Contenido

VERSIONES

Versión	Elaborado por	Revisado por	Aprobado por	Fecha	Motivo
1	JAKELINE SÁNCHEZ MERLY AMPARO TORRES BERNAL	LAURA MARCELA PERDOMO FONSECA	COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO	17/05/2022	Versión inicial

1. OBJETIVO

Proteger la información y los componentes de procesamiento de información frente a amenazas causadas por código malicioso.

2. ALCANCE

Lo indicado en este documento debe ser aplicado por todos los servidores públicos, contratistas y colaboradores de RTVC.

3. DEFINICIONES

- **Integridad:** propiedad de la información que pretende mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.
- **Disponibilidad:** propiedad de la información que pretende garantizar el acceso y uso de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
- **Confidencialidad:** propiedad de la información que pretende garantizar que esta sólo es accedida por personas o sistemas autorizados.
- **Activo de información**: se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo.
- **Control**: medidas que se implementan para modificar el riesgo.
- ***Malware*:** *software* que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información. Palabra que nace de la unión de los términos en inglés de *software* malintencionado: *malicious software*. Dentro de esta definición tiene cabida un amplio elenco de programas maliciosos: virus, gusanos, troyanos, *backdoors*, *spyware*, etc.[1]
- **Virus**: programa diseñado para que, al ejecutarse, se copie a sí mismo adjuntándose en aplicaciones existentes en el equipo. De esta manera, cuando se ejecuta una aplicación infectada, puede infectar otros archivos. Los efectos

[1] Glosario de términos de Ciberseguridad - INCIBE

que pueden provocar varían dependiendo de cada tipo de virus: mostrar un mensaje, sobrescribir archivos, borrar archivos, enviar información confidencial mediante correos electrónicos a terceros, etc.[2]

- **Gusano**: programa malicioso que genera copias de sí mismos y se propaga automáticamente en la red sin necesidad de intervención humana, replicándose e infectando a otros equipos informáticos.
- **Troyano**: un troyano oculta *software* malicioso dentro de un archivo que parece normal. La mayoría de los troyanos tienen como objetivo controlar el equipo de un usuario, robar datos e introducir más software malicioso en el equipo de la víctima. [3]
- ***Backdoor***: puerta trasera es cualquier punto débil de un programa o sistema mediante el cual una persona no autorizada puede acceder a un sistema. Se consideran puertas traseras a los programas que, una vez instalados en el equipo de la víctima, dan el control de éste de forma remota al atacante.
- ***Spyware***: *software* malicioso que recopila información de un equipo informático y la envía a una entidad remota sin el conocimiento o el consentimiento del propietario.
- **Antivirus:** programa informático específicamente diseñado para detectar, bloquear y eliminar código malicioso (virus, troyanos, gusanos, etc.), así como proteger los equipos de otros programas peligrosos conocidos genéricamente como *malware*. [4]
- **Vulnerabilidad:** fallos o deficiencias de un programa que pueden permitir que un usuario no legítimo acceda a la información o lleve a cabo operaciones no permitidas de manera remota. Los agujeros de seguridad pueden ser aprovechadas por atacantes mediante exploits, para acceder a los sistemas con fines maliciosos. [5]
- ***Exploit*:** secuencia de comandos utilizados para, aprovechándose de un fallo o vulnerabilidad en un sistema, provocar un comportamiento no deseado como acceso a un sistema de forma ilegitima, entre otros.

[2] Glosario de términos de Ciberseguridad - INCIBE
[3] Definición de Norton - https://co.norton.com/internetsecurity-malware-what-is-a-trojan.html
[4] Glosario de términos de Ciberseguridad - INCIBE
[5] Glosario de términos de Ciberseguridad - INCIBE

4. PROTECCIÓN CONTRA EL CÓDIGO MALICIOSO

El *software* y los recursos de tratamiento de información son vulnerables a la introducción de software malicioso como virus informáticos, gusanos y caballos de troya. Las vías de contagio por software malicioso son numerosas, destacando entre otras:

- Las descargas de archivos de todo tipo desde páginas Web
- Adjuntos en correos electrónicos
- La navegación por sitios webs de dudosa fiabilidad
- Sistemas operativos y aplicaciones desactualizadas

El daño que pueden causar a la entidad hace necesario el establecimiento de controles para prevenir, detectar y eliminar la ejecución de cualquier software malicioso en los sistemas.

RTVC enfoca esos controles hacia los siguientes aspectos:

4.1 Antivirus en equipos de Cómputo

- La Coordinación de T.I. es el área encargada de implementar las herramientas de antivirus que cubran activamente el 100% de las estaciones de trabajo y servidores, con las librerías y definiciones actualizadas en forma periódica.
- Para el correcto funcionamiento de la herramienta antivirus, se deberá realizar una adecuada configuración que permita, entre otros, establecer los siguientes controles:
  - ✓ Realizar análisis automáticos y periódicos para detectar software malicioso;
  - ✓ Realizar comprobaciones automáticas de los archivos que se descarguen;
  - ✓ Actualizar la base de datos de firmas de virus de manera automática con una periodicidad de búsqueda actualizaciones diaria, como mínimo.
- El o los administradores de la herramienta antivirus deben instalar las respectivas actualizaciones liberadas por el fabricante y monitorear que el licenciamiento esté vigente.
- Se debe mantener instalado y actualizado el *software* antivirus, en todas las estaciones de trabajo y servidores de la entidad.

- El o los administradores de la herramienta antivirus, deberán estar alertas a las notificaciones en la consola, para poder actuar oportunamente en caso de presentarse alguna infección por virus o comportamientos sospechosos.
- El o los administradores de la herramienta antivirus, deberán revisar mensualmente el reporte emitido para analizar posibles comportamientos sospechosos.
- El equipo de soporte junto con los administradores del directorio activo, deben activar políticas en las estaciones de trabajo para el uso de dispositivos removibles tales como discos duros externos o memorias USB, sean estos personales e institucionales, que incluyan el escaneo automático de estos dispositivos por parte del antivirus y la inhabilitación de *autorun* o autoejecución desde dispositivos de almacenamientos removibles.
- Para evitar infección por software malicioso a través de medios extraíbles o correo electrónico, los usuarios deben realizar la verificación respectiva de los archivos haciendo uso del antivirus instalado en sus equipos, cada vez que instalen o conecten un dispositivo, reciban archivos por correo electrónico o descarguen algún archivo desde sitios Web.
- Los usuarios que sospechen o detecten alguna infección por *software* malicioso deben notificar inmediatamente a la Coordinación de T.I., a través de la mesa de servicios (HelpDesk) https://helpcenter.rtvc.gov.co/mesadeservicio/Index.aspx, con el fin de que se tomen las medidas pertinentes.
- En caso de materializarse la infección por virus en un equipo de cómputo, se deben seguir los siguientes pasos:
  - ✓ Desconectar de manera inmediata el equipo de la red;
  - ✓ No ejecutar ninguna aplicación;
  - ✓ El equipo de soporte de T.I. debe realizar un análisis exhaustivo y realizar los correctivos para eliminar el virus y documentar el incidente.

4.2 Antivirus para el Correo electrónico

- La solución de correo electrónico de la entidad provee los mecanismos para análisis de virus en los correos electrónicos que ingresan a los buzones de los usuarios, así mismo, cuenta con una herramienta antispam que permite el bloqueo de remitentes identificados como sospechosos por parte del administrador de la plataforma.
- Cuando un usuario reciba un correo sospechoso por el nombre, la extensión de los archivos adjuntos, el remitente u otras características extrañas, se

recomienda no hacer la apertura o descarga de los archivos adjuntos y mucho menos la ejecución de estos y solicitar la revisión inmediata por parte del equipo de soporte técnico o seguridad de la información de RTVC.

- El uso del correo electrónico en la entidad debe regirse por los lineamientos de "**Uso aceptable de los activos de información**" establecidos en la Política operacional de Seguridad de la información y Seguridad digital.
- El o los administradores de la plataforma de correo, deberán estar alertas a las notificaciones generadas por la solución, con el fin de actuar oportunamente en caso de presentarse algún comportamiento sospechoso.

4.3 Filtrado Web

- Desde la solución de protección perimetral, firewall de la entidad, se provee el análisis de los sitios web visitados desde la red interna con el fin de detectar y evitar el uso de sitios web desconocidos o que se sospecha son maliciosos.
- El colaborador o contratista encargado del apoyo a monitoreo y control de la infraestructura tecnológica deberá estar alerta a las notificaciones generadas por el SOC (*Security Operation Center*), con el fin de actuar oportunamente en caso de presentarse algún comportamiento sospechoso.
- El uso del servicio de acceso a internet desde la entidad debe regirse por los lineamientos de "Uso aceptable de los activos de información" establecidos en la Política operacional de Seguridad de la información y Seguridad digital.

4.4 Actualizaciones de sistema operativo y parches de seguridad

- Se deben mantener permanentemente actualizados todos los sistemas, aplicaciones y equipos de la infraestructura tecnológica de la entidad a sus últimas versiones y con todos los parches de seguridad instalados.
- La distribución de actualizaciones y parches de seguridad para el sistema operativo de las estaciones de trabajo de los usuarios se realizará de manera automática a través de una herramienta centralizada.
- Las actualizaciones de sistemas operativos y parches de seguridad en los equipos servidores, aplicaciones y dispositivos son responsabilidad de los administradores de tecnología, quienes se comprometerán a realizarlos de manera oportuna.

4.5 Uso e instalación de programas de software

- Todos los equipos de cómputo administrados por la Coordinación de T.I., deben tener habilitado la solicitud de clave de administrador cuando se intente realizar la instalación de un programa.
- Las credenciales de acceso para la instalación de programas deben ser cambiadas periódicamente, no deben ser conocidas por los usuarios estándar de la entidad y deben ajustarse a lo establecido en la Política para la administración de la infraestructura de T.I.
- Se utilizarán únicamente los programas de *software* autorizados por la Coordinación de T.I., los cuales deben mantenerse actualizados, con licencia vigente y serán instalados únicamente por el equipo de soporte de la Coordinación de T.I.

4.6 Concientización

En el contexto de la seguridad de la información y seguridad digital, el recurso humano es el eslabón más importante en la cadena, por ende, la falta de capacitación y concientización en esta materia constituye un alto riesgo para las organizaciones, por ello RTVC, desde la Coordinación de T.I. y la Coordinación de Gestión de Talento humano desarrollan un plan para fortalecer las capacidades en seguridad de la información de todos los colaboradores de la entidad, incluyendo actividades como campañas de sensibilización, charlas, capacitaciones, entre otros.

4.7 Gestión de vulnerabilidades

- Se realizarán análisis periódicos de los sistemas y dispositivos que hacen parte de la infraestructura tecnológica de la entidad con el fin de identificar debilidades de software o configuraciones.
- Los colaboradores y/o contratistas encargados de la administración de tecnología deberán ejecutar las tareas requeridas para la remediación de las vulnerabilidades técnicas identificadas.
- Desde el equipo de seguridad se hará seguimiento a la remediación de las vulnerabilidades.

5. NORMATIVIDAD ASOCIADA

Norma ISO 27001:2013