empocaldas	F-GC-01 Versión: 13 Julio de 2020	GESTIÓN CONTRATACIÓN
		ESTUDIO DE NECESIDAD DE CONTRATACIÓN

Fecha del estudio	18/05/2023

Objeto de la contratación	CONTRATAR LA PRESTACIÓN DE SERVICIO DE ANÁLISIS DE VULNERABILIDADES (PENTESTING / ETHICAL HACKING) EN LA PLATAFORMA TECNOLÓGICA (EQUIPOS, DISPOSITIVOS, REDES Y MEDIOS DE COMUNICACIÓN) DE EMPOCALDAS S.A. E.S.P.

VERIFICACIONES PREVIAS

Requerimiento previo	N/A

DESCRIPCIÓN DE LA NECESIDAD Y OPORTUNIDAD

Necesidad	La Empresa de Obras Sanitarias de Caldas "EMPOCALDAS S.A E.S.P" es una Sociedad Anónima Comercial de Nacionalidad Colombiana, del orden Departamental, clasificada como empresa de servicios públicos, con autonomía administrativa, patrimonial y presupuestal, que se rige por lo dispuesto en la Ley 142 de 1994 y la Ley 689 de 2001 disposiciones afines y reglamentarias vigentes o por las disposiciones legales que las modifiquen, complementen, adicionen o sustituyan; por las normas del Ministerio Medio Ambiente, Vivienda y Desarrollo Territorial, la Comisión de Regulación de Agua Potable y Saneamiento Básico y la Superintendencia de Servicios Públicos Domiciliarios. El capital de la Empresa en 100% oficial y los accionistas son el Departamento y 21 municipios de Caldas. EMPOCALDAS S.A E.S.P está conformada por una sede administrativa con domicilio en la Ciudad de Manizales y 24 seccionales ubicadas en 20 municipios, 3 corregimientos y 1 centro poblado, pertenecientes al Departamento de Caldas; igualmente cuenta con 22 plantas de tratamiento de agua potable, 10 bombeos y 1 planta de tratamiento de aguas residuales; en su condición de monopolio natural presta de manera integral los servicios de Acueducto y Alcantarillado en los municipios y corregimientos socios. Adicionalmente y tal como lo exige la ley (decreto 2668 del 2000), factura y recauda el servicio de aseo. La sección de Sistemas le brinda apoyo a todas las seccionales de la empresa, solucionando las novedades de Hardware, Software y Comunicaciones en el menor tiempo posible para garantizar el normal funcionamiento de todos los aplicativos que utiliza la empresa, garantizando así el desarrollo del objeto social según los Estatutos. La información es un activo con un alto valor, en consecuencia, requiere una protección adecuada. Esto es especialmente importante en el creciente ambiente de negocios interconectados por redes de datos en el que la información está expuesta a un mayor rango de amenazas y vulnerabilidades (debilidad existente en un sistema que puede ser utilizada por una persona malintencionada para comprometer su seguridad), la continua evolución, crecimiento y sofistificación de los ataques cibernéticos y la convergencia tecnológica, ponen de manifiesto la necesidad de adoptar medidas y controles que permitan proteger las entidades ante las nuevas amenazas; y en este contexto, EMPOCALDAS S.A. E.S.P., como empresa con una importante infraestructura tecnológica y que gestiona varios servicios ofrecidos a través de Internet, desea contratar la realización por parte de una empresa especialista de pruebas de intrusión y análisis de vulnerabilidades (Pentesting / Ethical hacking) en la plataforma tecnológica (equipos, dispositivos, redes y medios de comunicación) por parte de un proveedor externo, con el fin de identificar vulnerabilidades, tratar y mitigar los riesgos que puedan comprometer la seguridad de la información o que puedan afectar la prestación de los servicios de TI con los que cuenta entidad; dichas pruebas deben ser ejecutadas por personal capacitado y con experiencia, aplicando estándares vigentes y reconocidos a nivel internacional. El objeto del presente estudio de necesidad es contratar los servicios informáticos con resultado consistentes en la realización de pruebas de vulnerabilidad de seguridad informática en la infraestructura y sistemas de información de EMPOCALDAS S.A. E.S.P. proporcionando como resultado de las citadas pruebas, los correspondientes test que se realizaran sobre la plataforma tecnológica, los informes de resultados y evaluación, y los entregables. Llas pruebas estarán fundamentalmente encaminadas a buscar debilidades en el control de acceso, autenticación, diseño y o programación en la configuración y despliegue de los sistemas. Cualquier análisis, acceso, intrusion y/o ataque a la seguridad de los sistemas de información de EMPOCALDAS S.A. E.S.P. que con motivo del desarrollo de los trabajos del presente estudio de vulnerabilidades / Pentesting (consiste en una penetración controlada en los sistemas informáticos de una empresa a las cuales se tiene accesos remotamente a través de un browser o navegador) deba llevarse a cabo por el adjudicatario, serán realizados con la máxima diligencia y con el único fin de analizar el estado de la seguridad de los sistemas de información, entornos de operaciones, y elementos de comunicaciones de EMPOCALDAS S.A. E.S.P. de acuerdo con los objetivos señalados en el presente estudio.
Conveniencia	Es conveniente para EMPOCALDAS S.A. E.S.P. "CONTRATAR LA PRESTACIÓN DE SERVICIO DE ANÁLISIS DE VULNERABILIDADES (PENTESTING / ETHICAL HACKING) EN LA PLATAFORMA TECNOLÓGICA (EQUIPOS, DISPOSITIVOS, REDES Y MEDIOS DE COMUNICACIÓN) DE EMPOCALDAS S.A. E.S.P." para continuar con los avances en la implementación de la Política de Gobierno Digital en el Habilitador de Seguridad y Privacidad de la Información y aumentar los niveles de seguridad, cumplimiento de la RESOLUCIÓN NÚMERO 00500 DE MARZO 10 DE 2021.

Oportunidad	Es oportuno para EMPOCALDAS S.A. E.S.P. "CONTRATAR LA PRESTACIÓN DE SERVICIO DE ANÁLISIS DE VULNERABILIDADES (PENTESTING / ETHICAL HACKING) EN LA PLATAFORMA TECNOLÓGICA (EQUIPOS, DISPOSITIVOS, REDES Y MEDIOS DE COMUNICACIÓN) DE EMPOCALDAS S.A. E.S.P." para identificar vulnerabilidades, tratar y mitigar los riesgos que puedan comprometer la seguridad de la información o que puedan afectar la prestación de los servicios de TI, tener el conocimiento del grado de vulnerabilidad de los sistemas de información, que es imprescindible para aplicar las medidas correctivas, así como generar planes de remediación, y tratar los riesgos asociados de acuerdo al Plan de Tratamiento de Riesgos de Seguridad Digital que hace parte del habilitador Seguridad y Privacidad de la Información de la Política de Gobierno Digital.

REQUISITOS TÉCNICOS Y LEGALES DEL BIEN O SERVICIO

Aspectos Técnicos del bien y/o servicio	**Los siguientes son los aspectos mínimos que se debe cumplir para lograr el objeto del contrato:** * Análisis e identificación de vulnerabilidades sobre la plataforma tecnológica (controles de información y datos, niveles de conciencia de seguridad en el personal, niveles de los controles de fraude e ingeniería social, redes de computadoras y telecomunicaciones, dispositivos inalámbricos, dispositivos móviles, seguridad de controles de acceso físico, procesos de seguridad y localizaciones física) de EMPOCALDAS S.A. E.S.P. * Análisis testeo de aplicativos WEB, teniendo como base el top 10 de OWASP en todas sus versiones. * Evaluación Red WAN y LAN * Pruebas de vulnerabilidad y penetración: - Hacking Ético Externo Caja Blanca - Hacking Ético Externo Caja Negra - Hacking Ético Externo Gris - Hacking Ético de Aplicaciones Web - Hacking Ético Interno - Hacking Ético de Sistemas de Comunicaciones (redes de datos, hardware de red, comunicaciones de voz, fraude en telecomunicaciones (uso fraudulento de centralitas, telefonía pública, acceso no autorizado a Internet, redes de transmisión de datos por radio, etc.) con el fin de estudiar la disponibilidad de los sistemas, la posibilidad de una interceptación o introducción no autorizada de información. * Test de Denegación de Servicio (DoS), previa aprobación y coordinación con EMPOCALDAS S.A. E.S.P. * Charla de consideraciones ciberseguridad (concientización seguridad). * Campaña de Ingeniería Social. * El proponente debe contar con personal capacitado y con experiencia, aplicando estándares vigentes y reconocidos a nivel internacional. * El contrato será desarrollado tanto de forma remota con en sitio. **Alcance mínimo de la propuesta:** * 24 (Veinticuatro) servidores * 100 (Cien) Estaciones de trabajo (Sede Administrativa - Manizales) * 1 (Un) Portal Web * Test de Redes WIFI * Análisis de tráfico **Nota:** En la propuesta se debe definir claramente las fases y actividades a desarrollar para el cumplimiento del
	Entregables: * Informe donde se identifiquen los sistemas en los que se ha logrado penetrar y la información confidencial y/o secreta conseguida. * Informe de vulnerabilidades, así como las recomendaciones para solventar cada una de ellas * Informe de Hacking Ético de Sistemas de Comunicaciones, con recomendaciones para solventar las vulnerabiiidades. * Informe final donde se indiquen resultados obtenidos del Test de Denegación de Servicio (DoS) y una descripción de las situaciones específicas en las que se haya conseguido dado el caso. * Lista de Chequeo por Prioridades. (Corto, Mediano y Largo Plazo).

Codificación estándar de producto y servicios de la Naciones Unidas.	CÓDIGO	NOMBRE
	81111700	SISTEMAS DE MANEJO DE INFORMACIÓN MIS
	81111800	SERVICIOS DE SISTEMAS Y ADMINISTRACION DE COMPONENTES DE SISTEMAS
	81140000	ANALISIS DE RIESGO O SEGURIDAD

Ítem	Código inventario	Descripción del bien o servicio	unidad	Cantidad
NA	NA	NA	NA	NA

EXPERIENCIA REQUERIDA	
Condiciones de idoneidad y experiencia que llevan a contratar a la persona natural o jurídica	El proveedor deberá contar con personal calificado con alguna Certificacion en Seguridad tal como: CISSP – GIAC – CEH - THD-EPC La experiencia será un requisito habilitante, el proponente deberá acreditar mediante documento expedido por el contratante haber prestado servicios profesionales similares al objeto del presente estudio de necesidad por valor mayor o igual al presupuesto oficial, en máximo tres (3) contratos.

SOPORTE DE PRECIOS DEL MERCADO				
Persona natural o Jurídica	Contacto	Email	Teléfono	Valor cotización
		Presupuesto Oficial		-

Adjuntar soportes del precio del mercado

Todos los precios deben incluir IVA

Adjuntar matriz de precio del mercado, deberá adjuntar constancia de las condiciones de calidad, condiciones de especialidad o idoneidad del oferente, con su respectiva cotización.

PRESUPUESTO		
Vigencia actual (2023)	Vigencia futura (2024)	Total vigencias
17.850.000	0	17.850.000

Cod. Rubro	Nombre rubro de apropiación	Valor de la apropiación
212020200806	Sistematización	17.850.000
	TOTAL CDP	17.850.000

LA INVERSIÓN OBJETO DEL PRESENTE ANÁLISIS ESTÁ INCLUIDA EN EL POIR?		
Consecutivo del proyecto	Nombre del Proyecto	Año de entrada en Operación
NA	NA	NA

OBLIGACIONES GENERALES DEL CONTRATISTA	
Obligación	APLICA
Cumplir con todas las especificaciones y requerimientos del Estudio de Necesidad de la contratación y aspectos contemplados en la solicitud de oferta.	**Aplica**
El contratista deberá concertar con el supervisor un cronograma de actividades o plan de entregas de acuerdo al objeto del contrato y las necesidades de la Empocaldas S.A. E.S.P..	**Aplica**
Asumir por su cuenta y riesgo todos los gastos en el desarrollo del contrato.	**Aplica**
Presentar el pago de aportes a la seguridad social cada mes al supervisor del contrato con el fin de autorizar el pago correspondiente.	**Aplica**
En caso de tener trabajadores a cargo deberá suministrar los elementos de protección requeridos para el desarrollo de su función y asegurarse de que los usen.	**Aplica**
Sin perjuicio de la autonomía técnica y administrativa, atender instrucciones y lineamientos que durante el desarrollo del contrato se le impartan por parte de la Empocaldas S.A. E.S.P. (Supervisor). Como presentar los informes que se exija.	**Aplica**
En el evento que algún o algunos de los elementos sea rechazado por el supervisor del contrato, dichos productos deberán ser retirados por cuenta y riesgos del contratista a la mayor brevedad posible. (o en el tiempo indicado en la invitación) El contratista deberá corregir cualquier problema que se presente, respondiendo por partes dañadas, por su cuenta y riesgo durante la garantía.	**No aplica**
Responder por los daños que ocasione en desarrollo del contrato a Empocaldas S.A. E.S.P. y a terceros afectados.	**Aplica**
Informar oportunamente al supervisor del contrato, los inconvenientes en la entrega de los bienes objeto de suministro y proponer soluciones para garantizar la prestación del servicio.	**Aplica**

Las demás obligaciones a su cargo que se deriven de la naturaleza del contrato y de las exigencias legales.	**Aplica**
Cada tubo suministrado debe ser marcado con los siguientes datos: 1) Número de Identificación del tubo o Código de trazabilidad, 2) Número de certificado, 3) Organismo de certificación del producto, 4)Número del Lote, 5) Fabricante de la tubería, 6) NIT-DV	**No aplica**
Junto con la tubería se deberá entregar la siguiente tabla con los datos solicitados:	**No aplica**
Número de Identificación del tubo / Número de certificado / Organismo de certificación del producto / Número del Lote / Fabricante de la tubería / NIT-DV	**No aplica**
	No aplica
- En la columna **"Número de certificado"**, se debe indicar el número de certificación de la tubería. - En la columna **"Organismo de certificación del producto"**, se debe escribir el Nombre o Razón social del organismo que realiza servicios de evaluación y certificación de la conformidad de la tubería. - En la columna **"Número del lote"**, Indicar el número del lote del fabricante al cual pertenece la tubería. - En la columna **"Fabricante de la tubería"**, se debe indicar el Nombre o Razón social de la empresa fabricante o empresa importadora de la tubería. - En la columna **"NIT-DV"**, se debe escribir el Número de identificación tributaria y dígito de verificación de la empresa fabricante o empresa importadora de la tubería.	**No aplica**
Para el caso de mercancías que se requieren que sean entregadas en las seccionales o en las plantas, se debe coordinar con el Administrador de la seccional, garantizando la debida anticipación para el adecuado descargue de las mercancías y una correcta inspección de los elementos entregados.	**No aplica**
El descargue de las mercancías se debe realizar por cuenta y riesgo del contratista.	**No aplica**
Para los bienes cuya entrega deba realizarse la sede administrativa en la ciudad de Manizales, ésta debe hacerse en la sección de suministros para verificar, de manera conjunta con el Supervisor del contrato, la entrada y el estado de las mercancías recibidas	**No aplica**
Se considerará como recibida la mercancía, por parte de EMPOCALDAS S.A. E.S.P en la sede central (Sede Administrativa de Manizales) cuando el documento de entrega cuente con la firma del Jefe de la Sección de Suministros y del Supervisor o los supervisores del contrato.	**No aplica**
Se considerará como recibida la mercancía, por parte de EMPOCALDAS S.A. E.S.P en las seccionales, cuando el documento de entrega cuente con la firma del Administrador en la respectiva remisión, y en el caso de contratos, adicionalmente se requiere la firma del Supervisor.	**Aplica**
OBLIGACIONES ESPECIFICAS DEL CONTRATISTA	
Las obligaciones específicas a cargo del contratista serán las siguientes:	APLICA
Prestar los Servicios con la diligencia y calidad de personal profesional tecnológico experto, asignando a la ejecución de las prestaciones objeto del contrato personal cualificado y con conocimientos en la materia, según los perfiles técnicos exigidos en el presente estudio.	**Aplica**
Llevar a cabo la ejecución del plan de pruebas presentado en la oferta de acuerdo a las especificaciones técnicas y cronograma acordado entre ambas partes.	**Aplica**
Solicitar autorización previa y por escrito a EMPOCALDAS S.A. E.S.P. para la realización de Servicios consistentes en ataques que puedan implicar una posible parada de servicio y/o pruebas en la que exista un riesgo significativo de pérdida de servicio.	**Aplica**
Elaborar y proporcionar a EMPOCALDAS S.A. E.S.P. toda la documentación, informes y entregables derivados de la ejecución del presente estudio de vulnerabilidades y en particular los descritos en el apartado "REQUISITOS TÉCNICOS Y LEGALES DEL BIEN O SERVICIO".	**Aplica**
Informar inmediatamente de cualquier riesgo grave detectado durante la ejecución del Servicio y que pudiera afectar a la integridad disponibilidad y confidencialidad de los sistemas de EMPOCALDAS S.A. E.S.P. incluidos en el plan de pruebas.	**Aplica**
El adjudicatario expresamente acepta y reconoce que todos los derechos de propiedad intelectual derivados de los trabajos realizados por el adjudicatario para EMPOCALDAS S.A. E.S.P. en relación con los Servicios objeto del presente estudio y posterior contrato (en adelante también obras resultantes de los trabajos realizados) corresponderán única y exclusivamente a EMPOCALDAS S.A. E.S.P.	**Aplica**

El adjudicatario guardará el debido secreto empresarial acerca de todo el know how o saber hacer resultante de la ejecución de los Servicios que sean contratados por EMPOCALDAS S.A. E.S.P. de acuerdo con lo previsto en el presente estudio postrior contrato, manteniendo dicha información en reserva y secreto por el adjudicatario y no siendo revelada de ninguna forma, en todo o en parte, a ninguna persona física o jurídica que no sea parte del contrato.	**Aplica**

OBLIGACIONES ESPECIFICAS DE EMPOCALDAS	
Las obligaciones específicas a cargo de Empocaldas S.A. E.S.P. serán las siguientes:	APLICA
Pago oportuno de las obligaciones contraídas con el contratista, después del visto bueno del supervisor del contrato 30 días después.	**Aplica**
Entrega de certificaciones y demás documentos solicitados por el contratista para el óptimo desarrollo del Contrato.	**Aplica**

LUGAR Y PLAZO DE EJECUCIÓN	
Lugar de ejecución	Manizales, Carrera 23 No. 75 - 82
Plazo de ejecución	45 días calendario a partir de la suscripción del acta de inicio

FORMA DE PAGO	
Forma de Pago	Actas parciales, previa verificación y autorización del supervisor del contrato
Condiciones para Pago	El contratista entiende que en virtud de la ordenanza 816 del 22 de Diciembre de 2017 de la Asamblea Departamental de Caldas, el recaudo sobre las estampillas se efectuará mediante retención sobre los anticipos, pagos parciales, pagos o abonos en cuenta; por lo tanto el contratista autoriza con la firma del presente contrato y/o carta de presentación de la oferta para que la Empocaldas S.A. E.S.P. efectué los descuentos correspondientes por el monto equivalente al valor de las estampillas 1. Presentación de la factura 2. Informe de recibo de almacén. 3. Certificado de cumplimiento expedido por el supervisor. 4. Certificado o planilla del pago de aportes de seguridad social y/o aportes parafiscales según corresponda. 5. Las demás que requiera el supervisor del contrato y la lista de chequeo de Empocaldas S.A. E.S.P.

Estampilla a descontar	APLICA
Estampilla Pro Universidad (1%)	**Aplica**
Estampilla Pro Desarrollo (2%)	**Aplica**
Estampilla Pro Hospital (1%)	**Aplica**
Estampilla Pro Adulto mayor (3%)	**Aplica**
Contribución Especial (5%) - Sólo aplica para obras	**No aplica**

ASIGNACIÓN Y DISTRIBUCIÓN DEL RIESGO
Riesgo
Está a cargo de contratista, el incremento de precios de los elementos relativos a la materia prima para producir el bien a adquirir a nivel nacional e internacional.
Está a cargo del contratista el riesgo comercial, entendido como los eventos desfavorables relacionados con el valor y pago del contrato, causados por variaciones en las condiciones del mercado, aumento en los factores de producción, en el valor de los insumos o de los fletes
Está a cargo del contratista el riesgo país, entendido como el cambio de las políticas en el país de origen.
Está a cargo del contratista el riesgo operativo, entendido como los eventos relacionados con los procesos de producción, transporte y entrega del producto, tales como: Falta de disponibilidad de Materia Prima, insuficiente capacidad de producción, retrasos en el tiempo de entrega, incumplimiento en los protocolos de la Empocaldas S.A. E.S.P. para la entrega de producto, entrega de producto no conforme, pérdida, destrucción o deterioro antes de efectuar la recepción en la Empocaldas S.A. E.S.P..
Esta a cargo del contratista el Incumplimiento de las obligaciones contractuales establecidas, como calidad del elemento suministrado. Fuga de información confidencial y privilegiada de la entidad. Pérdida de los elementos a suministrar.

La forma de mitigarlos será con la constitución de las garantías respectivas, calidad, cumplimiento y responsabilidad civil extracontractual.

SUPERVISIÓN

Nombre del Supervisor Administrativo	Cargo del Supervisor
DIANA PATRICIA SALAZAR MONTES	JEFE SECCIÓN SISTEMAS
Nombre del Supervisor Técnico	Cargo del Supervisor
DIANA PATRICIA SALAZAR MONTES	JEFE SECCIÓN SISTEMAS

GARANTÍAS

Tipo de garantías	APLICA
Póliza de garantía de seriedad de la oferta.	**No aplica**
Cumplimiento	**Aplica**
Salarios, prestaciones sociales e indemnización de personal	**No aplica**
Estabilidad y calidad de la obra	**No aplica**
Responsabilidad civil extracontractual	**No aplica**
Calidad y correcto funcionamiento de bienes y equipos suministrados	**No aplica**
Calidad	**Aplica**

TIPO DE CONTRATO

Tipo de contrato	
Suministros	**No aplica**
Arrendamiento	**No aplica**
Obra	**No aplica**
Consultoría	**No aplica**
Prestación de Servicio	**Aplica**
Interventoría	**No aplica**
Compra Venta	**No aplica**
Orden de compra o Servicio	**No aplica**
Convenio Inter-Administrativo	**No aplica**
Contrato Inter-Administrativo	**No aplica**
Otro	**No aplica**

De acuerdo con lo establecido en el Manual de Contratación de la Empresa y la Ley 142 de 1994, se hace necesario realizar el citado contrato, cumpliendo con los parámetros legales señalados en las normas anteriormente citadas y las demás complementarias. SE CONSIDERA OPORTUNA Y LEGAL LA CELEBRACIÓN DE ESTE CONTRATO

Solicitado por:	
Firma	
Nombre	DIANA PATRICIA SALAZAR M
Cargo	Jefe Sección Sistemas

Aprobado por:	
Firma	
Nombre	YUDY CRISTINA ALZATE CARDONA
Cargo	Jefe Administrativa y Financiera

Revisión Jurídica:	
Firma	
Nombre	LUCY ANDREA RODRIGUEZ JIMENEZ
Cargo	SECRETARIA GENERAL

Propuesta:

Pentesting Aplicativos Web

Hacking Ético – Infra Estructura Tecnológica

empocaldas
Construyendo juntos tu bienestar

Mayo 8 de 2023

Las partes se comprometen a mantener la confidencialidad absoluta con respecto a la información contenida en el presente documento. Esta "Información", solo podrá ser utilizada exclusivamente para el desarrollo de la(s) actividad(es) acordadas por las partes y las cuales han dado origen a este documento. Igualmente, las partes se comprometen a tomar todas las medidas necesarias para que la información no llegue a manos de terceros bajo ninguna circunstancia.

Carrera 14 # 12 A 35 Piso 1 - Manizales
Sedes: Colombia – Ecuador – Bolivia - Panamá
Telefax: (57-6) - 8804020 – Cel: 3116865526 - Email: itf@itforensic-la.com

THD SECURITY GROUP SAS
NIT.900.923.967-2
Carrera 14 # 12 A 35 Piso 1
Sedes: Colombia – Ecuador – Panamá –Bolivia
Telefax: (096) 8804020 Cel:3116865526
www.itforensic-la.com
www.thehackingday.com
thd@thdsecurity.com

Manizales, Mayo 8 de 2023 **THD2023-040**

Ingeniera
Diana Patricia Salazar Montes
Jefe Sección de Sistemas
Empocaldas S.A
Ciudad

Asunto: **Test de Seguridad Aplicativos Web y Hacking Ético Infraestructura Tecnológica**

Respetada Ingeniera

Reciba un cordial saludo **THD Security GROUP S.A.S** Correspondiéndole a su gentil invitación y respondiendo a sus necesidades presentamos nuestro portafolio de servicios.

IT FORENSIC Company y **ThD Security Group S.A.S** cuenta con más de Quince años (15) de experiencia transferida y complementada, es una empresa líder en Latinoamérica con expansión a nivel nacional e internacional del área de seguridad informática, con la experiencia comprobada, producto del conocimiento del mercado de delitos informáticos, de la formación técnica y experiencia de sus socios y del grupo de especialistas que tiene a su disposición, de su participación del mercado como proveedores de servicios a empresas importantes de la región y aplicación de las mejores prácticas, con el soporte directo de consultores líderes a nivel mundial.

Contamos con experiencia comprobada sobre las vulnerabilidades actuales del sector empresarial, lo que nos permitirá crear estrategias de TI para mitigarlas, conociendo habilidades tecnológicas del mercado colombiano y de otros países lo que nos permite tener un aseguramiento de los activos más importantes de una empresa, **LA INFORMACIÓN**, nuestro Know How cuentan con la formación académica y técnica a través de un grupo de especialistas certificados y reconocidos internacionalmente por su trayectoria en el ámbito de la Seguridad de los Datos Digitales.

Nuestra empresa ha tenido presencia tanto a nivel nacional en empresas públicas y privadas, como lo es también en el exterior: Ecuador, Panamá, México, Bolivia y Venezuela.
Hemos participado a través de nuestros proyectos de investigación y académicos en eventos Internacionales de Seguridad Informática y Computo Forense.

PRODUCTOS BANDERA

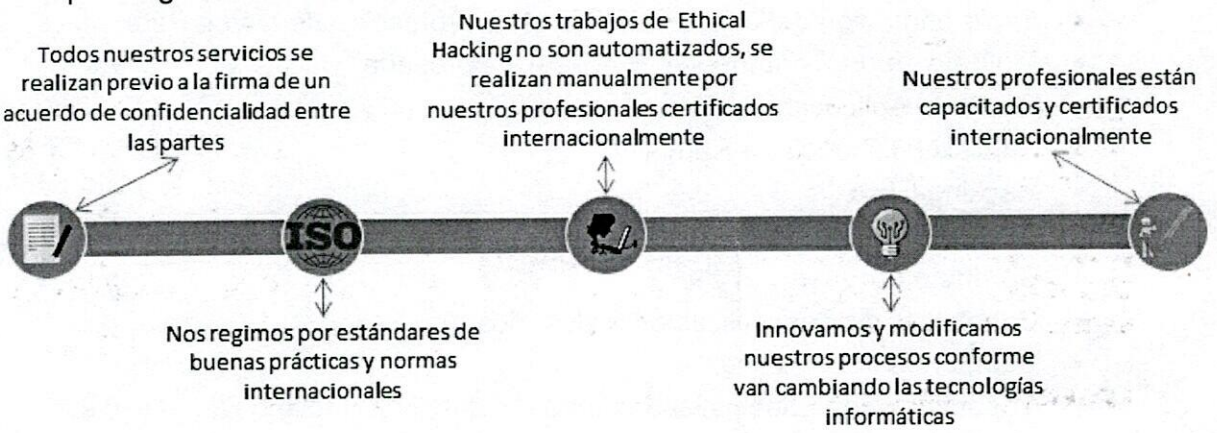
Nuestro portafolio cubre una alta gama de servicios y consultorías relacionadas con la protección de la seguridad de la información digital, a continuación, se enumeran los que son más solicitados a nuestra empresa.

- Implementación de un SGSI (Sistema General de Seguridad de la Información)
- Implementación de la ley Habeas Data y protección de Datos Personales
- Montaje de un Cortafuegos (Firewall) Empresarial
- Testeo a Aplicaciones Web
- Análisis de Trafico de Red
- Hacking Ético
- Auditoria de Sistemas Informáticos
- Computo Forense
- Campañas de Sensibilización a Usuarios
- Campañas de Phishing
- Capacitaciones Especializadas a través del "The Hacking Day – Project"
- Seguridad Prepagada
- Seguridad Gerenciada
- Seguridad Gestionada
- Solución de AntiVirus
- Control de Fuga de Información
- Recuperación de Información Eliminada
- Libros de Seguridad Informática de la Editorial 0xword
- Entre Otros

Sea la ocasión para agradecer la confianza y oportunidad que nos brindan para ofertar la prestación de nuestros servicios y entregar a ustedes con nuestra experiencia la estabilidad a su Core de negocio y protección de su información e infraestructura de TI, en las sucursales que requieran, con todo el soporte de nuestra compañía y con Talento humano certificado.

Deseamos el éxito del desarrollo de sus proyectos y que cada uno de ellos este enfocado a la mejora continua tanto en lo tecnológico como en la seguridad digital de la misma, es por esto, que puede contar con un socio estratégico como nosotros; ya que nuestra marca y experiencia han permitido a muchas empresas brindar al cliente final y proveedores la confianza requerida en las operaciones y procesos cuando la interconectividad es un factor clave.

Por qué elegirnos:



Cordialmente,

ING JHON CESAR ARANGO S
GERENTE – THD Security Group SAS
jca@itforensic-la.com
Sur – América

1. Resumen Ejecutivo

Esta propuesta contiene una serie de servicios profesionales, requeridos para el análisis testeo de sus aplicativos WEB, teniendo como base el top 10 de OWASP así como la evaluación de la Red WAN y LAN

2. Introducción

Un proyecto de ***PENTESTING WEB*** consiste en una penetración controlada en los sistemas informáticos de una empresa a las cuales se tiene accesos remotamente a través de un browser o navegador. El resultado es un informe donde se identifican los sistemas en los que se ha logrado penetrar y la información confidencial y/o secreta conseguida.

OSSTMM (Open-Source Security Testing Methodology Manual)

Es una metodología revisada por profesionales para realizar pruebas y métricas de seguridad. Las pruebas de OSSTMM están divididos en 6 secciones los cuales prueban colectivamente: controles de información y datos, niveles de conciencia de seguridad en el personal, niveles de los controles de fraude e ingeniería social, redes de computadoras y telecomunicaciones, dispositivos inalámbricos, dispositivos móviles, seguridad de controles de acceso físico, procesos de seguridad y localizaciones física como edificios, perímetros y bases militares.

Las distintas modalidades de Ethical Hacking son los siguientes:

Hacking Ético Externo Caja Blanca

Se nos facilita información para poder realizar la intrusión (normalmente las direcciones IP a testar). Se analizan en profundidad y extensión todas las posibles brechas de seguridad al alcance de un atacante de los sistemas de comunicaciones sometidos a estudio. Opcionalmente, el ámbito de actuación se puede ampliar a máquinas no perimetrales. El resultado es un informe amplio y detallado de las vulnerabilidades, así como las recomendaciones para solventar cada una de ellas.

Hacking Ético Externo Caja Negra

Es esencialmente lo mismo que en el de Caja Blanca con la dificultad añadida de que no se nos facilita ningún tipo de información inicial.

Hacking Ético Externo Gris

es la auditoría que mezcla características de las dos anteriores, se pude dar a conocer parte de la información al auditor y pedirle que a partir de ella intente "escalar" al resto del sistema.

Hacking Ético de Aplicaciones Web

Se simulan los intentos de ataque reales a las vulnerabilidades de una o varias aplicaciones determinadas, como pueden ser: sistemas de comercio electrónico, de información, o de acceso a bases de datos. No es necesaria la entrega del código fuente de la aplicación. El resultado es un informe amplio y detallado de las vulnerabilidades, así como las recomendaciones para solventar cada una de ellas.

Hacking Ético Interno

El ámbito de esta auditoría es la red interna de la empresa, para hacer frente a la amenaza de intento de intrusión, bien por un empleado que pueda realizar un uso indebido o una persona con acceso a los sistemas o un hacker que hubiera conseguido penetrar en la red. Para este servicio se hace necesaria la presencia de nuestros especialistas en las instalaciones de la empresa que se va a auditar. El resultado es un informe amplio y detallado de las vulnerabilidades, así como las recomendaciones para solventar cada una de ellas.

Hacking Ético de Sistemas de Comunicaciones

En esta auditoría se analiza la seguridad de las comunicaciones tales como: redes de datos, hardware de red, comunicaciones de voz, fraude en telecomunicaciones (uso fraudulento de centralitas, telefonía pública, acceso no autorizado a Internet, redes de transmisión de datos por radio, etc.) principalmente para estudiar la disponibilidad de los sistemas, la posibilidad de una interceptación o introducción no autorizada de información. El resultado es un informe amplio y detallado de las vulnerabilidades, así como las recomendaciones para solventar cada una de ellas.

Test de Denegación de Servicio (DoS)

Este test refleja el grado de solidez o resistencia de un servicio ante la agresión de un atacante local o remoto que intente deshabilitarlo. En nuestro informe final se indican los resultados obtenidos y una descripción de las situaciones específicas en las que se haya conseguido dicha denegación, si fuera el caso.

Beneficios

- Conocimiento del grado de vulnerabilidad de los sistemas de información, que es imprescindible para aplicar las medidas correctivas.
- Reducción de aquellos riesgos que, en caso de materializarse las amenazas que les originan, pueden representar pérdidas ingentes de capital, bien por facturación fallida, por reposición de los daños causados, por pérdida de oportunidad de negocio, por reclamación de clientes, por sanciones legales etc.
- Ahorro de tiempo y dinero al afrontar y corregir situaciones nefastas antes de que ocurran y nos obliguen a resolverlas con prisas y a cualquier precio.
- Mejora de la imagen y revalorización de la confianza en la empresa/institución de los accionistas, inversores, empleados, funcionarios públicos, autoridades, proveedores y clientes al mostrarles que se toman medidas diarias para garantizar la continuidad del negocio.

3. Alcance Y Metodología

Los servicios específicos ofrecidos en el marco de esta propuesta son los siguientes:

3.1. Alcance

Los servicios específicos ofrecidos en el marco de esta propuesta tendrán como alcance:

- Hasta 24 Servidores
- Hasta 100 Estaciones de Trabajo (Sede Principal)
- Hasta 1 Portales Web
- Test de Redes WiFi
- Análisis de Trafico

Nota: No se realizará ningún ataque de negación de servicio (DoS), sin la aprobación y coordinación con la empresa contratante.

3.2. Fase 1 - Planeación

Análisis de Riesgos y Vulnerabilidades

- Conformación y presentación del equipo de trabajo.
- Desarrollo del plan de trabajo a seguir.
  - Pentesting Servidores
  - Revisión Entorno Web Server y su Configuraciones
  - Revisión de Performance de la Web Application
  - Análisis de Seguridad WebApp
- Establecer cronograma de actividades.
- Autorización por escrito para desarrollar la presente propuesta. (en caso de der un tercero, se requiere firma adicional del canal directo).
- Firmas de los compromisos de confidencialidad
- Entrega de lista de chequeo del trabajo a realizar (66 Controles).
- Entrega del dominio o IP del aplicativo Web, e Ip's Publicas a Evaluar

3.3. Fase 2 - Ejecución

Desarrollo de las diferentes actividades propuestas en el plan de trabajo:

Pentesting IP's

Este tema cubre todo el tipo de auditoria de sistemas intrusivos sobre los servidores anfitriones de las aplicaciones web y las Ip's objetivos, orientando al cliente a la realización de este tipo de pruebas en todas sus fases, tales como:

- Red y dispositivos de Red
- Redes Inalámbricas
- Servidores
- Estaciones de Trabajo
- Y demás elementos definidos en el alcance

Revisión de entorno Web Server y sus configuraciones

- Reconocimiento de entorno y paquetes instalados y sus versiones.
- Revisión de buenas prácticas en configuración de Web Server.
- Pruebas de rendimiento actual de contenido estático.
- Auditoria de consumo de recursos al servir contenido estático.
- Elaboración de informe del status actual del Web Server.

Análisis de Seguridad WebApp

- Mapeo completo de todo el Web Site (Carpetas, link módulos, archivos)
- Scan de puertos habilitados y tipos de conexión.
- Revisión de Estabilidad y conexión al Web Server
- PRUEBAS DE INTRUSIÓN A NIVEL DE APLICACIONES WEB (Top 10 Owasp 2023 – Mitre Top25)
    - Pruebas de acceso remoto al portal (login , fuerza bruta)
    - Pruebas de Inyección
    - Pruebas XSS
    - Pruebas de Gestión de Sesiones
    - Pruebas de Referencia Directa
    - Pruebas CSRF
    - Pruebas de Configuración de Seguridad
    - Pruebas de Protocolos Criptográficos
    - Pruebas de Restricción Acceso URL
    - Pruebas a Nivel de Protocolo de Transporte
    - Pruebas de Redirecciones Invalidas
    - Pruebas de Subida de Archivos
    - Pruebas de Vulnerabilidades en Aplicaciones Web Conocidas
    - Otras Pruebas
- PRUEBAS DE INTRUSIÓN A NIVEL DE BASES DE DATOS
    - Pruebas de Control de Acceso
    - Pruebas a Nivel de Protocolo de Transporte
    - Otras Pruebas
- FASE DE DOCUMENTACIÓN DE RESULTADOS
    - Elaboración del informe de auditoría.
    - Incluye recomendaciones para correcciones necesarias a realizar
    - Scan de vulnerabilidades a todo el Web Site, posterior a las correcciones realizadas
    - Elaboración del informe de auditoría (Final)
- Exposición de Datos recabados en el análisis Web - Informe Ejecutivo.

3.4. Fase 3 - Informes

- Entrega de informes a la empresa contratante (Informe Técnico y Ejecutivo) y discusión con el equipo de trabajo de los hallazgos encontrados y con el plan de trabajo a seguir.
- Recomendaciones Futuras.
- Lista de Chequeo por Prioridades. (Corto, Mediano y Largo Plazo)

4. Presupuesto

4.1. Precio

SERVICIO	PRECIO
Pentesting Web y Hacking Ético	**$ 15.000.000**
IVA	**$ 2.850.000**
TOTAL	**$ 17.850.000**

4.2. Condiciones Comerciales

- Los precios de esta propuesta están expresados en Pesos Colombianos.
- Los pagos quedan estipulados de la siguiente manera:
  - 50% En Fase de Planeación
  - 50% a la Entrega de los Informes

4.3. Condiciones Generales de la oferta

- El trabajo se realizará una vez se cuente con la orden de servicios por parte de la empresa, donde se presentará un cronograma de actividades para el desarrollo de las mismas y a la firma de las cláusulas de confidencialidad entre las partes.

5. Valores Agregados

VALOR AGREGADO 1

TALLERES Y CHARLAS DE SENSIBILIZACION

ThD Security Group dará los siguientes valores agregados:

- 1 charlas de 60 Minutos con el tema **"Consideraciones de Ciberseguridad – 2023"**, para ser impartidas al personal interno de la Empresa a través de Zoom
- Una **Campaña de Ingeniería Social (Tipo Phishing)**, para medir el grado de sensibilización de los empleados en estos temas
- 1 Charla teórica que instruya a los implicados a cerrar las brechas encontradas en el presente análisis.

VALOR AGREGADO 2

REVISION POST INFORMES FINALES DE APLICACION DE CORRECTIVOS

ThD Security Group, hasta 3 meses después de la entrega del informe final, hará una revisión de los Ítems catalogados como **CRITICOS** que el Oficial de Seguridad determine para conocer si fueron aplicadas o no las medidas de Control.

6. Cronograma de Actividades

Aunque se estima un tiempo de 4 Semanas de trabajo (Remoto y en Sitio) y 1 Semanas laborables para desarrollo de informe final y presentación del mismo, este puede variar de acuerdo a disposición del personal interno de la empresa.

Se recuerda que en la fase de planeación se pasara un cronograma detallado.

7. Opciones de Teletrabajo

Es de aclarar que todo nuestro personal cumple con las recomendaciones de Bio Seguridad adoptadas por el gobierno nacional, para estos tiempos de pandemia. Sin embargo, si la empresa nos da los accesos tecnológicos adecuados podemos realizar el trabajo de manera remota.

8. Equipo de Trabajo

Todas las actividades realizadas durante la duración de los servicios profesionales estarán a cargo del siguiente equipo de trabajo:

Gerente de Proyecto

- Especialista en Redes y Telecomunicaciones
- Certificaciones de Seguridad: CISSP – GIAC – Microsoft – ITU – CEH – THD-EPC Instructor, FTK
- Certificaciones en Redes: CCNA – 3com
- Certificaciones en SO: Linux, Windows
- Certificación en Telefonía IP: Asterisk
- Docente y Consultor de varias empresas de la región
- 22 Años de Experiencia en Seguridad de la Información
- Auditor Líder BS 7799-2 (ISO 27001:2005)
- Certificado GSEC (SANS)

Ethical Hackers

- Ingeniero de Sistemas
- Certificaciones de Seguridad: CEH - CREA
- Docente y Consultor de varias empresas de Sur América
- 8 Años de Experiencia en Seguridad de la Información
- Acuerdos de Confidencialidad firmados con IT Forensic & THD Security Group

9. Gestión del Cambio

Todos los trabajos realizados durante esta consultoría serán facturados a un costo fijo. Si se descubren nuevos detalles necesarios diferentes a los señalados en la presente propuesta de servicios, y/o si son solicitadas tareas adicionales que estén consideradas por fuera del alcance del trabajo a realizar, cualquier costo adicional, demora o tiempo de espera será definido, documentado y acordado de manera mutua previo al inicio de cualquier tarea nueva o adicional.

10 Legislación

THD Security Group SAS. Se somete a todas las leyes Colombianas vigentes que sean aplicables en los aspectos laborales, industria y comercio, contratación estatal, e impuestos etc.; La Empresa no aceptará como causal de reclamo o incumplimiento la ignorancia de la Ley de Colombiana.

THD SECURITY GROUP SAS
NIT.900.923.967-2
Carrera 14 # 12 A 35 Piso 1
Sedes: Colombia – Ecuador – Panamá –Bolivia
Telefax: (096) 8804020 Cel:3116865526
www.itforensic-la.com
www.thehackingday.com
thd@thdsecurity.com

REERENCIAS COMERCIALES
NACIONAL

Cámara de Comercio de Manizales por Caldas
Confa Contigo, con todo
codesa
Universidad Católica de Manizales
FISCALIA GENERAL DE LA NACION
ALCALDÍA DE MANIZALES
super La magia de la alegría
Compañía Cafetera La Meseta S.A. Café para el mundo
Cámara de Comercio Pereira POR RISARALDA
UFPS Universidad Francisco de Paula Santander
BAC Business Alliance for Secure Commerce
GOBERNACIÓN DE CALDAS EN LA RUTA DE LA PROSPERIDAD
Normandy
CÁMARA DE COMERCIO DE BUCARAMANGA Creemos en Santander
Solati tecnología | innovación | nube
Industria Licorera de Caldas
Ceiba Motor Confianza en Movimiento
MEDIUM
Pontificia Universidad JAVERIANA Colombia
Universidad Pontificia Bolivariana
MegaRed
MEDIA commerce
Aladino Salas de Juegos
QBCo.
Ford El Roble Motor Tu concesionario Ford
FINESA COMPAÑÍA DE FINANCIACIÓN ESPECIALIZADA
INFIVALLE

INTERNACIONAL