

	INSTITUTO NACIONAL DE CANCEROLOGÍA ESE	CÓDIGO:	GDG-P05-F-04
	GESTIÓN DEL GASTO	VERSIÓN:	1
	ANEXO TÉCNICO	VIGENCIA:	09-01-2020
		Página 1 de 8	

OBJETO

EL INSTITUTO NACIONAL DE CANCEROLOGÍA EMPRESA SOCIAL DEL ESTADO – INVITA A PRESENTAR PROPUESTAS PARA SERVICIO DE HACKING ETICO SOBRE PLATAFORMA TECNOLÓGICA SAP, ACORDE A ESTA INVITACIÓN, SUS ANEXOS Y EL CONTRATO QUE SE CELEBRE PARA TAL EFECTO.

1. CARACTERÍSTICAS O ESPECIFICACIONES TÉCNICAS

Desarrollar pruebas que permitan la identificación de vulnerabilidades, así como pruebas de Hacking Ético (pruebas de penetración) -Externo e Interno-, sobre hardware y software, servidores, bases de datos y redes correspondientes al sistema de información SAP del Instituto Nacional de Cancerología, para establecer el estado de la seguridad de la información que se almacena y procesa a través de la plataforma tecnológica SAP de la entidad, mediante el uso y aplicación de herramientas y pruebas que permitan la revisión de vulnerabilidades para identificar oportunamente posibles fuentes de incidentes de seguridad.

Para cumplir con el anterior objetivo, el INSTITUTO NACIONAL DE CANCEROLOGIA determina que el ámbito de Pruebas de intrusión sea de tipo Caja Gris con conocimiento parcial de la infraestructura tecnológica.

Al finalizar las pruebas de caja gris se debe desarrollar pruebas de ingeniería social sobre una muestra representativa de funcionarios (no menor de 10 personas) los cuales pertenecen a dependencias de uso intensivo de módulos críticos de aplicativo SAP del Instituto. Esto para establecer el nivel de la formación y capacidad de funcionarios para reconocer y reaccionar frente a un ataque de Ingeniería Social, y validar si los funcionarios reconocen y desconfían de fuentes de datos desconocidas o sospechosas.

También se desarrollará una auditoria de roles y perfiles tipo caja blanca, para validar el correcto manejo y aplicación de permisos de acceso a la información y a la administración de la plataforma SAP

Posterior al análisis inicial se realizará un análisis posterior (Retest) en cual no debe superar los 3 meses, en donde se identificará la efectividad de las remediaciones aplicadas sobre una muestra del 50 % del total de direcciones IP seleccionadas. No se realizará Retest para las pruebas de ingeniería social.

Como resultado del trabajo realizado, se debe entregar un informe en los que se incluirán los hallazgos realizados, las conclusiones obtenidas, las recomendaciones de seguridad que sean aplicables, y el detalle técnico; y se debe ejecutar la respectiva socialización y transferencia de conocimiento para el Oficial de seguridad de la información

Las características o especificaciones técnicas detalladas que constituyen el alcance del objeto se incluyen en el formato ANEXO TÉCNICO que forma parte del presente documento.

1.1. DESCRIPCIÓN DE LAS CARACTERÍSTICAS TÉCNICAS DEL OBJETO A CONTRATAR

- **Ethical Hacking y Análisis de vulnerabilidades:** para el servicio que prestara el proveedor en la realización de las pruebas de Análisis de vulnerabilidades y explotación (Ethical Hacking) tipo Caja Gris, se considerara un alcance de 25 activos (direcciones IP) sobre los servicios de la plataforma tecnológica SAP, en donde se realizará el análisis de vulnerabilidades de cada una de ellos y la explotación de las vulnerabilidades críticas sobre estas 25 direcciones IP. Posterior al análisis inicial se realizará un análisis

	INSTITUTO NACIONAL DE CANCEROLOGÍA ESE	CÓDIGO:	GDG-P05-F-04
	GESTIÓN DEL GASTO	VERSIÓN:	1
	ANEXO TÉCNICO	VIGENCIA:	09-01-2020
		Página 2 de 8	

posterior (Retest) en cual no debe superar los 3 meses, en donde se identificará la efectividad de las remediaciones aplicadas sobre una muestra del 50 % del total de direcciones IP seleccionadas.

- **Entorno de Operación:** el entorno de operación define como se va a interactuar con los activos:
 - Análisis de infraestructura de red interna y externa: entorno de redes de datos, con interacciones a través del protocolo TCP/IP, y a través de las redes de datos que proporcionen tanto el **INC** (en su entorno local) como los proveedores de Internet. No habrá contacto físico con el sistema a analizar.
- **Tipo de Análisis:**
 - Análisis de infraestructura de red interna y externa: el análisis a efectuar será de tipo Prueba de intrusión, de caja Gris, incluyendo pruebas automáticas y validaciones manuales.
 - ingeniería Social: Se contempla pruebas de acceso físico y lógico sobre 10 usuarios que seleccionara el supervisor de contrato de INC como muestra representativa
 - Auditoría de roles y Perfiles del aplicativo SAP en modo caja blanca.
- **Reglas de Compromiso:** El oferente se debe acoger a las reglas de compromiso enumeradas dentro de la metodología OWASP, entre las cuales se destaca la que atañe a la realización Pruebas de seguridad Pasiva, es decir, sin comprometer ni la integridad ni la disponibilidad de los activos que componen el objetivo. En caso de que exista la necesidad de realización de pruebas especialmente peligrosas que puedan causar la parada de servicios, se debe contar con el permiso expreso del INC para realizarlas y se deberán realizar de forma controlada y siempre bajo la supervisión de personal del Instituto.
- **Plan de Pruebas:** El oferente debe elaborar y presentar al INSTITUTO NACIONAL DE CANCEROLOGIA un plan de pruebas y actividades a realizar, así como de las herramientas a utilizar, las cuales deben ser aprobadas por el Instituto. Este plan debe ser presentado en el término de (15) quince días hábiles, una vez iniciado el contrato.

El plan de pruebas deberá establecer y presentar al INSTITUTO NACIONAL DE CANCEROLOGIA para su aprobación, los tipos de prueba de vulnerabilidad a ejecutar y la metodología detallada para su ejecución, especificando, entre otros aspectos, los criterios según los cuales se considerará que una vulnerabilidad hallada se clasifica como "crítica" o "No crítica". El oferente deberá incluir por lo menos los siguientes tipos de pruebas:

- ✓ Debilidades de Autenticación.

	INSTITUTO NACIONAL DE CANCEROLOGÍA ESE	CÓDIGO:	GDG-P05-F-04
	GESTIÓN DEL GASTO	VERSIÓN:	1
	ANEXO TÉCNICO	VIGENCIA:	09-01-2020
		Página 3 de 8	

- ✓ Uso de usuarios estándar
- ✓ Encriptación de comunicaciones entre componentes
- ✓ Parámetros incorrectos de SAP
- ✓ Carga inusual de transacciones y canales
- ✓ Bugs propios de SAP
- ✓ Ataques comunes a la aplicación SAP.
- ✓ Revisión de Log de Errores de plataforma SAP
- ✓ Identificación del sistema operativo.
- ✓ Identificación de instalaciones por defecto de servicios y aplicativo.
- ✓ Identificación de puertos abiertos TCP y UDP.
- ✓ Identificación de los servicios en ejecución.
- ✓ Rompimiento de claves.
- ✓ Identificación de vulnerabilidades del SO.
- ✓ Negación de servicios.
- ✓ Búsqueda de información sensible sobre la plataforma
- ✓ Identificación de vulnerabilidades asociadas a malas prácticas de programación.
- ✓ Explotación de vulnerabilidades.
- ✓ Buffer Overflow
- ✓ Negación de servicios.
- ✓ Abuso de formas.
- ✓ Directory transversal.
- ✓ Inapropiada validación de metacaracteres.
- ✓ Sesión hijacking.
- ✓ Mensajes y códigos de error incontrolados.
- ✓ SQL Injection.(desde el cliente SAP)
- ✓ Claves por defecto y claves fáciles.
- ✓ Intentos de autenticación a la base de datos.
- ✓ Extracción de información confidencial.

El oferente deberá incluir por lo menos los siguientes tipos de pruebas de ingeniería social:

- ✓ Pretexting: Llamar por teléfono a usuarios que tengan acceso a información sensible y pedirle cierta información, simulando ser alguien que precisa su ayuda.
- ✓ Tailgating: Tratar de obtener acceso no autorizado a áreas restringidas. El tailgating supone lograr acceso a una instalación física mediante engaño a su personal, o simplemente colándose dentro.
- ✓ Baiting: Tratar de infectar un equipo o varios en la red por medio de una USB infectada, mediante la instalación de un pequeño programa, sin riesgo, dentro de la red del cliente y después ejecutarlo de forma remota.
- ✓ Phishing: Tratar de suplantar el sitio de producción de SAP o sitio similar con el objetivo de hacerse con usuarios y contraseñas.

Nota: dentro de su propuesta, el contratista deberá especificar otros tipos de pruebas que esté dispuesto a realizar.

Para cada tipo de prueba del plan de pruebas se debe especificar:

1. Alcance o cobertura.
2. Objetivo(s).

	INSTITUTO NACIONAL DE CANCEROLOGÍA ESE	CÓDIGO:	GDG-P05-F-04
	GESTIÓN DEL GASTO	VERSIÓN:	1
	ANEXO TÉCNICO	VIGENCIA:	09-01-2020
		Página 4 de 8	

3. Participantes, y roles de estos.
4. Fecha(s) y hora(s) programadas para la ejecución de la actividad.
5. Paso a paso de la actividad.
6. Indicador propuesto para medir el resultado.
7. Resultado esperado de la actividad

- **Herramientas de Prueba:** Para la realización de esta prueba, se deben usar las herramientas pertinentes y usadas para el desarrollo de las pruebas de penetración, homologadas por el CVE (Common Vulnerabilities and Exposures), y/o www.mitre.org y deben estar actualizadas a la fecha de su utilización. Para lo anterior, se deberá adjuntar en los informes presentados certificado de homologación de CVE, o ruta de la página de CVE donde se pueda evidenciar que la herramienta ofrecida está homologada por dicha entidad. Dichas herramientas deben ser licenciadas o de propiedad del oferente y pueden ser complementadas con herramientas de uso libre o gratuito.

- **Informes:** Para la generación de los informes solicitados se deberá tomar como referencia la lista de nombres de vulnerabilidades CVE publicada por la corporación Mitre (www.mitre.org).

El oferente deberá levantar la información necesaria para realizar la verificación del Sistema SAP del INSTITUTO NACIONAL DE CANCEROLOGIA, y conceptuar sobre el mismo a nivel de los controles implementados que permiten mantener la seguridad de esta plataforma. Para ello, tendrá acceso a las configuraciones de los dispositivos de aseguramiento de redes implementados en INSTITUTO NACIONAL DE CANCEROLOGIA que el supervisor de contrato le facilite.

Como producto de la prestación del servicio, el contratista debe generar y entregar (3) informes relacionados con el análisis de vulnerabilidades, en idioma español que contengan como mínimo:

1. **Informe técnico** que incluya la valoración de todas y cada una de las vulnerabilidades y Ethical Hacking encontradas. Debe contener al menos la siguiente información: equipo en que se detectó la vulnerabilidad, direcciones IP, sistema operativo, Nombre del equipo, vulnerabilidad(es) encontrada(s), severidad, factor de riesgo, puerto, descripción, tipo según el CVE (Riesgos y Vulnerabilidades Comunes), solución propuesta y acciones.

Debe contemplar capítulos como:

- ✓ Reporte del nivel de riesgo basado en las evidencias recolectadas.
- ✓ Reporte vulnerabilidades por ip y servidor.
- ✓ Reporte de vulnerabilidades catalogado por sistema operativo, bases de datos y aplicaciones.
- ✓ Reportes agrupados por solución o tipo de solución.
- ✓ Reporte de servidores contra parches de seguridad del fabricante

2. **Informe gerencial** que resuma el informe técnico, con clasificación de comportamiento y tipificación de las vulnerabilidades detectadas, y presente el estado de las condiciones de seguridad de la

	INSTITUTO NACIONAL DE CANCEROLOGÍA ESE	CÓDIGO:	GDG-P05-F-04
	GESTIÓN DEL GASTO	VERSIÓN:	1
	ANEXO TÉCNICO	VIGENCIA:	09-01-2020
		Página 5 de 8	

infraestructura tecnológica de sistema SAP del INSTITUTO NACIONAL DE CANCEROLOGIA. Debe incluir los resultados de las pruebas de ingeniería social y auditoria de perfiles y roles.

3. **Plan de remediación** detallado de los hallazgos que permita la reducción de las brechas de seguridad informática de la plataforma y la optimización de esta. Este informe debe incluir según la priorización resultante: identificación de brechas de seguridad, recomendaciones a implementar, responsables, y tiempos estimados de ejecución.

No se acepta como informe técnico el resultado de las herramientas utilizadas solamente. Los informes de las herramientas deben ser revisados por el contratista, interpretados y entregados al INSTITUTO NACIONAL DE CANCEROLOGIA para su aprobación.

Los informes y los hallazgos deben ser socializados al Oficial de Seguridad de la Información del INSTITUTO NACIONAL DE CANCEROLOGIA, con la respectiva transferencia de conocimiento que aplique.

- **Compatibilidad de Herramientas:** Las herramientas deben ser compatibles con la plataforma computacional del INSTITUTO NACIONAL DE CANCEROLOGIA, de acuerdo con la siguiente información:
 - Sistemas Operativos AIX V7 o superior
 - Sistemas Operativos Microsoft Windows versiones 2003 a 2012
 - Sistemas Operativos de Usuario Final Windows 7 y Windows 10
 - Sistemas Operativos Linux: Ubuntu, SUSE, Red Hat, Oracle y CentOS
 - Motor de base de datos Db2

2. REQUISITOS TECNICOS

La empresa ofertante debe presentar:

Experiencia General:

- Presentar Experiencia mínima de 5 años en proyectos de servicios y soluciones de tecnología de la información relacionados con seguridad de la información y seguridad informática, cuyo alcance enfoque actividades relacionadas a análisis de vulnerabilidades, pen testing y ethical hacking y controles de seguridad informática para gestionar las vulnerabilidades; cuya permanencia acumulada debe ser mínimo de 1 año.
- Experiencia certificada en proyectos que se acrediten como parte de la experiencia, debieran tener cada uno, un plazo mínimo de ejecución de dos (2) meses
- En caso de consorcios, uniones temporales, se debe acreditar la experiencia a solo una de las compañías que conforman la figura jurídica.

Experiencia Específica:

	INSTITUTO NACIONAL DE CANCEROLOGÍA ESE	CÓDIGO:	GDG-P05-F-04
	GESTIÓN DEL GASTO	VERSIÓN:	1
	ANEXO TÉCNICO	VIGENCIA:	09-01-2020
		Página 6 de 8	

- Experiencia específica en al menos un proyecto relacionado con el análisis de vulnerabilidades en seguridad informática sobre la infraestructura tecnológica, donde uno de los activos de información está relacionado con una aplicación o plataforma relacionada con SAP en la nube o plataforma SAP On Premise, debidamente finalizados y/o en ejecución, a través de un contrato o documento que avale el plan de actividades ejecutados.
- Experiencia específica en al menos tres (3) proyectos relacionados con el objeto a contratar, los cuales deben estar relacionados con el sector salud debidamente finalizados y/o en ejecución, a través de un contrato o documento que avale el plan de actividades ejecutados.

Perfiles Requeridos:

Cantidad personas	Rol	Formación Académica	Experiencia	Cantidad de contratos Terminados
1	Consultor Líder (QA) de Seguridad	Profesional en Ingeniería de Sistemas o Electrónica o Telecomunicaciones o carreras afines con registro en el SNIES. Postgrado / Maestría en seguridad de la información o seguridad informática y contar como mínimo con las siguientes certificaciones: • Certified Ethical Hacking CEH v8 o superior vigente • CISSP (Certified Information Systems Security Professional) • CISM (Certified Information Security Manager) • IPv6 Forum Certified Security Engineer Silver vigente • RISK MANAGER ISO 31000:2018 • ECIH EC-Council Certified Incident Handler • Manager Cybersecurity ISO 27032 • Lead Auditor ISO 27032 • Implementador Líder ISO 27001:2013	Experiencia profesional de mínimo 10 años en seguridad informática.	Experiencia profesional específica en cinco (5) proyectos relacionados con el análisis de vulnerabilidades en seguridad informática sobre la infraestructura tecnológica. Los proyectos que se acrediten como parte de la experiencia, debieron tener, cada uno, un plazo mínimo de ejecución de dos (2) meses
1	Consultor Senior en Seguridad Informática	Profesional en Ingeniería de Sistemas o Electrónica o Telecomunicaciones o carreras afines con registro en el SNIES. Posgrado en seguridad en redes o seguridad informática o seguridad de la información y mínimo cuatro (4) de las siguientes certificaciones: • CISSP (Certified Information Systems Security Professional) • CISM (Certified Information Security Manager) • CEH -Certified Ethical Hacker - EC-Council. • Auditor Líder ISO 27001:2013 (IRCA).	Experiencia profesional de mínimo 5 años en seguridad informática.	Experiencia profesional específica en cuatro (4) proyectos relacionados con el análisis de vulnerabilidades en seguridad informática sobre la infraestructura tecnológica. Los proyectos que se acrediten como parte de la experiencia, debieron tener, cada uno, un plazo mínimo de ejecución de dos (2) meses

	INSTITUTO NACIONAL DE CANCEROLOGÍA ESE	CÓDIGO:	GDG-P05-F-04
	GESTIÓN DEL GASTO	VERSIÓN:	1
	ANEXO TÉCNICO	VIGENCIA:	09-01-2020
		Página 7 de 8	

		• CHFI – Certified Hacking Forensic Investigator -EC-Council. • CISA – ISACA • Auditor Líder ISO 27032. • ECSA/LPT		
1	Consultor junior en Seguridad Informática	Profesional en Ingeniería de Sistemas o Electrónica o Telecomunicaciones o carreras afines con registro en el SNIES. Deseable al menos una (1) de las siguientes certificaciones: • CEH -Certified Ethical Hacker - EC-Council. • CISA -Certified Information Systems Auditor - ISACA. • CISSP - Certified Information Systems Security Professional - ISC2. • Auditor Líder ISO 27001:2013.	Experiencia profesional de mínimo 1 año en seguridad informática.	Experiencia profesional específica en dos (2) proyectos relacionados con el análisis de vulnerabilidades en seguridad informática sobre la infraestructura tecnológica. Los proyectos que se acrediten como parte de la experiencia, debieron tener, cada uno, un plazo mínimo de ejecución de dos (2) meses

El ofertante deberá allegar los siguientes documentos de los perfiles requeridos para la ejecución de las pruebas de Hacking Ético:

- Carta de compromiso y disponibilidad firmada por el profesional propuesto.
- Hoja de vida.
- Fotocopia de la cédula de ciudadanía de cada profesional propuesto o documento de identificación
- Fotocopia del diploma de pregrado.
- Fotocopia de diploma de Posgrado o Maestría solicitada
- Certificaciones de estudio adicionales solicitadas.
- Certificaciones que acrediten la experiencia profesional solicitada.
- Tarjeta profesional y certificado de vigencia de la misma.
- Certificado de vigencia y antecedentes disciplinarios del personal.

Nota 1. En caso de existir discrepancia entre la hoja de vida y los documentos exigidos prevalecerán estos últimos documentos.

Nota 2. En el evento de que un título haya sido obtenido en el extranjero el proponente deberá acreditar la convalidación de dicho título ante el Ministerio de Educación Nacional. Este requisito no se exigirá cuando se trate de profesionales titulados y domiciliados en el exterior que pretendan ejercer temporalmente la profesión en Colombia.

El Ministerio de Educación Nacional homologa los estudios de pregrado (universitarios) por disciplina y/o licenciatura y los de posgrado en los niveles de especialización, incluida los tecnológicos, maestría y doctorado. En el evento que el adjudicatario del presente proceso de selección hubiese ofrecido personal titulado y domiciliado en el exterior en los términos señalados en el proceso, deberá presentar la autorización expedida por el Consejo Profesional Nacional correspondiente.

Nota3. Tener en cuenta que los requisitos técnicos que se propongan en el proceso deben poder ser valorados en la fase de verificación de documentos, por lo tanto, todo requisito solicitado debe ser demostrado por el oferente al momento de entregar la propuesta

Nota 4. Las certificaciones técnicas aceptadas, deberán estar vigentes a la fecha de la presentación de la oferta.

	INSTITUTO NACIONAL DE CANCEROLOGÍA ESE	CÓDIGO:	GDG-P05-F-04
	GESTIÓN DEL GASTO	VERSIÓN:	1
	ANEXO TÉCNICO	VIGENCIA:	09-01-2020
Página 8 de 8			

Nota 5. El ofertante seleccionado cuenta con plena independencia y autonomía de definir el tiempo de dedicación necesaria del personal que requiera para el cumplimiento de las obligaciones y suministrar el personal adicional que considere necesario y pertinente para la ejecución de las actividades del contrato.

2. SUPERVISIÓN DEL CONTRATO

Firma: 

Nombre: Jennifer Dahana Gutierrez

Cargo: Coordinadora de Redes y Hardware

Elaborado por: Carlos Andrés Guerrero / Profesional Especializado I

Versión	Fecha de actualización	Descripción de actualización	Responsable OYM
1	09-01-2020	Versión inicial del documento	Xiomara Falsuly Rubiano Aguilar

"TODA VERSIÓN IMPRESA DE ESTE DOCUMENTO SE CONSIDERA DOCUMENTO NO CONTROLADO"

ELABORÓ		REVISÓ		APROBÓ	
Cargo:	Profesional Universitario	Cargo:	Coordinador Grupo Gestión de Compras y Contratación (E.)	Cargo:	Coordinador Grupo Gestión de Compras y Contratación (E.)
Dependencia:	Oficina Asesora de Planeación y Sistemas	Dependencia:	Grupo Gestión de Compras y Contratación	Dependencia:	Grupo Gestión de Compras y Contratación
Fecha:	09-01-2020	Fecha:	09-01-2020	Fecha:	09-01-2020