Supersubsidio

ADENDA No. 02

PROCESO SELECCIÓN ABREVIADA POR SUBASTA INVERSA No. SSF SASI 003 DE 2024

La Secretaria General de la Superintendencia de Subsidio Familiar, con base al literal a) el numeral Segundo del Artículo segundo de la Resolución 426 de 2014 por el cual se delega la ordenación del gasto y en uso de la las facultades constitucionales y legales, especialmente las conferidas en el artículo 12 de la ley 80 de 1993 y las establecidas en los artículos 2.2.1.1.1.3.1 y 2.2.1.1.2.2.1 del decreto 1082 de 2015 y el decreto 142 del 1 de febrero de 2023, a través de la presente adenda INFORMA QUE:

Que el día 31 de octubre de 2024, la **SUPERINTENDENCIA DEL SUBSIDIO FAMILIAR** realizó la Apertura y publicación de Pliego de Condiciones Definitivo del proceso selección abreviada por Subasta Inversa No. SSF SASI 003 DE 2024 cuyo objeto es: "*PRESTAR SERVICIOS DE MONITOREO Y ATENCIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN (ID: OTIC-756)*".

Que el día 08 de noviembre de 2024, el proponente OPEN GROUP, presenta de manera extemporánea observación referente al Anexo Técnico del proceso SSF-SASI-003 DE 2024; en respuesta la Entidad señala que:" (...) En atención a la observación del interesado, la Superintendencia del Subsidio Familiar ha realizado la respectiva validación del estudio de mercado, en el cual se evidenció que el ítem mencionado no fue contemplado. Por tal motivo, la Superintendencia del Subsidio Familiar informa que acoge su solicitud y, en consecuencia, procederá a retirar el ítem mencionado (...)"

Que, el día 08 de noviembre de 2024 por medio de comunicación interna la jefe de la Oficina TIC, solicita lo siguiente: "(...)

Modifíquese el numeral 1.4 del anexo técnico denominado- Especificaciones Técnicas Generales del Servicio de Gestión de Vulnerabilidades, el cual quedara así:

1.4 Especificaciones Técnicas Generales del Servicio de Gestión de Vulnerabilidades.

Gestión, atención y análisis de Incidentes: En el momento de detectar actividades sospechosas, se deberá realizar un análisis exhaustivo que permita determinar la naturaleza y el alcance del incidente, incluida la identificación de la causa raíz y el impacto potencial.

Gestión y análisis de Vulnerabilidades: Realizar evaluaciones regulares de vulnerabilidades en la infraestructura de la organización y coordinar la aplicación de parches y actualizaciones de seguridad para mitigar posibles riesgos.

Gestión y atención de incidentes de Seguridad: Coordinar y gestionar todos los aspectos relacionados con los incidentes de seguridad, incluyendo la comunicación

con las partes interesadas internas y externas, la documentación de los incidentes y la realización de informes 'post-mortem' para mejorar los procesos de seguridad.

Gestión de alertas: Deberá gestionar los diferentes eventos, alertas o incidentes de seguridad informática y ciberseguridad.

El proveedor deberá poner a servicio de la Superintendencia del Subsidio Familiar, al menos dos usuarios para poder realizar test de vulnerabilidades a demanda para los activos de información tanto a nivel externo aquellos expuestos a internet como interno aquellos expuesto únicamente en la red local de entidad.

Tipo de amenazas a analizar: se enlistan a continuación sin embargo se aclara que no se deben limitar a las mencionadas a continuación:

o Malware y ransomware.

o Phishing.

o Ataques DDoS.

o Violencia de datos.

o Vulnerabilidades y parches: Seguimiento de sistemas que no están actualizados y que pueden ser objetivos fáciles para atacantes

o Tendencias en amenazas emergentes

En general las nuevas tácticas, técnicas y procedimientos (TTP) utilizados por atacantes, y los incidentes relacionados con la falta de cumplimiento de regulaciones y su impacto en la seguridad.

Las herramientas dispuestas para realizar el análisis podrán ser establecidas por el contratista según considere.

El análisis deberá permitir realizar comparativos mensuales que permitan identificar patrones en el tiempo.".

Que, al revisar LA SOLICITUD PRESENTADA SE PROCEDE A MODIFICAR EL Anexo Técnico del Proceso Sai-003 de 2024 SOC, a través de la presente adenda así:

RESUELVE

PRIMERO: MODIFICAR el numeral 1.4 del anexo técnico denominado- Especificaciones Técnicas Generales del Servicio de Gestión de Vulnerabilidades, el cual quedara así:

1.4 Especificaciones Técnicas Generales del Servicio de Gestión de Vulnerabilidades.

Gestión, atención y análisis de Incidentes: En el momento de detectar actividades sospechosas, se deberá realizar un análisis exhaustivo que permita determinar la naturaleza y el alcance del incidente, incluida la identificación de la causa raíz y el impacto potencial.

Gestión y análisis de Vulnerabilidades: Realizar evaluaciones regulares de vulnerabilidades en la infraestructura de la organización y coordinar la aplicación de parches y actualizaciones de seguridad para mitigar posibles riesgos.

Gestión y atención de incidentes de Seguridad: Coordinar y gestionar todos los aspectos relacionados con los incidentes de seguridad, incluyendo la comunicación

con las partes interesadas internas y externas, la documentación de los incidentes y la realización de informes 'post-mortem' para mejorar los procesos de seguridad.

Gestión de alertas: Deberá gestionar los diferentes eventos, alertas o incidentes de seguridad informática y ciberseguridad.

El proveedor deberá poner a servicio de la Superintendencia del Subsidio Familiar, al menos dos usuarios para poder realizar test de vulnerabilidades a demanda para los activos de información tanto a nivel externo aquellos expuestos a internet como interno aquellos expuesto únicamente en la red local de entidad.

Tipo de amenazas a analizar: se enlistan a continuación sin embargo se aclara que no se deben limitar a las mencionadas a continuación:

o Malware y ransomware.

o Phishing.

o Ataques DDoS.

o Violencia de datos.

o Vulnerabilidades y parches: Seguimiento de sistemas que no están actualizados y que pueden ser objetivos fáciles para atacantes

o Tendencias en amenazas emergentes

En general las nuevas tácticas, técnicas y procedimientos (TTP) utilizados por atacantes, y los incidentes relacionados con la falta de cumplimiento de regulaciones y su impacto en la seguridad.

Las herramientas dispuestas para realizar el análisis podrán ser establecidas por el contratista según considere.

El análisis deberá permitir realizar comparativos mensuales que permitan identificar patrones en el tiempo.".

SEGUNDO: Las demás estipulaciones del Pliego de Condiciones y anexo técnico, así como los demás documentos publicados NO SON MODIFICADOS NI ACLARADOS con la presente adenda, se mantienen como se expidieron originalmente.

PUBLÍQUESE Y CÚMPLASE

KATERIN GOMEZ OLAYA
SECRETARIA GENERAL

Proyectó: Andrés Barrios Suárez/ Abogado Contratista Grupo de Gestión Contractual
Reviso por parte de la Oficina TIC/ Luisa Fernanda Pardo Sánchez Jefe Oficina TIC
Reviso por parte de la Oficina TIC/ Juan Pablo López Mejia/ Oficina TIC

Revisó: Sandra Patricia Gaitán Fajardo/ Abogada Contratista Grupo de Gestión Contractual
Revisó: Jenny Milena Collazos Caro/ Coordinadora Grupo de Gestión Contractual