1. OBJETIVO

Definir las medidas de prevención, detección y corrección frente a las amenazas causadas por códigos maliciosos en el Senado de la República

2. ALCANCE

Inicia con el registro de la solicitud en la herramienta de gestión de incidentes y finaliza con la documentación del caso.

Los lineamientos definidos deben ser aplicados por todos los funcionarios, contratistas, practicantes, judicantes, pasantes o terceros del Senado de la República.

3. TÉRMINOS Y DEFINICIONES

Antivirus: son programas cuyo objetivo es detectar y eliminar virus informáticos. Con el transcurso del tiempo, la aparición de sistemas operativos más avanzados e internet, los antivirus han evolucionado hacia programas más avanzados que además de buscar y detectar virus informáticos consiguen bloquearlos, desinfectar archivos y prevenir una infección de los mismos. Actualmente son capaces de reconocer otros tipos de malware como spyware, gusanos, troyanos, rootkits, pseudovirus etc.[1]

Antimalware: El software anti-malware bloquea y elimina de forma efectiva y eficiente el malware. Este software incluye el núcleo de protección de las suites de seguridad, aunque obviando algunos extras que no resultan necesarios para combatir el malware, como el control parental o administradores de contraseñas.[2]

Antispam: El principal objetivo de una herramienta antispam, es lograr un buen porcentaje de filtrado de correo no deseado. Pero tampoco deben identificar al correo deseado como no deseado, pues eso traería peores consecuencias que "olvidar" filtrar algún spam.[3]

Algoritmo: es un conjunto prescrito de instrucciones o reglas bien definidas, ordenadas y finitas que permiten llevar a cabo una actividad mediante pasos sucesivos que no generen dudas a quien deba hacer dicha actividad.[4]

Código malicioso: El código malicioso es un tipo de código informático o script web dañino diseñado para crear vulnerabilidades en el sistema que permiten la generación de puertas traseras, brechas de seguridad, robo de información y datos, así como otros perjuicios potenciales en archivos y sistemas informáticos. Se trata de un tipo de amenaza que no siempre puede bloquearse con solo un software antivirus. Según Kaspersky Lab, no toda la protección antivirus puede tratar ciertas infecciones causadas por código malicioso, que es diferente del malware. El término malware se refiere específicamente a software malicioso, pero el código malicioso incluye scripts de sitios web que pueden aprovechar vulnerabilidades con el fin de cargar malware.[5]

Criptología: a disciplina que se dedica al estudio de la escritura secreta, es decir, estudia los mensajes que, procesados de cierta manera, se convierten en difíciles o imposibles de leer por entidades no autorizadas. [6]

Cifrar: es un procedimiento que utiliza un algoritmo de cifrado con cierta clave (clave de cifrado) para transformar un mensaje, sin atender a su estructura lingüística o significado, de tal forma que sea incomprensible o, al menos, difícil de comprender a toda persona que no tenga la clave secreta (clave de descifrado) del algoritmo.[7]

Malware: Malware hace referencia a cualquier tipo de software malicioso que trata de infectar un ordenador o un dispositivo móvil. Los hackers utilizan el malware con múltiples finalidades, tales como extraer información personal o contraseñas, robar dinero o evitar que los propietarios accedan a su dispositivo. Puede protegerse contra el malware mediante el uso de software antimalware.[8]

Firewall: Un firewall o cortafuegos es un programa informático o un hardware que brinda protección a una computadora (ordenador) o a una red frente a intrusos. Se trata de un sistema cuya función es bloquear el acceso no permitido al equipo o a la infraestructura en cuestión.[9]

IPS: Un IPS es un sistema de prevención/protección contra las intrusiones y no solo para reconocerlas e informar acerca de ellas, como hacen la mayoría de los IDS. Hay dos características principales que distinguen a un IDS de un IPS: el IPS se localiza en línea dentro de la red IPS y no solo escucha de manera pasiva a la red como un IDS (tradicionalmente colocado como un rastreador de puertos en la red); el IPS tiene la habilidad de bloquear inmediatamente las intrusiones, sin importar el protocolo de transporte empleado y sin reconfigurar un dispositivo externo[10]

Herramientas de seguridad informática: conjunto de dispositivos o servicios de protección informática como lo son ips, firewall, antivirus

Phishing: conocido como suplantación de identidad, es un término informático que denomina un modelo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña, información detallada sobre tarjetas de crédito u otra información bancaria). El cibercriminal, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas.[11]

---

[1] https://definicion.de/firewall/

[2] https://es.ccm.net/contents/163-sistema-de-prevencion-de-intrusiones-ips

[3] https://es.wikipedia.org/wiki/Phishing

[4] http://www.alegsa.com.ar/Dic/antispam.php

[5] https://es.wikipedia.org/wiki/Algoritmo

[6] https://latam.kaspersky.com/resource-center/definitions/malicious-code

[7] https://es.wikipedia.org/wiki/Criptolog%C3%ADa

[8] https://es.wikipedia.org/wiki/Cifrado_(criptograf%C3%ADa)

[9] https://www.avast.com/es-es/c-malware

[10] https://es.wikipedia.org/wiki/Antivirus

[11] http://www.mejor-antivirus.es/preguntas/antimalware.html

4. RESPONSABLES

- **Jefe División de Planeación y Sistemas:** es responsable del cumplimiento del procedimiento

- **Administrador herramienta de seguridad:** personal que administra las diferentes herramientas de seguridad informática

- **Grupo de control de cambios:** grupo que revisa aprueba o niega las solicitudes del formato de control de cambios

- **Administradores de infraestructura:** personal que apoya la administración de los diferentes servicios prestados por la entidad

- **Personal Técnico de primer nivel de Mesa de Servicios:** es responsabilidad del personal de la mesa de servicios realizar el registro de todas solicitudes, incidentes y problemas por la herramienta de gestión para la mesa de servicios.

- **Personal Técnico Especializado Segundo Nivel Senado:** nivel de escalamiento especializado para dar solución a un caso, incidente o problema técnico de mesa de servicio.

5. CONDICIONES GENERALES

El Senado de la República, cuenta con un sistema de detección y prevención de intrusos de antivirus, herramienta de Anti-Spam y sistemas de control de navegación, con el fin de asegurar que no se ejecuten virus o códigos maliciosos.

Se debe restringir la ejecución de aplicaciones y mantener instalado y actualizado el antivirus, en todas las estaciones de trabajo y servidores del Senado de la República.

Se debe restringir la ejecución de código móvil, aplicando políticas a nivel de sistemas operativos, navegadores y servicio de control de navegación. Todos los funcionarios, colaboradores y terceros que hacen uso de los servicios de tecnología de la información y comunicaciones del Senado de la República son responsables del manejo del antivirus para analizar, verificar y eliminar virus o código malicioso del computador, los dispositivos de almacenamiento fijos, removibles, archivos, correo electrónico que estén utilizando para el desempeño de sus funciones laborales.

A- El Senado de la República a través de los administradores de Infraestructura y la mesa de servicios, administrarán los recursos tecnológicos para la protección de la información y los recursos de procesamiento, adoptando mecanismos necesarios para evitar su divulgación, modificación o daño permanente ocasionados por la contaminación o el contagio de software malicioso.

B- El Senado de la República a través de la mesa de servicios y los administradores de Infraestructura tecnológica, debe asegurar que el software de antivirus, antimalware, antispam y antispyware o la herramienta de gestión con la que cuente la entidad, tenga las licencias de uso requeridas y las actualizaciones periódicas dadas por el fabricante.

C- El Senado de la República a través de la mesa de servicios y de los administradores Infraestructura Tecnológica , deben garantizar que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antispyware, antispam, antimalware.

D- El usuario no deberá hacer uso de software que no sea instalado por los administradores de Infraestructura y mesa de servicios, toda vez que esto puede llevar a infecciones por virus u otro tipo de código malicioso.

E- Los usuarios deben asegurarse de que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos o instalación de software malicioso.

F- Para evitar problemas de códigos maliciosos a través de medios extraíbles o correo electrónico, los usuarios, deben realizar la verificación respectiva de los archivos a través del software de antivirus, instalado en sus equipos cada vez que instale o conecte un dispositivo o se reciban archivos sospechosos por correo electrónico.

G- Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar inmediatamente a la mesa de servicios del Senado de la República con el fin de tomar las respectivas medidas de prevención o escalamiento según sea el caso.

6. DESCRIPCIÓN DE ACTIVIDADES

No.	Descripción de la Actividad	Responsables o Rol	Registros
PROCEDIMIENTO PROTECCIÓN CONTRA CÓDIGO MALICIOSO			
1	**REALIZAR MONITOREO A LA PLATAFORMA TECNOLÓGICA** Los administradores de servicio realizarán el monitoreo con lo descrito en el procedimiento **RT-Pr03 Procedimiento gestión y monitoreo de la plataforma tecnológica.** Los administradores de las herramientas de seguridad deben instalar las respectivas actualizaciones liberadas por el fabricante y monitorear que el licenciamiento esté vigente notificando mediante correo electrónico el estado del licenciamiento de manera mensual a la jefatura.	Administradores herramientas de seguridad	Reporte de monitoreo Correo electrónico estado de licencias
2	**REPORTAR CÓDIGO MALICIOSO** Las solicitudes pueden ser reportadas por el usuario final o por el administrador del servicio a través de los medios de contacto establecido para la Mesa de servicios, cuando se identifiquen problemas de virus, spam, phishing entre otros. **(Ver RT-Pr01-V03 PROCEDIMIENTO SOPORTE TÉCNICO Y ATENCIÓN DE SERVICIOS)**	Usuario, Administradores de Infraestructura	Registro en la herramienta de gestión

3	**ATENDER SOLICITUD DE DETECCIÓN DE CÓDIGO MALICIOSO** La mesa de servicios debe realizar el diagnóstico preliminar en caso de que el reporte de código malicioso sea a nivel de estación de trabajo, si el técnico de mesa de servicios brinda una solución satisfactoria se debe continuar a la **Actividad 5**. En caso contrario de debe escalar el servicio a un nivel superior **(Ver RT-Pr01-V03 PROCEDIMIENTO SOPORTE TÉCNICO Y ATENCIÓN DE SERVICIOS)** En caso de que exista una afectación de servicio o el nivel al cual fue escalado el servicio no puede realizar una solución definitiva, se debe solicitar un control de cambios si se requiere y se debe pasar **Actividad 4**, de lo contrario se debe informar a la jefatura mediante solicitud, para realizar un diagnóstico por parte de un tercero o especialista, pasar a la **Actividad 5.**	Personal Técnico de primer nivel de Mesa de Servicios Personal Técnico Especializado Segundo Nivel	Registro herramienta de gestión Solicitud a la jefatura
4	**SOLICITAR CONTROL DE CAMBIOS** El administrador del servicio afectado debe solicitar reunión del grupo control de cambios para poner en consideración el caso y generar una posible solución de restauración en caso de que sea aprobado el control de cambios ver (**RT-Pr02 V04 PROCEDIMIENTO GENERACIÓN DE COPIAS DE SEGURIDAD Y RESTAURACIÓN DE DATOS PARA AMBIENTES VIRTUALIZADOS)** de lo contrario se debe pasar nuevamente a la **actividad 3**. y realizar el respectivo seguimiento a la solicitud de diagnóstico por parte de un especialista externo Nota: la solicitud será remitida por la jefatura a la Dirección General	Administrador Herramienta de Gestión y Jefe de división	Solicitud reunión de control de cambios, Formato control de cambios, Correos de seguimiento y oficio remisorio

5	**CERRAR EL CASO** EL personal técnico de primer nivel de Mesa de Servicios o personal técnico especializado Segundo Nivel debe realizar la respectiva documentación, de igual forma tiene que solicitar la calificación del servicio y notificar al usuario que el caso ha sido cerrado.	Personal Técnico de primer nivel de Mesa de Servicios o Personal Técnico Especializado Segundo Nivel	Registro herramienta de gestión

7. PUNTOS DE CONTROL

N/A

8. BASE LEGAL

N/A

9. ANEXOS

N/A

10. FORMATOS

N/A

11. DOCUMENTOS RELACIONADOS

RT-Pr03 Procedimiento gestión y monitoreo de la plataforma tecnológica.

RT-Pr02 V04 PROCEDIMIENTO GENERACIÓN DE COPIAS DE SEGURIDAD Y RESTAURACIÓN DE DATOS PARA AMBIENTES VIRTUALIZADOS

RT-Pr01-V03 PROCEDIMIENTO SOPORTE TÉCNICO Y ATENCIÓN DE SERVICIOS

12. CONTROL DE CAMBIOS

Control de Cambios

- Ver. 001// Rev. 1// FV. 8 de julio de 2019

  Cambios:

  Creación del documento versión 001

  Justificación:

  Responsable: Andres Felipe Olarte Reales

  Fecha: 2019-07-24

ELABORÓ	REVISÓ	APROBÓ
Nombre: Guillermo Moreno	Nombre: Diana Plata Arango	Nombre: Grupo evaluador documento SGC
Cargo: Contratista DPS	Cargo: Jefe División de Planeación y Sistemas	No. Acta y Fecha: Acta No 183 Julio 4 de 2019

Por favor describa las actividades del documento aquí

Mary Alexandra Rodriguez Bernal @2019-07-24, 10:23:25