Al contestar refiérase
al oficio N° 17890

12 de noviembre, 2020
DFOE-SOC-1117

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

Estimada señora:

Asunto: Solicitud de información sobre las pruebas de penetración a la plataforma Bono Proteger.

Como parte de la auditoría de carácter especial sobre la plataforma tecnológica implementada para gestionar el Bono Proteger y el proceso de las pruebas de penetración, revisión de vulnerabilidades, verificación de posibles ataques de ingeniería social y pruebas de concepto que se encuentra realizando esta Contraloría General; el 10 de noviembre pasado se realizó una sesión de trabajo con el Director Nacional de Empleo y el representante de Continum Datacenter S.A, con el fin de conocer algunos controles implementados en la plataforma tecnológica que gestiona el Bono Proteger para evitar posibles ataques.

Al respecto, se nos indicó que se consideraba oportuno que dicho requerimiento fuese realizado por este medio, de ahí que se le agradece suministrar la siguiente información:

A. Para cada dominio mostrado en la sesión de trabajo, a saber: www.proteger.go.cr y www.proteger.payfacility.com, señale lo siguiente:

1. La distinción de los procesos que se realizan en cada uno.
2. Los datos de los solicitantes que se administran en cada uno.
3. Explicar si el convenio de donación incluye ambos dominios.
4. ¿Cómo se procederá con la devolución y eliminación de la información relacionada con Bono Proteger de ambos dominios, al finalizar el convenio?

B. Para las siguientes preguntas, que fueron respondidas en la sesión de trabajo, favor remitir la evidencia solicitada en cada uno de los ítemes:

1. ¿Qué tipos de mecanismos de monitoreo, defensa y prevención ante amenazas cibernéticas posee el sitio web PROTEGER (IPS, IDS, WAF)?
   Evidencia solicitada: Captura de pantalla del *dashboard* de las herramientas que posee la plataforma para evitar estas amenazas.

2. ¿Durante la etapa de pruebas se realizó algún tipo de análisis de código con respecto a alguna guía de buenas prácticas, antes de salir a producción?
   Evidencia solicitada: Captura de pantalla de los correos electrónicos donde se remiten los informes de vulnerabilidades realizados y se pueda ver la fecha de envío.

3. ¿El alojamiento de la aplicación web es administrado en servidores locales o de un proveedor (tercero ajeno a la entidad)?
   Evidencia solicitada: Captura de pantalla del virtualizador donde se pueda observar los servidores virtualizados que soportan la aplicación de Bono Proteger.

4. ¿Existen planes de contingencia en caso de que se presente alguna falla en el sistema o se presenten ataques cibernéticos que puedan afectar el rendimiento o disponibilidad de la aplicación (DDoS, DoS, entre otros)?
   Evidencia solicitada: Protocolo de contingencia implementado ante una posible falla en la aplicación del Bono Proteger.

5. ¿Se transmiten datos considerados sensibles o confidenciales a través de enlaces de comunicación no cifrados?
   Evidencia solicitada: Captura de pantalla de una parte de la configuración de los enlaces mencionados en la sesión, a través de los cuales se administra información sensible.

6. ¿Qué controles específicos se tienen implementados para la validación de caracteres especiales en campos de texto, ataques de directorios transversales, mensaje de errores de la aplicación, desbordamiento de *buffer*, *Cross site scripting*, inyección de código, entre otros?
   Evidencia solicitada: Captura de pantalla donde se observe el método de validación/limitación en la programación de la aplicación de los datos que se ingresan en los campos de texto.

7. ¿Existe algún proceso o plan que indique cómo proceder una vez identificada una vulnerabilidad en la aplicación web, que contemple como resolverla, plan de acción y criticidad?
   Evidencia solicitada: Captura de pantalla donde se observe el protocolo interno definido ante vulnerabilidades identificadas y reportadas o correos

electrónicos donde se identifique cómo la aplicación se sacó de producción para remediar alguna vulnerabilidad identificada.

En virtud de la importancia de contar con la información solicitada, se le agradece suministrar a más tardar el **17 de noviembre** de los corrientes. La presente solicitud de información se realiza con fundamento en los artículos números 13 y 21 de la Ley Orgánica de esta Contraloría General, N° 7428.

ara cualquier consulta no dude en contactar al correo electrónico viria.rodriguez@cgr.go.cr, o vía telefónica al número 2501-8162.

Cabe aclarar que, dada la naturaleza de la información solicitada, tanto la presente solicitud como la respuesta que se reciba serán tratados como información de acceso restringido por parte de este Órgano Contralor.

No se omite señalar que, el número uno en color rojo ubicado en la parte superior derecha de este oficio, es indicativo de que este documento tiene carácter confidencial, por lo que debe guardar las previsiones contenidas en los numerales 6 de la Ley General de Control Interno, N° 8292 y 8 de la Ley N° 8422, referentes al tema de la confidencialidad en el manejo de la documentación y la información.

Atentamente,

CONTRALORIA GENERAL DE LA REPUBLICA ★ COSTA RICA ★

Firmado digitalmente por MANUEL JESUS CORRALES UMAÑA
Fecha: 2020-11-12 15:43

Lic. Manuel Corrales Umaña. MBA
GERENTE DE ÁREA

VMRS/AFRA/JMER/mmg

Ce: Licda. Jensie Bolaños Vega, Asesora Despacho Ministerial
Lic Marcos Solano Chacón, Director Nacional de Empleo

G: 2020002318-1