ALCALDÍA MAYOR DE BOGOTÁ - SECRETARÍA GENERAL
Rad. No. 2-2018-5409
Fecha: 09/03/2018 15:47:29
Destino: ENTIDADES DISTRITALES
Copia: N/A
Anexos: N/A

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA GENERAL

CIRCULAR N°. 010

Para: **SECRETARIOS(AS) DE DESPACHO, DIRECTORES(AS) DE DEPARTAMENTOS ADMINISTRATIVOS, GERENTES Y DIRECTORES(AS) DE UNIDADES ADMINISTRATIVAS ESPECIALES, GERENTES PRESIDENTES(AS) Y DIRECTORES(AS) DE ESTABLECIMIENTOS PÚBLICOS, EMPRESAS INDUSTRIALES Y COMERCIALES, SOCIEDADES PÚBLICAS, SOCIEDADES MIXTAS, ENTES UNIVERSITARIOS, HOSPITALES, ALCALDES LOCALES, VEEDOR DISTRITAL, CONTRALOR DISTRITAL Y LOCALES, DE BOGOTÁ, PERSONERO DE BOGOTÁ.**

De: **ALTA CONSEJERÍA DISTRITAL DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES.**

Asunto: **CUIDADOS PAGINAS WEB ENTIDADES DITRITALES EN PROCESO ELECTORALES**

Teniendo en cuenta que en el año 2018 se desarrollaran diferentes procesos electorales, desde la oficina de la Alta Consejería Distrital de TIC, recomendamos estar atentos y vigilantes a sus sitios Web con dominios gov.co como prevención en cualquier caso de ataque que pretenda desestabilizar las jornadas electorales.

Por tanto a la hora de proteger los sitios web, es importante tener en cuenta diferentes aspectos de Ciberseguridad, que harán aumentar la resiliencia del sistema, y por ende la confianza que la ciudadanía tiene depositada en nuestro portafolio de trámites y servicios publicados en el sitio web de la entidad.

Entre los posibles ataques, se encuentran entre otros ataques "DoS" denegación de servicio dirigido a las aplicaciones web que están incluidas, estos no solo se llevan a cabo a través de la sobrecarga del sistema, saturación del servicio o agotamiento del ancho de banda, sino a través de la explotación de vulnerabilidades en la aplicación, por lo que la regla de seguridad más importante es instalar las actualizaciones de

seguridad que sean publicadas y que solucionen posibles problemas de seguridad en la aplicación.

Además es muy recomendable disponer del sistema CAPTCHA en los formularios de las diferentes web, de esta manera no será posible ejecutar un ataque automatizado a través de ellos.

Existen ataques de tipo "Defacement" estos son usado por ciberdelincuentes cuyo objetivo es modificar una sitio web total o parcialmente. En la mayoría de las ocasiones suelen modificar textos o incluir imágenes llamativas en la página principal de la web. Algunas de las motivaciones son de: carácter político, sociocultural, publicidad de un grupo de ciberdelincuentes, económicas, etc; buscando dañar a su vez la imagen de la entidad atacada.

Para prevenir que el sitio web sea víctima de esta actividad delictiva, se recomienda: Utilizar metodologías de desarrollo seguro a la hora de construir la web, garantizar un acceso seguro al panel de control del sitio web, realizar copias de seguridad periódicas de todos los elementos que conforman el sitio web, mantener el gestor de contenidos actualizado, guardar registros de la actividad generada en el servidor.

Por último los ataques de Phishing, son otra forma de robo de identidad que se produce cuando un sitio web malicioso suplanta a otro legítimo con el fin de engañar al usuario para que proporcione información confidencial, como contraseñas, detalles de la cuenta o números de tarjetas de crédito.

Estos pueden ser contrarrestados mediante el uso e implementación de certificados de seguridad digital SSL (Secure Sockets Layer), estos certificados mantienen la información encriptado y segura en sitios web. El uso de estos en los sitios web permiten a la entidad:

- Que los datos compartidos en las plataformas de Internet, solo pueden ser consultados, editados, manipulados y manejados por la parte correspondiente, ya sea el emisor o el receptor.
- Cifrar la información confidencial durante las transacciones en línea.
- Cada certificado SSL contiene información exclusiva y autenticada sobre el propietario del certificado.
- Una autoridad de certificación verifica la identidad del propietario del certificado SSL cuando se emite.

En ese sentido es de crucial importancia el monitoreo preventivo a lo largo de la jornada electoral, con el fin de prevenir, detectar y atender oportunamente los posibles incidentes que puedan presentarse, apoyando el ejercicio de la labor democrática de la ciudadanía y su normal desarrollo.

Cabe recomendar que cada entidad deberá tomar las medidas de prevención necesarias para asegurar y fortalecer sus páginas Web, y no ser víctimas de personas inescrupulosas.

Las dudas respecto a dichos temas serán con gusto atendidas por la funcionaria María del Pilar Niño Campos a través del correo electrónico: mpninc@alcaldiabogota.gov.co o al teléfono 3813000 Ext. 3061.

Cordialmente,

SERGIO MARTÍNEZ MEDINA
Alto Consejero Distrital de TIC

Anexos: Ninguno.
Proyectó: María Del Pilar Niño Campos
Revisó: Iván Mauricio Hernández Lanao.