Al contestar refiérase
al oficio No.13199

26 de agosto, 2020
DFOE-SOC-0862

Licenciada
Geaninna Dinarte Romero
Ministra
MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL (MTSS)

Estimada señora:

Asunto: Comunicación con respecto a la realización de pruebas de penetración a la plataforma Bono Proteger.

Con el propósito de complementar la auditoría que está realizando este Órgano Contralor, vinculada con la plataforma tecnológica implementada para gestionar el Bono Proteger, nos permitimos comunicarle que se van a desarrollar, con la colaboración de la empresa Deloitte and Touche, pruebas para evaluar la seguridad de la plataforma tecnológica que soporta el Bono Proteger, específicamente se implementarán una batería de pruebas de penetración (conocidas como PenTest).

Dentro de este contexto, se detallan de seguido las partes interesadas y sus respectivos roles, a saber:

Ministerio de Trabajo y Seguridad Social: Como encargado de la ejecución del Programa Bono Proteger, y de la implementación de la plataforma tecnológica que le respalda, tendrá la responsabilidad de facilitar el acceso a la plataforma implementada por medio del proveedor.

Continum Datacenter: Como desarrollador y operador de la plataforma tecnológica deberá facilitar los recursos técnicos necesarios para llevar adelante las pruebas y en caso de ser necesario tomar las medidas que sean necesarias para solventar las vulnerabilidades que sean detectadas.

Deloitte & Touche: Empresa que colaborará con la realización de las pruebas de penetración a la plataforma tecnológica, remitirá los informes que sean acordados entre partes. Además, deberá respetar las condiciones de privacidad y confidencialidad que sean pactadas de previo al inicio de las pruebas.

Contraloría General de la República: Funge como ente fiscalizador y como coordinador entre las partes. En cuyo caso, en todo momento será informado del avance

alcanzado en la ejecución de las pruebas, y en colaboración con la empresa citada *(Deloitte & Touche)*, valorará la calidad de los entregables.

A mayor abundamiento sobre este particular, el objetivo es alcanzar una seguridad razonable sobre las salvaguardas presentes en la plataforma mediante:

-Pruebas a los controles de seguridad del sistema WEB utilizados para mitigación de ataques cibernéticos
-Pruebas a los controles de seguridad de la infraestructura que soporta el sistema WEB y que tiene presencia o están expuestos en internet de manera pública
-Revisión de mecanismos de seguridad implementados en la plataforma WEB que no correspondan a temas de programación, lógica o flujo de datos del sistema
-Utilización de metodologías y estándares internacionales para la ejecución del proyecto

Estas pruebas tienen por alcance la evaluación de controles de seguridad tanto perimetral (elementos circundantes) como a nivel de plataforma web (la aplicación propiamente). Esto implica:

- Pruebas de penetración a componentes externos
- Pruebas de penetración y revisión de vulnerabilidades del sistema Web Proteger
- Pruebas a controles de seguridad adicionales utilizados por la plataforma Proteger
- Revisión de vectores de ataque adicionales

Al tratarse de una herramienta de acceso público, basada en la web, se ve expuesta a una serie de riesgos de seguridad, uno de los más relevantes, es el de acceso no autorizado, sea por parte de un actor mal intencionado (cibercriminal) o por desconocimiento (acceso fortuito) en cuyo caso se podría ver expuesta información sensible.

Resulta importante mencionar que, para la revisión de informes semanales de avance que se generen, la discusión de los resultados parciales así como del informe final, se requiere instaurar un equipo de trabajo interinstitucional, conformado por especialistas técnicos del MTSS, la empresa desarrolladora de la plataforma y de la Contraloría General de la República, quienes revisarán cada entregable y verificarán que se encuentre acorde con lo especificado en cada prueba solicitada.

Cabe agregar que, toda la documentación e información a que tenga acceso la empresa colaboradora en este proceso se considerará confidencial y para ello se requiere la firma de un acuerdo en este sentido. Los informes de avance, resultados parciales y el informe final serán tratados de manera confidencial hasta tanto no sean solventadas cualesquiera debilidades manifestadas en los mismos.

Finamente, no se omite señalar que, las fechas específicas para la realización de las pruebas deben ser acordadas en forma conjunta con ese Ministerio, por lo que se agradece que, a partir de la recepción del presente oficio, se asigne a un colaborador del

MTSS como enlace para atender este particular, y se comunique a este Órgano Contralor, al correo electrónico contraloria.general@cgrcr.go.cr con copia a la Licda Viria Rodríguez Salas, correo electrónico viria.rodriguez@cgr.go.cr, coordinadora de la presente auditoría.

Para cualquier consulta no dude en contactar a la señora Rodríguez Salas, al correo electrónico indicado, o vía telefónica al número 2501-8162 o 2501-8384.

Atentamente,

CONTRALORIA GENERAL DE LA REPUBLICA
COSTA RICA

Firmado digitalmente por MANUEL JESUS CORRALES UMAÑA
Fecha: 2020-08-26 16:02

Lic. Manuel Corrales Umaña, MBA.
GERENTE DE ÁREA

AZG/VRS/

Ce: Licda. Jensie Bolaños Vega, Asesora Despacho Ministerial, MTSS
jensie.bolanos@mtss.go.cr

G: 2020002318-1