Ministerio de Hacienda Viceministerio de Monitoreo Instituciones Descentralizadas del Sistema Financiero	Dirección General del Catastro Nacional **Departamento de Tecnología de la Información y Comunicación**	*Cód. No.:* ***DGCN-POL-TIC-004*** *Versión 1.0-2017*
	Política **Utilización de antivirus en la Infraestructura Tecnológica**	20/07/2017 Página **1** de **7**

I. Objetivo:	Asegurar la operación libre de virus de la infraestructura tecnológica institucional.
II. Alcance:	Todas las áreas de la DGCN, que poseen acceso a la infraestructura tecnológica institucional. Toda la infraestructura tecnológica en la Dirección General de Catastro Nacional.
III. Responsables.	• Director (a) General. • Encargados. • Empleados.
IV. Definiciones:	• **COBIT** (Objetivos de Control para la Información y Tecnologías Relacionadas) Es un marco de gobierno de Tecnología de la Información (TI) que permite el desarrollo de políticas y buenas prácticas para el control de TI en todas las partes de la organización • **ISO** Organización internacional para la estandarización de normas relativas a productos y seguridad para las empresas u organizaciones a nivel internacional. • **Mensajes de datos** Información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, tales como el intercambio electrónico, el correo electrónico, telegrama, Télex o telefax • **Destinatario** Persona que recibirá el mensaje • **Remitente** Persona que envía el mensaje • **Intermediario** Persona que, en relación con un determinado mensaje de datos, actuando por cuenta de otra, envíe, reciba o archive dicho mensaje o preste algún otro servicio respecto de él • **Firma Digital** Valor numérico que se adhiere a un mensaje de datos, permitiendo determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y el texto del mensaje inicial no ha sido modificado después de efectuada la trasmisión • **Custodio de Recursos Tecnológicos** Son los encargados del recurso, su gestión y operación. • **Usuario Técnico** Es el empleado del área de tecnología que crea y modifica los sistemas • **Usuario Final** Es que hace uso de la tecnología como un servicio para sus actividades

	• **Servicios de TI** Conjunto de funciones de soporte y mantenimiento a cargo de personal técnico calificado • **Gestión de Servicios** TI Método ordenado y profesional seguido por un departamento de TI para proporcionar sistemas de información confiable, eficiente y cumplir con los requerimientos institucionales • **Incidente** Interrupción no planeada de un servicio de TI o la reducción de la calidad del servicio • **Levantamiento de un incidente** Documentar el requerimiento, problemas y cambios • **Gestión de Incidente** Restaurar los niveles normales del servicio lo más rápido posible • **Gestión de Problemas** Detecta, ofrece soluciones a los problemas • **Mesa de servicio de tecnología** Punto único de contacto para los usuarios que necesitan ayuda, proporcionando un servicio de soporte de alta calidad • **Datos** Información o representación simbólica, algorítmica, numérica que define las características u operaciones de una entidad; es un bien inmaterial que como activo es un bien con cierto valor y una vida útil • **Frecuencia** Periodicidad de una activad • **Respaldo** Copia de los datos de información en un medio magnético alterno, de tal modo que permita al sistema poder ser restaurado y recuperada la información • **Recuperación** Tarea que se realiza cuando es necesario volver al estado original, la aplicación al momento del último respaldo • **Respaldo simultáneo** Realiza una copia exactamente igual al mismo tiempo en que los datos son procesados • **Respaldo /global** Se respalda la totalidad de las bases de datos y la totalidad de las operaciones que se mantienen en línea • **Respaldo Parcial** Se respalda solo una parte de la información, es decir una aplicación, plataforma o datos críticos o las bases de datos nuevas • **Registro de Respaldos** Historia de los respaldos y las recuperaciones llevados a cabo, conteniendo las observaciones relevantes sobre la aplicación, debe contener la siguiente información: fecha, identificación del operador, identificación del juego de respaldo, hora de inicio, hora de termino, resultado y firma del operador

	• **Resultado** Se refiere a es cómo se finalizó la ejecución, debe informar si se realizó sin observaciones y correctamente o bien con anomalías y especificar cuales, por ejemplo, falla en el servicio eléctrico, cinta con error, entre otros. • **Bienes, servicios y accesorios** Se refieren a el abastecimiento y servicio de equipos de telecomunicaciones, servicios públicos (luz, agua, aseo urbano), capacitación especializada, servicios de imprenta simple, servicios de ayuda personal o personal de limpieza temporal, servicios de tasaciones independientes, servicios de mantenimiento y apoyo a programas de computación con licencia, compra de bienes y mercaderías, reparación y mantenimiento de activos fijos, servicios de agencias de viajes y transporte, servicios de banco corresponsal, servicios de alquiler de flota, conferencias externas • **Contratación Externa** Tiene lugar cuando una organización llega a un acuerdo con un proveedor externo de servicios a fines de que éste realice una actividad, función o proceso relacionado a las actividades propias del negocio. La institución considera de manera enunciativa, pero no limitativa, la Contratación externa a los siguientes servicios: procesamiento, mantenimiento o gestión de sistemas de datos; registros o información financiera; conservación y gestión de registros; administración de beneficios; gestión de garantías y cobro; gestión de servicios administrativos; operaciones de custodia; gestión de recursos humanos y respaldo técnico de segunda línea; servicios de representación jurídicos y asesoría legal; servicios de asesoría independiente. Las operaciones que representan la adquisición de bienes y servicios accesorios (suministros o abastecimientos) no son considerados contratación externa. En ese tenor, refiérase a la definición de "bienes y servicios accesorios" para una mayor aclaración. • **Archivo del Acuerdo de Contratación Externa** Es un archivo individual llevado por una unidad o departamento que contiene toda la información relacionada a un acuerdo de contratación externa en particular • **Consecuencias desfavorables** Incluyen, pero no se limitan a, pérdidas financieras serias, gastos importantes, litigios, sanciones o penalidades reglamentarias, daños a la reputación de la institución, pérdidas de

	riesgos operativos de mayor cuantía • **Comité de Compras** Se refiere al órgano que evalúa, compara y decide sobre las adquisiciones de bienes y servicios en vista de las diversas propuestas o cotizaciones presentadas por las áreas, de acuerdo a las disposiciones institucionales. • **Evaluación de la relevancia de un acuerdo de contratación** Se refiere tanto al proceso y al formulario que lo documenta, por medio del cual se determina si un acuerdo de contratación externa es relevante, no relevante o irrelevante • **Proveedor de Servicios** Es un tercero, ya sea una persona física o moral que cumple con los requisitos de aceptación establecidos, con quien la institución ha suscrito un contrato de servicios
V. Base Legal/Referencias:	• NOBACI • COBIT 5.1 • ISO-27001

VI. Políticas:

1. Los servidores, computadores (portátiles y de escritorios) deben tener un antivirus instalado que prevea y pueda detectar los virus. Esto debe ser antes de ponerlos en marcha para su utilización.

2. El software de antivirus debe estar administrado por la mesa de servicio de tecnología y tener colaboración con el resto del personal de TI para casos de limpieza masiva u otras actividades de gran alcance que se tengan que realizar.

3. El antivirus debe estar actualizado con las últimas versiones del suplidor.

4. Los usuarios no deben actualizar el antivirus de sus computadores. Este debe ser actualizado automáticamente desde el servidor o por un técnico de la mesa de servicio de tecnología.

5. La administración del antivirus debe tener una autenticación y protección interna para que solo el personal autorizado pueda acceder a la misma.

6. El antivirus debe estar en un servidor exclusivo para tales fines, el cual debe residir en un segmento de red seguro y en el cuarto de servidores.

7. Las descargas de software o de archivos adjuntos en correos electrónicos debe cumplir con la política de control del software y dichas descargadas deben ser en computadores o servidores autorizados con antivirus, filtrados por firewall, antispyware, actualizaciones de sistemas operativos realizadas, scanner de vulnerabilidades y cualquier otro software de seguridad que la DGCN tenga para proteger sus

sistemas.

8. El equipo que se vea afectado por un virus debe ser desconectado inmediatamente de la red y realizar el proceso de limpieza con la solución antivirus que tiene la DGCN. Si el virus ha infectado en gran porcentaje el equipo, se debe formatear su disco, reinstalar el sistema operativo, reinstalar su antivirus, el software correspondiente, aplicaciones correspondientes, realizar un scanner y habilitar nuevamente el equipo tomando las medidas preventivas según esta política.

9. Los servidores y computadores (portátiles y de escritorios) deben tener restringido el uso de zip, drives, cd-rw, dvd-rw, puertos usb, discos removibles, conexiones MP3 player, IPOD/MP3 player, PDA, cámaras portátiles, webcarn u otros dispositivos que puedan ser portadores de virus.

9.1. Las excepciones a este artículo, serán solicitadas por escrito por el supervisor de la persona que requiera el acceso y aprobadas por el Encargado de Tecnología o la Dirección General de la DGCN.

9.2. Todo acceso otorgado será monitoreado por un sistema de prevención de pérdidas de datos (DLP — por sus siglas en ingles).

10. La información que se reciba en la DGCN de fuentes externas o internas en correos electrónicos, archivos adjuntos u otras, debe ser filtrada por el antivirus antes de su utilización.

11. La información bajada desde el internet por usuarios autorizados y en servidores o computadores (portátiles o de escritorios) autorizados debe aplicársele el antivirus previo a su utilización.

12. Los usuarios deben reportar a Mesa de Servicios o la administración de sistemas de tecnología cualquier incidente de virus que puedan detectar en sus computadores o en la red.

13. El monitoreo del antivirus debe contemplar los correos electrónicos recibidos y enviados, los archivos adjuntos si aplica, los eventos generados, las estadísticas de posibles virus, las bitácoras de infecciones si aplica, tener filtros de información o correos no deseados y cualquier otra posible amenaza o evento que pueda ser detectada, que ha sucedido o que resulte riesgosa.

14. Semanalmente se deberá realizar una revisión ("scan" por su nombre en ingles) de toda la red para detectar cualquier virus proveniente de fuentes internas o externas y poder eliminarlos.

15. El antivirus debe estar centralizadamente en la red para facilitar la administración y el monitoreo de todos los eventos.

16. La DGCN se reserva el derecho de eliminar los archivos y correos electrónicos que se detecten que están infectados por virus.

17. Los usuarios no deben abrir mensajes por correo que no conozcan su origen sin antes consultar con el área de Mesa de Servicios, Tecnología o el administrador del correo electrónico, ya que estos pueden

estar infectados con virus.

18. Los archivos de usuarios deben ser grabados en el servidor de archivos.

19. Las cadenas de correos electrónicos no están permitidas en la DGCN, pues pueden ser portadoras de virus para la red. Todo correo público autorizado y que sea necesario distribuir masivamente debe ser filtrado por el antivirus antes de su envío.

20. Los usuarios deben colaborar en la detección de virus manteniéndose alerta e informando cualquier amenaza detectada.

21. El antivirus debe tener filtrados y no permitir su circulación por la red de los correos spam, correos que son enviados y recibidos reincidentemente por una misma dirección, los spyware, los adware u otros códigos maliciosos no deseados.

22. El administrador del antivirus debe estar actualizado de las noticias de virus u otras amenazas o vulnerabilidades que puedan surgir como productos de los virus.

23. El antivirus debe cumplir con la política de control de servidor, computadores (portátiles y de escritorios), software y cualquier otra política que sea aplicable.

24. El departamento de Planificación y Desarrollo debe realizar revisiones periódicas al cumplimiento de esta política de antivirus o control de virus.

25. Todos los empleados, deberán firmar anualmente una constancia de haber leído esta política y que son responsables de seguirla al pie de la letra.

VII. Documentos y Aplicaciones Informáticas:

- Toda la infraestructura informática de la DGCP.

VIII. Procedimientos Relacionados:

Elaborado por:

Sr. Felipe Aquiles Ciprian
Analista de Calidad
Planificación y Desarrollo

Revisado por:

Licda. Anny Reyes Ramírez
Encargada del Departamento de
Planificación y Desarrollo

DIRECCION GENERAL DEL CATASTRO NACIONAL
OPTO. PLANIFICACIÓN Y DESARROLLO
Santo Domingo, R.D.

Aprobado por:

Ing. Catalino Solís
Encargado de Programación

DIRECCION GENERAL DEL CATASTRO NACIONAL
OPTO. DE TECNOLOGÍA
Santo Domingo, R.D.

Aprobado por:

Ing. Teresina Pérez
Encargado del Área Administrativa
de Tecnología

DIRECCION GENERAL DEL CATASTRO NACIONAL
OPTO. DE TECNOLOGÍA
Santo Domingo, R.D.

CONTROL DE MODIFICACIÓN DEL PROCEDIMIENTO			
REVISION	**DESCRIPCION DEL CAMBIO**	**APROBACION DEL CAMBIO**	**FECHA**