Aviso en materia de amenaza cibernética de la República Popular Democrática de Corea

Emitido: **15 de abril de 2020**

Título: **Pautas sobre la amenaza cibernética de Corea del Norte**

Los Departamentos de Estado, del Tesoro y de Seguridad Nacional de los Estados Unidos, así como el Dirección Federal de Investigaciones (FBI), emiten el presente aviso como recurso integral sobre la amenaza cibernética que representa Corea del Norte para la comunidad internacional, los defensores de la red y el público en general. En el aviso se destaca la amenaza cibernética que representa Corea del Norte —formalmente conocida como la República Popular Democrática de Corea (RPDC)— y se recomiendan pasos para atenuar la amenaza. En particular, en el Anexo 1 se enumeran los recursos del Gobierno de los Estados Unidos relacionados con las amenazas cibernéticas de la RPDC y en el Anexo 2 se incluye un enlace a los informes del Grupo de Expertos del Comité del Consejo de Seguridad de las Naciones Unidas establecido en virtud de la resolución 1718.

Las actividades cibernéticas malintencionadas emprendidas por la RPDC constituyen una amenaza para los Estados Unidos y la comunidad internacional en general y, en particular, ponen seriamente en peligro la integridad y la estabilidad del sistema financiero internacional. Ante la presión de las enérgicas sanciones impuestas por los Estados Unidos y las Naciones Unidas, la RPDC depende cada vez más de actividades ilícitas —entre ellas la delincuencia informática— para generar ingresos con el fin de financiar sus armas de destrucción masiva y sus programas de misiles balísticos. En particular, los Estados Unidos están sumamente preocupados por las actividades cibernéticas malintencionadas de Corea del Norte, a las que el Gobierno de los Estados Unidos se refiere como HIDDEN COBRA (cobra oculta). La RPDC tiene la capacidad de realizar actividades cibernéticas perjudiciales o destructivas que afectan a la infraestructura crítica de los Estados Unidos. La RPDC también se sirve de capacidades cibernéticas para robar a instituciones financieras y ha demostrado un patrón de actividades cibernéticas perjudiciales y nocivas que es totalmente incompatible con el creciente consenso internacional sobre lo que constituye un comportamiento responsable de los Estados en el ciberespacio.

Los Estados Unidos trabajan estrechamente con países que tienen ideas afines para centrar la atención en el comportamiento perjudicial, destructivo o desestabilizador de la RPDC en el ciberespacio y condenarlo. Por ejemplo, en diciembre de 2017 Australia, Canadá, Nueva Zelandia, los Estados Unidos y el Reino Unido atribuyeron públicamente a la RPDC el ataque del programa secuestrador WannaCry 2.0 y denunciaron las actividades cibernéticas nocivas e

irresponsables emprendidas por ese país. Dinamarca y el Japón emitieron declaraciones de apoyo a la denuncia conjunta respecto al ataque destructivo del programa secuestrador WannaCry 2.0 que en mayo de 2017 afectó a cientos de miles de computadoras en todo el mundo.

Es fundamental que la comunidad internacional, los defensores de la red y el público en general permanezcan alerta y colaboren para atenuar la amenaza cibernética planteada por Corea del Norte.

Actividades cibernéticas malintencionadas de la RPDC dirigidas al sector financiero

Muchos agentes cibernéticos de la RPDC están subordinados a entidades designadas por las Naciones Unidas y los Estados Unidos, como la Oficina General de Reconocimiento. Los agentes cibernéticos patrocinados por el Estado de la RPDC son principalmente piratas informáticos, codificadores y desarrolladores de programas informáticos que realizan actividades de espionaje, robos por medios informáticos dirigidos a instituciones financieras y a plataformas de cambio de cibermonedas, y operaciones que responden a motivos políticos contra empresas extranjeras de medios de comunicación. Esos agentes crean y despliegan en todo el mundo una gran variedad de herramientas malignas para facilitar esas actividades y se han vuelto cada vez más sofisticados. Entre las tácticas comunes que utilizan los agentes cibernéticos patrocinados por el Estado de la RPDC para aumentar sus ingresos de manera ilícita se encuentran las siguientes:

Robo de instituciones financieras por medios informáticos y lavado de dinero. En el informe de mitad de período de 2019 elaborado por el Grupo de Expertos del Comité del Consejo de Seguridad de las Naciones Unidas establecido en virtud de la resolución 1718 (el Informe de mitad de período de 2019) se indica que, a pesar de las sanciones impuestas por el Consejo de Seguridad de las Naciones Unidas, la RPDC tiene cada vez más capacidad para generar ingresos mediante actividades cibernéticas malintencionadas tendientes a robar a instituciones financieras por medio de herramientas y tácticas cada vez más sofisticadas. En el Informe de mitad de período de 2019 también se señala que, en algunos casos, esas actividades cibernéticas malintencionadas también se extendieron al lavado de fondos a través de múltiples jurisdicciones. En dicho informe se menciona que se están investigando decenas de supuestos robos por medios informáticos perpetrados por la RPDC y que, hasta fines de 2019, ese país había intentado robar hasta US $2.000 millones por medio de esas actividades cibernéticas ilícitas. Las acusaciones formuladas en una denuncia por confiscación presentada por el Departamento de Justicia en marzo de 2020 son congruentes con secciones de las conclusiones del Informe de mitad de período de 2019. Concretamente, en la denuncia por confiscación se indicaba la manera en que los agentes cibernéticos de Corea del Norte utilizaban la infraestructura de ese país con miras a promover su conspiración para piratear plataformas de cambio de cibermonedas, robar cientos de millones de dólares en monedas digitales y lavar fondos.

Campañas de extorsión. Los agentes cibernéticos de la RPDC también han realizado campañas de extorsión contra entidades de terceros países poniendo en peligro la red de la institución y amenazando con desactivarla si la entidad no paga un rescate. En algunos casos, los agentes cibernéticos de la RPDC exigieron a las víctimas pagos en forma de acuerdos de consultorías

remuneradas a largo plazo, para garantizar que no sufrieran actividades cibernéticas malintencionadas en el futuro. También se ha pagado a los agentes cibernéticos de la RPDC para que pirateen sitios web y extorsionen a objetivos para terceros clientes.

Criptosecuestro. En el Informe de mitad de período de 2019 se señala que el Grupo de Expertos también está investigando la utilización del "criptosecuestro" por parte de la RPDC. Se trata de un mecanismo para poner en peligro la máquina de una víctima y robar sus recursos informáticos para extraer monedas digitales. El Grupo de Expertos detectó varios incidentes en los que las computadoras infectadas con el programa maligno de criptosecuestro enviaban los activos extraídos —en su mayoría monedas digitales con más anonimato (a veces también conocidas como "moneda de privacidad")— a servidores ubicados en la RPDC, incluida la Universidad Kim Il Sung de Pyongyang.

Esas actividades ponen de manifiesto el uso por parte de la RPDC de medios cibernéticos para generar ingresos, al tiempo que atenúan los efectos de las sanciones y muestran que cualquier país puede estar expuesto a la RPDC y ser explotado por ella. Según el Informe de mitad de período de 2019, el Grupo de Expertos también está investigando actividades como intentos de violación de las sanciones impuestas por el Consejo de Seguridad de las Naciones Unidas a la RPDC.

Operaciones cibernéticas atribuidas públicamente por el Gobierno de los Estados Unidos a la RPDC

En reiteradas ocasiones la RPDC ha atacado redes de los Estados Unidos y otras redes gubernamentales y militares, así como algunas relacionadas con entidades privadas e infraestructura crítica, para robar datos y llevar a cabo actividades cibernéticas perjudiciales y destructivas. Hasta la fecha, el Gobierno de los Estados Unidos ha atribuido públicamente los siguientes incidentes cibernéticos a agentes cibernéticos y otros conspiradores patrocinados por el Estado de la RPDC:

- ***Sony Pictures***. En noviembre de 2014, agentes cibernéticos patrocinados por el Estado de la RPDC presuntamente lanzaron un ataque cibernético contra Sony Pictures Entertainment en represalia por la película de 2014 "Una loca entrevista". Los agentes cibernéticos de la RPDC piratearon la red de Sony Pictures Entertainment para robar datos confidenciales, amenazaron a ejecutivos y empleados de la empresa y dañaron miles de computadoras.

    - Actualización del FBI sobre la investigación en Sony (19 de diciembre de 2014) https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation
    - Denuncia penal del Departamento de Justicia contra un programador respaldado por el régimen de Corea del Norte (6 de septiembre de 2018) https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

- ***Robo del Banco de Bangladesh.*** En febrero de 2016 agentes cibernéticos patrocinados por el Estado de la RPDC presuntamente intentaron robar al menos US

$1.000 millones de instituciones financieras de todo el mundo y supuestamente robaron US $81 millones del Banco de Bangladesh mediante operaciones no autorizadas en la red Sociedad para las Telecomunicaciones Financieras Interbancarias Internacionales (SWIFT). Según lo indicado en la denuncia, agentes cibernéticos de la RPDC accedieron a las terminales informáticas del Banco de Bangladesh que interactuaban con la red SWIFT tras poner en peligro la red informática del Banco por medio de correos electrónicos de *phishing* personalizado dirigidos a empleados del banco. Posteriormente los agentes cibernéticos de la RPDC enviaron mensajes SWIFT autenticados de manera fraudulenta en los que ordenaban al Banco de la Reserva Federal en Nueva York transferir fondos de la cuenta de la Reserva Federal del Banco de Bangladesh a cuentas controladas por los conspiradores.

  - Denuncia penal del Departamento de Justicia contra un programador respaldado por el régimen de Corea del Norte (6 de septiembre de 2018) https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

- ***WannaCry 2.0***. Los agentes cibernéticos patrocinados por el Estado de la RPDC desarrollaron el programa secuestrador conocido como WannaCry 2.0, así como dos versiones anteriores de dicho programa. En mayo de 2017, el programa secuestrador WannaCry 2.0 infectó a cientos de miles de computadoras en hospitales, escuelas, empresas y hogares de más de 150 países. Ese programa encripta los datos de una computadora infectada y permite a los agentes cibernéticos exigir pagos por concepto de rescate en la moneda digital Bitcoin. El Departamento del Tesoro nombró a un programador informático de Corea del Norte por su participación en la conspiración de WannaCry 2.0, así como su papel en el ataque cibernético de Sony Pictures y el robo del Banco de Bangladesh, y designó, además, la organización para la que trabajaba.

  - Alerta técnica de CISA (Agencia de Ciberseguridad y Seguridad de la Infraestructura): Indicadores relacionados con el programa secuestrador WannaCry (12 de mayo de 2017) https://www.us-cert.gov/ncas/alerts/TA17-132A
  - Conferencia de prensa de la Casa Blanca relativa a la atribución del programa secuestrador WannaCry (19 de diciembre de 2017) https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/
  - Denuncia penal del Departamento de Justicia contra un programador respaldado por el régimen de Corea del Norte (6 de septiembre de 2018) https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and
  - El Departamento del Tesoro señala a Corea del Norte como autora de múltiples ataques cibernéticos (6 de septiembre de 2018) https://home.treasury.gov/news/press-releases/sm473

- ***Campaña FASTCash.*** Desde fines de 2016, agentes cibernéticos patrocinados por el Estado de la RPDC han empleado un mecanismo fraudulento de retiro de dinero en efectivo de cajeros automáticos conocido como "FASTCash", con el fin de robar decenas de millones de dólares de cajeros automáticos en Asia y África. Los mecanismos FASTCash intervienen a distancia en los servidores de aplicaciones de cambio de pagos en bancos para facilitar operaciones fraudulentas. En un incidente ocurrido en 2017, agentes cibernéticos de la RPDC posibilitaron el retiro simultáneo de dinero en efectivo de cajeros automáticos ubicados en más de 30 países diferentes. En otro incidente ocurrido en 2018, agentes cibernéticos de la RPDC posibilitaron el retiro simultáneo de dinero en efectivo de cajeros automáticos situados en 23 países diferentes.

    - Alerta de CISA sobre la campaña FASTCash (2 de octubre de 2018) https://www.us-cert.gov/ncas/alerts/TA18-275A
    - Informe de análisis de CISA sobre un programa maligno: Programa maligno relacionado con FASTCash (2 de octubre de 2018) https://www.us-cert.gov/ncas/analysis-reports/AR18-275A

- ***Pirateo de plataformas de cambio de cibermonedas.*** Conforme se detalla en las acusaciones expuestas en la denuncia por confiscación real presentada por el Departamento de Justicia en abril de 2018, agentes cibernéticos patrocinados por el Estado de la RPDC accedieron a una plataforma de cambio de cibermonedas y robaron monedas digitales por un valor de casi US $250 millones. En la denuncia se describe además cómo se lavaron los activos robados por medio de cientos de operaciones automatizadas de monedas digitales con el fin de ofuscar los orígenes de los fondos, en un intento por evitar que las fuerzas del orden rastreasen los activos. Posteriormente, según se indica en la denuncia, dos ciudadanos chinos presuntamente lavaron los activos en nombre del grupo norcoreano y recibieron aproximadamente US $91 millones provenientes de cuentas controladas por la RPDC, así como un monto adicional de US $9,5 millones proveniente del pirateo de otra plataforma de cambio. En marzo de 2020, el Departamento del Tesoro designó a esas dos personas en virtud de las normas sobre sanciones a la RPDC y cibernéticas, junto con un anuncio del Departamento de Justicia en el que se indicaba que las personas habían sido acusadas previamente de lavado de dinero y de transmisión de dinero sin licencia, y que 113 cuentas de moneda digital eran susceptibles de confiscación.

    - Sanciones del Tesoro contra las personas que efectuaron actividades de lavado de cibermonedas para el Grupo Lazarus (2 de marzo de 2020) https://home.treasury.gov/news/press-releases/sm924
    - Acusación formal del Departamento de Justicia contra dos ciudadanos chinos acusados de lavado de cibermonedas extraídas del pirateo de una plataforma de cambio y denuncia civil por confiscación (2 de marzo de 2020) https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack

Medidas para combatir la amenaza cibernética de la RPDC

Corea del Norte ataca la infraestructura informática de todo el mundo para generar ingresos on el fin de financiar las prioridades de su régimen, entre ellas los programas de armas de destrucción masiva. Exhortamos enérgicamente a los gobiernos, la industria, la sociedad civil y las personas en general a adoptar todas las medidas pertinentes que se describen a continuación para protegerse de la amenaza cibernética planteada por la RPDC y combatirla.

- **Sensibilizar sobre la amenaza cibernética que representa la RPDC.** Hacer hincapié en la gravedad, el alcance y la diversidad de las actividades cibernéticas realizadas por la RPDC contribuirá a sensibilizar en general a los sectores público y privado sobre la amenaza y promoverá la adopción y la aplicación de medidas cautelares y de mitigación de riesgos adecuadas.

- **Compartir información técnica sobre la amenaza cibernética de la RPDC.** El intercambio de información a nivel nacional e internacional para detectar las amenazas cibernéticas de la RPDC y defenderse de ellas permitirá mejorar la seguridad cibernética de las redes y los sistemas. Es preciso compartir las prácticas óptimas con los gobiernos y el sector privado. En virtud de las disposiciones de la Ley de intercambio de información sobre ciberseguridad de 2015 (secciones 1501 a 1510 del Título 6 del USC), las entidades no federales pueden compartir con entidades federales y no federales indicadores de seguridad cibernética y medidas defensivas relacionadas con el tema HIDDEN COBRA.

- **Poner en práctica y promover prácticas óptimas de seguridad cibernética.** La adopción de medidas —tanto técnicas como de comportamiento— para perfeccionar la seguridad cibernética mejorará la seguridad y la resiliencia de la infraestructura cibernética de los Estados Unidos y del resto del mundo. Las instituciones financieras, incluidas las empresas de servicios de dinero, deberían adoptar medidas independientes para protegerse contra las actividades cibernéticas malintencionadas de la RPDC. Entre ellas, compartir información sobre amenazas por intermedio del gobierno o la industria, segmentar las redes para minimizar los riesgos, realizar periódicamente copias de seguridad de los datos, efectuar capacitaciones de sensibilización sobre tácticas comunes de la ingeniería social, poner en práctica políticas que rijan el intercambio de información y el acceso a las redes y elaborar planes de respuesta a incidentes cibernéticos. El Modelo de Madurez de Capacidad de la Seguridad Cibernética del Departamento de Energía y el Marco de seguridad cibernética del Instituto Nacional de Normas y Tecnología proporcionan pautas sobre el desarrollo y la aplicación de prácticas sólidas de seguridad cibernética. Como se muestra en el Anexo I, la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA) suministra amplios recursos, incluidas alertas técnicas e informes de análisis de programas malignos, que permiten a los defensores de redes detectar actividades cibernéticas malintencionadas y reducir la exposición a ellas.

- **Notificar a las fuerzas del orden.** Si una organización sospecha que ha sido víctima de una actividad cibernética malintencionada, proveniente o no de la RPDC, es

fundamental que notifique a las fuerzas del orden sin dilación. Esto puede no solamente acelerar la investigación, sino también incrementar las posibilidades de recuperar los activos robados, en el caso de un delito financiero.

Las fuerzas del orden de los Estados Unidos han confiscado millones de dólares en monedas digitales robadas por agentes cibernéticos de Corea del Norte. Se alienta a las instituciones financieras de toda índole, incluidas las empresas de servicios de dinero, a cooperar en primera instancia respondiendo a las solicitudes de información de las fuerzas del orden de los Estados Unidos sobre esas amenazas cibernéticas, y posteriormente identificando activos confiscables cuando reciben una solicitud de las fuerzas del orden o una orden judicial de los Estados Unidos, y colaborando con las fuerzas del orden de ese país para respaldar la confiscación de esos activos.

- **Reforzar la observancia de las normas de lucha contra el lavado de dinero, la financiación del terrorismo y la financiación de la proliferación.** Los países deberían aplicar con eficacia y celeridad las normas del Grupo de Acción Financiera Internacional (GAFI) en materia de lucha contra el lavado de dinero, la financiación del terrorismo y la financiación de la proliferación. Ello implica velar por que las instituciones financieras y otras entidades incluidas en ese ámbito apliquen medidas de mitigación de riesgos en consonancia con las normas del GAFI y sus declaraciones y orientaciones públicas. Concretamente, el GAFI instó a todos los países a aplicar contramedidas para proteger el sistema financiero internacional contra los continuos riesgos de lavado de dinero, financiación del terrorismo y financiación de la proliferación provenientes de la RPDC[1]. Ello implica aconsejar a las instituciones financieras y otras entidades incluidas en ese ámbito que presten especial atención a las relaciones y operaciones comerciales con la RPDC, incluidas las empresas, las instituciones financieras y entidades que actúan en su nombre de ese país. De acuerdo con el párrafo 33 de la parte dispositiva de la resolución 2270 del Consejo de Seguridad de las Naciones Unidas, los Estados Miembros deberían cerrar las sucursales, filiales y oficinas de representación existentes de los bancos de la RPDC en sus territorios y poner fin a las relaciones de corresponsalía bancaria con los bancos de ese país.

  Además, en junio de 2019 el GAFI enmendó sus normas para exigir a todos los países que reglamenten y supervisen a los proveedores de servicios de activos digitales, incluidas las plataformas de cambio de cibermonedas, y mitiguen los riesgos al momento de realizar operaciones de monedas digitales. Los proveedores de servicios de activos digitales deberían permanecer atentos a los cambios en las actividades de sus clientes, dado que sus empresas pueden utilizarse para facilitar el lavado de dinero, la financiación del terrorismo y la financiación de la proliferación. Los Estados Unidos están particularmente preocupados por las plataformas que permiten el funcionamiento de servicios de cuentas y pagos anónimos sin hacer un seguimiento

[1] *El documento completo del llamado a la acción del GAFI sobre Corea del Norte puede consultarse en:* https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/call-for-action-february-2020.html.

a las operaciones, notificar las actividades sospechosas y hacer un examen de debida diligencia de los clientes, entre otras obligaciones.

Las instituciones financieras de los Estados Unidos, incluidos los proveedores de servicios de activos digitales ubicados en el exterior que hacen negocios en todos los Estados Unidos o en parte del país, así como otras empresas y personas incluidas en ese ámbito, deberían garantizar la observancia de sus obligaciones normativas en virtud de la Ley de Secreto Bancario (puesta en práctica mediante las reglamentaciones de la Red contra los delitos financieros (FinCEN) del Departamento del Tesoro establecidas en el Capítulo X del Título 31 del CFR). En lo que respecta a las instituciones financieras, esas obligaciones comprenden el desarrollo y mantenimiento de programas eficaces de lucha contra el lavado de dinero que estén diseñados razonablemente para evitar que las empresas que prestan servicios de dinero se utilicen para propiciar actividades de lavado de dinero y de financiación del terrorismo, y para detectar y notificar operaciones sospechosas, incluidas las realizadas, afectadas o facilitadas por acontecimientos cibernéticos o financiación ilícita que implican activos digitales, en el marco de la notificación de actividades sospechosas a la FinCEN.

Cooperación internacional. Para contrarrestar las actividades cibernéticas malintencionadas de la RPDC, los Estados Unidos mantienen contacto periódico con otros países para sensibilizar sobre las amenazas cibernéticas de la RPDC e intercambiar información y pruebas por la vía diplomática, militar, policial y judicial, la defensa de la red y otros conductos. Para obstaculizar las iniciativas de la RPDC tendientes a robar fondos a través de medios cibernéticos y para defenderse de las actividades cibernéticas malintencionadas de ese país, los Estados Unidos exhortan firmemente a los países a fortalecer la defensa de la red, cerrar los emprendimientos conjuntos con la RPDC en terceros países y deportar a los trabajadores norcoreanos del sector de las tecnologías de la información que residen fuera de Corea del Norte, de conformidad con la legislación internacional vigente. En una resolución del Consejo de Seguridad de las Naciones Unidas de 2017 se exigió a todos los Estados Miembros que repatriaran a los ciudadanos de la RPDC que generaban ingresos en el extranjero, incluidos los trabajadores del sector de las tecnologías de la información, antes del 22 de diciembre de 2019. Los Estados Unidos también procuran mejorar la capacidad de los gobiernos extranjeros y del sector privado para comprender las amenazas cibernéticas de la RPDC, identificarlas, defenderse contra ellas, investigarlas, responder a ellas y enjuiciar a los responsables, y para participar en las iniciativas internacionales tendientes a garantizar la estabilidad del ciberespacio.

Consecuencias de adoptar un comportamiento prohibido o sancionable

Las personas y las entidades que participen en actividades cibernéticas de la RPDC o las respalden, incluida la tramitación de operaciones financieras conexas, deberían tener conocimiento de las posibles consecuencias de adoptar un comportamiento prohibido o sancionable.

La Oficina de Control de Activos Extranjeros (OFAC) del Departamento del Tesoro tiene la facultad de imponer sanciones a cualquier persona que, según se determine, haya intervenido, entre otras:

- en actividades importantes que perjudiquen la seguridad cibernética en nombre del Gobierno de Corea del Norte o del Partido de los Trabajadores de ese país;
- en operaciones del sector de las tecnologías de la información en Corea del Norte;
- en otras actividades cibernéticas malintencionadas; o
- en al menos una actividad importante de importación a Corea del Norte o de exportación de ese país de bienes, servicios o tecnología.

Además, si el Secretario del Tesoro, en consulta con el Secretario de Estado, determina que una institución financiera extranjera ha efectuado o facilitado con conocimiento de causa operaciones comerciales importantes con Corea del Norte, o ha realizado o propiciado a sabiendas una operación importante en nombre de una persona designada en el marco de una Orden Ejecutiva relacionada con Corea del Norte, o de la Orden Ejecutiva 13382 (contra agentes que facilitan la proliferación de las armas de destrucción masiva y quienes apoyan esa actividad) para una actividad relacionada con Corea del Norte, esa institución financiera podrá, entre otras posibles restricciones, perder su capacidad de mantener una cuenta para pagos o de corresponsalía en los Estados Unidos.

La OFAC investiga presuntas violaciones a sus reglamentos de sanciones y ejerce autoridad de ejecución, conforme se establece en las Directrices para la Aplicación de las Sanciones Económicas que figuran en la parte 501 del Apéndice A del Título 31 del CFR. Las personas que infrinjan los reglamentos de sanciones relativas a Corea del Norte (parte 510 del Título 31 del CFR) son susceptibles de recibir sanciones pecuniarias civiles que pueden alcanzar el tope de la pena legal máxima vigente o duplicar el valor de la operación en cuestión.

En el Informe de mitad de período de 2019 se señala que el uso y la tentativa de uso de medios cibernéticos por parte de la RPDC para robar fondos de bancos y plataformas de cambio de cibermonedas podría violar múltiples resoluciones del Consejo de Seguridad de las Naciones Unidas (por ejemplo, el párrafo 8 d) de la parte dispositiva de la resolución 1718; los párrafos 8 y 11 de la parte dispositiva de la resolución 2094; y el párrafo 32 de la parte dispositiva de la resolución 2270). Las resoluciones del Consejo de Seguridad de las Naciones Unidas relacionadas con la RPDC también proporcionan diversos mecanismos para promover la observancia de las sanciones impuestas por las Naciones Unidas con relación a la RPDC. Por ejemplo, en virtud de la resolución 1718 del Comité del Consejo de Seguridad de las Naciones Unidas se pueden imponer sanciones específicas (por ejemplo, el congelamiento de activos y, para las personas físicas, la prohibición de viajar) a cualquier persona o entidad que participe en una operación comercial con entidades designadas por las Naciones Unidas o que evada las sanciones.

El Departamento de Justicia procesa penalmente a quienes infringen deliberadamente las leyes de sanciones vigentes, como la Ley de Poderes Económicos de Emergencia Internacional (secciones 1701 y siguientes del Título 50 del USC). Las personas que infringen deliberadamente esas leyes pueden recibir condenas de hasta 20 años de prisión, multas de hasta US $1 millón o

el doble de la ganancia bruta, lo que sea más elevado, y la confiscación de todos los fondos involucrados en esas operaciones. El Departamento de Justicia también procesa penalmente a quienes infringen deliberadamente la Ley de Secreto Bancario (secciones 5318 y 5322 del Título 31 del USC), que exige, entre otras cosas, que las instituciones financieras lleven adelante programas eficaces de lucha contra el lavado de dinero y presenten determinados informes a la FinCEN. Las personas que infringen esa ley pueden recibir condenas de hasta cinco años de prisión, una multa de hasta US $250.000 y la posible confiscación de los bienes involucrados en las infracciones. Cuando proceda, el Departamento de Justicia también procesará penalmente a las sociedades y otras entidades que violen esas leyes. El Departamento de Justicia también trabaja con asociados extranjeros para compartir pruebas que respaldan las investigaciones y los enjuiciamientos penales de ambas partes.

De conformidad con la sección 5318 k) del Título 31 del USC, el Secretario del Tesoro o el Fiscal General puede citar a una institución financiera extranjera que tenga una cuenta bancaria de corresponsalía en los Estados Unidos para obtener los registros archivados en el extranjero. Cuando el Secretario del Tesoro o el Fiscal General notifica por escrito a una institución financiera de los Estados Unidos que una entidad homóloga en el extranjero no compareció tras la citación, la institución financiera de los Estados Unidos debe terminar la relación de corresponsalía bancaria dentro de los 10 días siguientes a la notificación. El incumplimiento de esta obligación puede exponer a la institución financiera en los Estados Unidos a sanciones civiles diarias.

Recompensas por la justicia en casos relacionados con la RPDC

Si usted dispone de información sobre actividades ilícitas de la RPDC en el ciberespacio, incluidas operaciones pasadas o en curso, proporcionar esa información a través del programa de Recompensas por la Justicia del Departamento de Estado podría darle derecho a recibir una recompensa de hasta US $5 millones. Para obtener más detalles al respecto, visite el sitio web www.rewardsforjustice.net.

ANEXO I: Información pública del Gobierno de los Estados Unidos sobre amenazas cibernéticas de la RPDC y recursos para luchar contra ellas

Evaluaciones anuales de la amenaza mundial por la comunidad de inteligencia de los Estados Unidos, Oficina del director de Inteligencia Nacional. En 2019, la comunidad de inteligencia de los Estados Unidos determinó por medio de una evaluación que la RPDC presenta una amenaza cibernética importante para las instituciones financieras, sigue representando una amenaza de espionaje cibernético y mantiene la capacidad de perpetrar ataques cibernéticos perjudiciales. La RPDC continúa utilizando capacidades cibernéticas para robar a instituciones financieras y generar ingresos. Entre las operaciones de delitos cibernéticos de Pyongyang se encuentran tentativas de robo de más de US $1.000 millones a instituciones financieras de todo el mundo, incluido un exitoso robo al Banco de Bangladesh estimado en US $81 millones). El informe al respecto puede consultarse en https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

Informes técnicos de la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA). El Gobierno de los Estados Unidos se refiere a las actividades cibernéticas malintencionadas realizadas por la RPDC como HIDDEN COBRA (cobra oculta). En los informes sobre HIDDEN COBRA se proporcionan detalles técnicos sobre las herramientas y la infraestructura utilizadas por los agentes cibernéticos de la RPDC. Esos informes permiten a los defensores de la red detectar actividades cibernéticas malintencionadas por parte de la RPDC y reducir la exposición a ellas. El sitio web de la CISA contiene la última información actualizada sobre esas amenazas persistentes: https://www.us-cert.gov/northkorea.

Además, la CISA proporciona a sus partes interesadas amplios conocimientos y prácticas en materia de seguridad cibernética y de la infraestructura, comparte esos conocimientos para permitir una mejor gestión del riesgo y los pone en práctica para proteger las funciones más críticas de la nación. A continuación se presentan los enlaces hacia los recursos de la CISA:

- Protección de infraestructura crítica: https://www.cisa.gov/protecting-critical-infrastructure
- Seguridad cibernética: https://www.cisa.gov/cyber-safety
- Detección y prevención: https://www.cisa.gov/detection-and-prevention
- Intercambio de información: https://www.cisa.gov/information-sharing-and-awareness
- Reflexiones de la CISA: https://www.cisa.gov/insights
- Lucha contra la delincuencia cibernética: https://www.cisa.gov/combating-cyber-crime
- Nociones básicas del ámbito cibernético: https://www.cisa.gov/cyber-essentials
- Sugerencias: https://www.us-cert.gov/ncas/tips
- Sistema Nacional de Sensibilización en materia Cibernética: https://www.us-cert.gov/ncas
- Avisos en materia de sistemas de control industrial: https://www.us-cert.gov/ics
- Notificación de incidentes, phishing, programas malignos y vulnerabilidades: https://www.us-cert.gov/report

Informes PIN y FLASH del FBI. Las Notificaciones para el Sector Privado (PIN) del FBI proporcionan información actual que mejorará la sensibilización del sector privado sobre

posibles amenazas cibernéticas. Los informes del Sistema de Alerta de Enlace (FLASH) contienen información crítica recopilada por el FBI para su uso por determinados socios del sector privado. Esos documentos tienen por objeto proporcionar a los destinatarios información de inteligencia práctica que ayude a profesionales de la seguridad cibernética y los administradores de sistemas a protegerse de las acciones malintencionadas persistentes de delincuentes cibernéticos. Si usted detecta alguna actividad sospechosa en su empresa o tiene información relacionada con ella, contacte inmediatamente a FBI CYWATCH. Para obtener los informes PIN o FLASH sobre amenazas cibernéticas relacionadas con la RPDC, contacte a cywatch@fbi.gov.

- División cibernética del FBI: https://www.fbi.gov/investigate/cyber
- Programa del agregado para Asuntos Jurídicos del FBI: La misión central del agregado para Asuntos Jurídicos del FBI es establecer y mantener enlaces con los principales servicios de seguridad y fuerzas del orden en determinados países extranjeros. https://www.fbi.gov/contact-us/legal-attache-offices

Publicación por el Comando Cibernético de los Estados Unidos de información sobre programas malignos. Las fuerzas cibernéticas del Departamento de Defensa buscan activamente actividades cibernéticas malintencionadas de la RPDC, incluidos programas malignos de ese país que se aprovechan de instituciones financieras, realizan operaciones de espionaje y promueven actividades cibernéticas malintencionadas en contra de los Estados Unidos y sus aliados. El Comando Cibernético de los Estados Unidos publica periódicamente información sobre programas malignos en la que se determinan las vulnerabilidades para que la industria y el gobierno defiendan su infraestructura y sus redes contra las actividades ilícitas de la RPDC. La información sobre programas malignos destinada a reforzar la seguridad cibernética puede consultarse en las siguientes cuentas de Twitter: @US_CYBERCOM y @CNMF_VirusAlert.

Información sobre las sanciones del Departamento del Tesoro de los Estados Unidos y avisos en materia de financiación ilícita

El centro de recursos en línea de la ***Oficina de Control de Activos Extranjeros*** (OFAC) proporciona abundante información relativa a las sanciones contra la RPDC y las sanciones a las actividades cibernéticas malintencionadas, incluidos avisos de sanciones, las leyes pertinentes, las Órdenes Ejecutivas, las normas y los reglamentos relacionados con la RPDC y sanciones relacionadas con actividades cibernéticas. La OFAC también publicó varias preguntas frecuentes relacionadas con las sanciones a la RPDC, las sanciones relacionadas con actividades cibernéticas y las monedas digitales. Para plantear consultas o inquietudes relacionadas con los requisitos y reglamentos de sanciones de la OFAC, contacte la línea telefónica directa de cumplimiento de la OFAC al 1-800-540-6322 o escriba a OFAC_Feedback@treasury.gov.

- Sanciones a la RPDC
  - https://www.treasury.gov/resource-center/sanctions/Programs/pages/nkorea.aspx
  - Preguntas frecuentes: https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#nk
- Sanciones a las actividades cibernéticas malintencionadas
  - https://www.treasury.gov/resource-center/sanctions/Programs/pages/cyber.aspx
  - Preguntas frecuentes: https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#cyber

- Preguntas frecuentes sobre monedas virtuales: https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx#vc_faqs

La ***Red contra los delitos financieros (FinCEN)*** publicó un aviso sobre el uso por Corea del Norte del sistema financiero internacional (https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2017-a008). La FinCEN también publicó avisos específicos para instituciones financieras con obligaciones de presentación de informes sobre actividades sospechosas, que proporcionan orientaciones sobre cuándo y cómo han de notificarse los delitos cibernéticos o la actividad delictiva relacionada con monedas digitales.

- Delincuencia cibernética
  - https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a005
- Actividades ilícitas con monedas digitales
  - https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2019-a003
- Ataques a correos electrónicos de empresas
  - https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2019-a005
  - https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a003

El ***Consejo Federal de Inspección de Instituciones Financieras (FFIEC)*** desarrolló la herramienta de evaluación de la seguridad cibernética para ayudar a las instituciones financieras a determinar sus riesgos y su estado de preparación en materia de seguridad cibernética. La herramienta de evaluación puede consultarse en https://www.ffiec.gov/cyberassessmenttool.htm.

ANEXO II: Informes del Grupo de Expertos de las Naciones Unidas sobre amenazas cibernéticas de la RPDC

Informes del Grupo de Expertos del Comité del Consejo de Seguridad de las Naciones Unidas establecido en virtud de la resolución 1718. El Comité sobre la RPDC del Consejo de Seguridad de las Naciones Unidas establecido en virtud de la resolución 1718 cuenta con el apoyo de un Grupo de Expertos que tiene como cometido "reunir, examinar y analizar la información" proporcionada por los Estados Miembros de las Naciones Unidas, los órganos pertinentes de ese sistema y otras partes sobre la aplicación de las medidas establecidas en las resoluciones del Consejo de Seguridad de las Naciones Unidas contra Corea del Norte. El Grupo de Expertos también formula recomendaciones sobre la manera de mejorar la aplicación de las sanciones en dos informes que presenta al Comité, a saber, el informe de mitad de período y el informe final, que pueden consultarse en https://www.un.org/securitycouncil/es/sanctions/1718/panel_experts/reports.