios públicos, empleados de confianza, servidores públicos; así como a terceros que tengan participación directa o indirecta en la determinación de las características técnicas y/o valor referencial o valor estimado, elaboración de documentos del procedimiento de selección, calificación y evaluación de oferta, y la conformidad de los contratos derivados de dicho procedimiento.

- El contratista se compromete a denunciar, en base de una creencia razonable ode buena fe cualquier intento de soborno, supuesto o real, que tuviera conocimiento a través del canal de denuncias de soborno ubicado en el portal web del OSCE.

18. ACUERDO DE CONFIDENCIALIDAD:

El contratista se comprometo a guardar reserva de la información privilegiada que conociera en el ejercicio de sus funciones, tareas y demás actividades como parte de la ejecución de la prestación, no revelando en forma oral, escrita, ni por cualquierotro medio, hechos, datos, procedimientos, documentación e información de acceso restringido (confidencial), a la que tuviera acceso a partir del inicio de las prestaciones relacionadas con el referido servicio, manteniendo la confidencialidad de la misma de manera permanente.

De igual manera se compromete a cumplir con: la Política Integrada de la Gestión de la Calidad ISO 9001, Gestión de Seguridad de la Información ISO 27001 y Gestión Antisoborno ISO 37001 del OSCE, las Políticas de Seguridad de la Información del OSCE, y demás normas y Leyes correspondientes a seguridad de la información, vigentes.

En caso que incumpliera con cualquiera de las obligaciones estipuladas en el presente acuerdo, el OSCE está autorizado a iniciar todas las acciones judiciales oextrajudiciales necesarias para resarcir del perjuicio, y la obligación de confidencialidad perdurará mientas la información conserve las características paraconsiderarse Confidencial.

19. MATERIAL DE ORIENTACIÓN PARA DENUNCIAR ACTOS DE CORRUPCIÓNEN LOS PROCESOS DE CONTRATACION (ANEXO N°4 DE LA DIRECTIVA N°004-2022-OSCE/SGE)

En el Organismo Supervisor de las Contrataciones del Estado promovemos la éticae integridad de la función pública, por lo que, si conoces de algún acto de corrupciónejercido por un/a servidor/a del OSCE, comunícanos tu denuncia ingresando de manera virtual a la Plataforma Digital Única de Denuncias del Ciudadano (https://denuncias.servicios.gob.pe/).2

Ejemplos:

1. Adecuación o manipulación de las especificaciones técnicas, expedientetécnico o términos de referencia para favorecer a un proveedor específico.
2. Generación de falsas necesidades con la finalidad de contratar obras, bienes o servicios.
3. Otorgamiento de la buena pro obviando deliberadamente el procedimiento requerido conforme a ley.
4. Permisividad indebida frente a la presentación de documentación incompleta de parte del ganador de la buena pro.
5. Otorgamiento de la buena pro a postores de quienes se sabe han presentado documentación falsa o no vigente.
6. Otorgamiento de la buena pro de (o ejercicio de influencia para el mismo fin) a empresas ligadas a exfuncionarios, de quienes se sabe están incursosen algunos de los impedimentos para contratar con el Estado que prevé la ley.
7. Admisibilidad de postor (o ejercicio de influencia para el mismo fin) ligado auna misma empresa, grupo empresarial, familia o allegado/a, de quien estáincurso en alguno de los impedimentos para contratar con el Estado que prevé la ley.
8. Pago indebido por obras, bienes o servicios no entregados o no prestados en su totalidad.
9. Sobrevaloración deliberada de obras, bienes o servicios y su consecuente pago en exceso a los proveedores que las entregan o brindan.
10. Negligencia en el manejo y/o mantenimiento de equipos y/o tecnología queimpliquen la afectación de los servicios que brinda la institución.

¿Conoces de alguno de estos actos de corrupción, o de otros que puedenhaberse cometido?, COMUNÍCANOS.

Notas:

(1) La denuncia puede ser anónima.
(2) Si el denunciante decide identificarse, se garantiza la reserva de suidentidad y/o de los testigos que quieran corroborar la denuncia, y puede otorgar una garantía institucional de no perjudicar su posición en la relacióncontractual establecida con la Entidad o su posición como postor en el proceso de contratación en el que participa o en los que participe en el futuro.
(3) Es importante documentar la denuncia, pero si no es posible, se recomienda

proporcionar información valiosa acerca de donde obtenerla oprestar colaboración con la entidad para dicho fin.

(4) La interposición de una denuncia no constituye impedimento para gestionar por otras vías que la ley prevé para cuestionar decisiones de la administración o sus agentes (OSCE, Contraloría General de la República,Ministerio Público, etc.).
(5) La interposición de una denuncia no servirá en ningún caso para paralizarun proceso de contratación del Estado.

20. SOLUCIÓN DE CONTROVERSIA

Todos los conflictos que se deriven de la ejecución e interpretación de la presente contratación, son resueltos mediante trato directo, conciliación y/o acción judicial.

21. ANEXOS: No aplica

Firmado digitalmente por SILVA PLASENCIA Joseph Edgard FAU 20419026809 soft
Motivo: Soy el autor del documento
Fecha: 11.02.2025 11:31:59 -05:00

_____

Firma y Sello
Responsable del
Área Usuaria

Firmado digitalmente por ALCALA NEGRON Christian Nelson FAU 20419026809 soft
Motivo: Soy el autor del documento
Fecha: 11.02.2025 11:28:31 -05:00