Fundación Karisma

GOBIERNO DE COLOMBIA

CASO DE ÉXITO EN LA APLICACIÓN DE LA POLÍTICA DE SEGURIDAD DIGITAL Y EJEMPLO DE COLABORACIÓN Y CORRESPONSABILIDAD ENTRE GOBIERNO Y SOCIEDAD CIVIL

31 de agosto de 2017

1. INTRODUCCIÓN

La política nacional en materia de seguridad digital tuvo un cambio importante en el 2016 cuando se adoptó el nuevo CONPES 3854 de 2016 de seguridad digital. Al día de hoy la política favorece la gestión de riesgo como elemento central para abordar la seguridad digital. Además, estableció la necesidad de incluir el modelo de múltiples partes interesadas en este contexto.

Los cuatro principios fundamentales de la política de seguridad digital que describe el CONPES son respetar los derechos humanos, adoptar un enfoque incluyente y colaborativo, asegurar una responsabilidad compartida y adoptar un enfoque basado en la gestión de riesgos. Estos principios suponen que las múltiples partes interesadas (gobierno, empresas, funcionarios públicos, sociedad civil, organismos militares, comunidad técnica, ciudadanía, etcétera) participen activa y conjuntamente en mitigar riesgos de seguridad digital y en elevar las capacidades para enfrentarlos.[1]

En un esfuerzo conjunto entre el gobierno y la sociedad civil se ha logrado fortalecer la seguridad digital de la información publicada en la página web de La Unidad para la Atención y Reparación Integral a las Víctimas, dando cumplimiento a la normatividad vigente relacionada con la protección de datos personales.

Este caso de éxito es debido a la participación entre el gobierno y la sociedad civil ante riesgos de seguridad digital, teniendo en cuenta lo difícil que es lograr la cooperación de diferentes actores en un tema sensible como el que se menciona.

1 Departamento de Planeación. *Política Nacional de Seguridad Digital*. Conpes 3854 de 11 de abril de 2016. Disponible en https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf.

2. ANTECEDENTES

Fundación Karisma, como organización de la sociedad civil que se ocupa de analizar la intersección entre tecnología y derechos humanos, se propuso analizar sitios web del Gobierno colombiano para evaluar la información que ofrecen a la ciudadanía, la seguridad digital que implementan y la forma cómo protegen su privacidad. El propósito de estos análisis es mejorar estas características de los sitios web y beneficiar tanto a la ciudadanía como a las entidades responsables de estos sitios. De estos ejercicios deben surgir aprendizajes cruzados que se pueden incluir dentro de las estrategias de uso de las tecnologías de la información y las comunicaciones (TIC) para las instituciones del Estado.

Es así como la Fundación Karisma, realizó una exploración del sitio web de La Unidad para la Atención y Reparación Integral a las Víctimas -UARIV-, www.unidadvictimas.gov.co encontrando algunos aspectos a mejorar en la seguridad del mismo.

El informe fue presentado realizándose seguimiento a los avances derivados del mismo en tres reuniones con equipos de trabajo de La UARIV y el MinTIC. Durante estas reuniones se llegaron a acuerdos sobre cómo avanzar. Bajo la coordinación de MinTIC, la Unidad implementó en corto tiempo, una serie de medidas tendientes a minimizar los riesgos identificados en el marco de la metodología establecida y basados en las buenas prácticas.

3. OBJETIVO

El informe que se presentó daba cuenta del estado en que se encontraba el sitio web de la Unidad para la Atención y Reparación Integral a las Víctimas durante abril y mayo de 2017, ocupándose de tres ejes principales: (1) cumplimiento de los requisitos de la Ley de protección de datos (información legal, transparencia y contratos); (2) seguridad digital del sitio web; y (3) prácticas para proteger la privacidad.

Con ello, lo que se buscaba era fortalecer la seguridad digital de la información publicada en la página web de la UARIV www.unidadvictimas.gov.co por medio de la aplicación de la gestión de riesgos relacionados con los comentarios realizados por la Fundación Karisma, reduciendo su probabilidad de ocurrencia.

4. METODOLOGÍA

La UARIV toma como marco de referencia para verificar el cumplimiento de buenas prácticas, las normas y estándares de aceptación universal definidas en los modelos de control COBIT, CRISK, ISO27001 e ITIL, de la siguiente manera:

La metodología de análisis de riesgo llevada a cabo por la Unidad como respuesta al informe de Karisma contempló los lineamientos definidos por el Modelo Estándar de Control Interno 2014

(MECI), la Guía para Administración de Riesgos del DAFP y la Norma Técnica de Gestión de Riesgos NTC31000. En el proceso la UARIV identificó el riesgo para cada uno de los hallazgos —que incluye la determinación de las causas y consecuencias—; determinó su respectiva valoración del riesgo — que incluye la calificación de la probabilidad de que sucedan eventos no deseados y su impacto para determinar el riesgo inherente—; estableció y evaluó los controles necesarios para la mitigación de los riesgos; y diagnosticó el riesgo residual una vez ejecutadas las mejoras.

La Fundación Karisma, con el apoyo de Access Now [2], realizó el análisis del sitio web de la Unidad, buscando con ello, ayudarles a mejorar los aspectos mencionados anteriormente.

5. ASPECTOS TRABAJADOS

- En relación con los servicios que transmiten información personal de usuarios, la Unidad realizó el aseguramiento mediante la implementación del protocolo seguro https, para algunos servicios, aplicaciones y la página web de la Unidad.
- Frente a la divulgación de las políticas de privacidad y protección de datos personales, la Unidad generó las respectivas políticas, así como el aviso de privacidad, publicados en la sección inferior de la página Web de la Unidad.
- Frente al tema de seguridad digital y posible fuga de datos, la Unidad implementa el control de acceso para minimizar el riesgo de fuga de información de un reporte con información sensible.
- Respecto al tema de Actualizaciones de los servidores y vulnerabilidades, La Unidad está en proceso de actualización del software del servidor Web en ambiente de pruebas del sitio de la Unidad: www.unidadvictimas.gov.co
- En lo referente a Rastreo (tracking) y privacidad, la Unidad tomó acciones correctivas frente a la configuración de herramientas de servicios de búsqueda y estadísticas de visitas al sitio web, en el marco de la gestión de riegos.

6. ACOMPAÑAMIENTO Y SEGUIMIENTOS DE LAS MEJORAS A FUTURO

Con el objetivo de asegurar que las acciones realizadas se mantengan en el tiempo, el MinTic se encargará de hacer el debido seguimiento al trabajo realizado de fortalecimiento en la seguridad de la presencia en línea de la UARIV, y la Fundación Karisma se compromete a acompañar a una organización de la sociedad civil que representen a las víctimas, con el fin de incrementar sus capacidades en este tema y puedan hacer seguimiento al trabajo de fortalecimiento de la presencia en línea de esta entidad gubernamental.

2 Access Now es una ONG internacional que trabaja en temas de derechos digitales y apoya este trabajo de Fundación Karisma en temas de seguridad digital. Su sitio web está disponible en https://www.accessnow.org/.

7. CONCLUSIONES GENERALES DE BUENAS PRÁCTICAS Y APRENDIZAJES DEL CASO DE ÉXITO

a. La seguridad digital es un asunto de toda la sociedad y sus instituciones. Crear espacios para que las partes colaboren en la identificación de vulnerabilidades y en su solución, a pesar de lo complejo que pueda ser, no solo es importante, sino que es una necesidad.
b. Se requiere diseñar y establecer espacios debidamente reglamentados en los que la sociedad civil, la comunidad técnica y/o cualquier persona pueda reportar vulnerabilidades sobre la infraestructura tecnológica del Estado, y crear canales para atenderlos y hacer seguimiento.
c. Muchos de los problemas identificados en el sitio web de la Unidad para la Atención y Reparación Integral a las Víctimas pueden presentarse en otros sitios web. Es importante crear un mecanismo que permita aprovechar de manera constructiva estos ejercicios para actualizar e integrar las buenas prácticas identificadas en los lineamientos y manuales del gobierno en línea.
d. Se deben mantener las acciones de cada actor como resultado de este tipo de ejercicios, que siempre deberán tender a salvaguardar la seguridad digital de la información publicada por las entidades.

8. LA CORRESPONSABILIDAD EN ACCIÓN

La corresponsabilidad es uno de los aspectos más importantes que introduce la nueva política de seguridad digital. Este enfoque reconoce que hay un papel para todos los actores involucrados. El caso de éxito descrito en este documento muestra que es posible el trabajo de diferentes actores para el reporte, solución y seguimiento de problemas de seguridad digital y que el éxito se logra con la disposición de diálogo y cooperación de todas las partes interesadas.