INFORME DE INVESTIGACIÓN

OIG-QI-23-003

DEPARTAMENTO DE RECURSOS NATURALES Y AMBIENTALES (DRNA)

Incidente en Centro de Cómputos

19 de diciembre de 2022

OIG
OFICINA DEL INSPECTOR GENERAL
GOBIERNO DE PUERTO RICO

TABLA DE CONTENIDO

Página

RESUMEN EJECUTIVO

El 29 de septiembre de 2022, la Oficina del Inspector General de Puerto Rico (en adelante, OIG), advino en conocimiento de información que trascendió públicamente, sobre un alegado incidente en el Centro de Cómputos de las oficinas del Departamento de Recursos Naturales y Ambientales (en adelante, DRNA), del cual no surgía certeza sobre la causa pero que tuvo un impacto negativo en las operaciones y los sistemas de información de la entidad.

Según la información publicada, hubo un incendio en la entidad que afectó los discos duros del Centro de Cómputos, así como los sistemas de información. Posteriormente, la entidad aclaró que, el incidente surgió a raíz de fallas eléctricas que no permitían la sincronización adecuada de los sistemas.

En su función preventiva y en el ejercicio de la jurisdicción y competencia que le ha sido conferida a la OIG mediante el Artículo 7, inciso (t) de la Ley Núm. 15-2017, según enmendada, conocida como *Ley del Inspector General de Puerto Rico* (en adelante, Ley Núm. 15-2017), el Área de Querellas e Investigaciones de la OIG (en adelante, Área de QI) determinó iniciar un proceso investigativo. Ello, a los fines de validar la información, así como evaluar la situación e identificar las causas y los efectos provocados a raíz del alegado incidente y las posibles consecuencias en el servicio y operación de la entidad.

El 30 de septiembre de 2022, el Área de QI, diligenció una comunicación al DRNA, sobre Notificación de Visita, Inspección y Requerimiento de Información para la Investigación QI-050-23-005. Esto, con el propósito de examinar métodos de manejo y control de seguridad en los sistemas de información del DRNA y validar su cumplimiento. Como parte de la investigación, se llevaron a cabo entrevistas, visitas y requerimientos de información.

Entre otras cosas, de la información recopilada, surgió que, a principios de agosto hubo un patrón de fallas eléctricas que atentaban contra los sistemas y las operaciones del DRNA. En específico, el DRNA indicó que, el 12 de septiembre de 2022, hubo una falla que provocó la interrupción de servicios esenciales provistos al ciudadano, así como a entidades estatales y federales. A su vez, las herramientas de trabajo relacionadas a los sistemas de información del personal del DRNA resultaron inoperables.

A raíz de este incidente, se identificaron riesgos adicionales sobre posible pérdida irreparable de información esencial o privilegiada por no llevarse a cabo actos preventivos suficientes, ante las alertas y amenazas. Como resultado de la investigación, la OIG identificó que, el DRNA pudo haber incurrido en deficiencias e incumplimientos con la política pública de controles internos y medidas preventivas para seguridad cibernética, establecida por el Gobierno de Puerto Rico y con las disposiciones de la Ley Núm. 75-2019, conocida como *Ley de la Puerto Rico Innovation and Technology Service* (PRITS) y otras normativas relacionadas.

Se identificó que, en la División de Infraestructura, desde donde opera la Oficina de Informática, existe ausencia de protocolos, planes y procedimientos detallados sobre manejo de contingencias

tecnológicas. Además, no existen planes o mecanismos fijos y detallados para llevar a cabo análisis de riesgos, de manera periódica. Esto pudo haber contribuido en el incremento del impacto de los sucesos mencionados.

El contenido del presente informe es público, conforme con lo establecido en la Ley Núm. 15-2017, según enmendada, conocida como *Ley del Inspector General de Puerto Rico* (Ley Núm. 15-2017)*;* el Artículo 1.9 del Reglamento Núm. 9135, titulado como *Reglamento sobre Asuntos Programáticos de la Oficina del Inspector General;* el Artículo 1.5 del Reglamento Núm. 9136, titulado como *Reglamento para la Publicación de Informes y Documentos Públicos Rutinarios de la Oficina del Inspector General de Puerto Rico;* así como otras normativas aplicables.

INFORMACIÓN SOBRE LA ENTIDAD

La Ley Núm. 23 de 20 de junio de 1972, según enmendada, conocida como la *Ley Orgánica del Departamento de Recursos Naturales y Ambientales* (DRNA), expone que, este será responsable de implementar la política pública del Gobierno de Puerto Rico contenida en la sección 19 del Artículo VI de la Constitución de Puerto Rico.

Dicha sección establece que, será política pública del Estado Libre Asociado de Puerto Rico, la más eficaz conservación de sus recursos naturales, así como el mayor desarrollo y aprovechamiento de los mismos para el beneficio general de la comunidad. A esos efectos, el DRNA pone en vigor, programas para la utilización y conservación del ambiente y de los recursos naturales de Puerto Rico conforme a lo establecido en la Ley Núm. 416-2004, según enmendada, conocida como *Ley Sobre Política Pública Ambiental*.

La Ley Núm. 171-2018, conocida como *Ley para Implementar el Plan de Reorganización del Departamento de Recursos Naturales y Ambientales de 2018*, tiene el propósito de ejecutar y dar cumplimiento al Plan de Reorganización del DRNA, adoptado al amparo de la Ley Núm. 122-2017, conocida como *Ley del Nuevo Gobierno de Puerto Rico*, el cual transfiere, agrupa y consolida en el DRNA, facultades, funciones, servicios y estructuras de la Junta de Calidad Ambiental (JCA), la Autoridad de Desperdicios Sólidos (ADS) y el Programa de Parques Nacionales adscrito al Departamento de Recreación y Deportes, (Programa de Parques Nacionales), a los fines de agilizar los trámites, compartir recursos gubernamentales, lograr ahorros y viabilizar la externalización de ciertas funciones o servicios.

El DRNA cuenta con 7 oficinas regionales que están localizadas en los municipios de San Juan, Arecibo, Aguadilla, Mayagüez, Ponce, Guayama y Humacao. El propósito de las oficinas regionales es hacer más accesible, al público general alrededor de toda la Isla, los servicios que ofrece la agencia. Las funciones y servicios que cada una de las oficinas ofrecen son: radicación de solicitudes de caza y pesca, permisos para acampar, solicitudes para franquicias de agua, permisos de corte y poda, entre otros.

Las oficinas regionales cuentan con las siguientes áreas: navegación, recaudación, mantenimiento de playas, mantenimiento de cuerpos de agua, vivero regional y geología. El DRNA trabaja un total, de 242 permisos, 215, estos están divididos por conceptos o etapas, y se proyectan 27 permisos adicionales.

BASE LEGAL

La OIG tiene la responsabilidad de coordinar y ampliar los esfuerzos gubernamentales para promover la integridad y detectar y prevenir fraude, la malversación y el abuso en el uso de los fondos públicos estatales y federales. De la misma manera, detecta e investiga posibles fuentes de corrupción y toma acciones proactivas para prevenir situaciones de esta naturaleza y así, fomentar una sana administración gubernamental.

El presente informe se emite en virtud de los Artículos 7, 8, 9 y 17 de la Ley Núm. 15-2017, según enmendada. De igual forma, a tenor con las disposiciones contenidas en el Reglamento Núm. 9135-2019, conocido como *Reglamento sobre Asuntos Programáticos de la Oficina del Inspector General* y otras normativas aplicables.

ALCANCE Y METODOLOGÍA DE LA INVESTIGACIÓN

La investigación cubrió el periodo del 1 de agosto de 2022 al 18 de octubre de 2022. La metodología utilizada fue la siguiente:

1. Análisis de la información que trascendió públicamente sobre alegado incendio en el Centro de Cómputos del DRNA.
2. Análisis y evaluación de información obtenida en respuestas a cuestionario durante entrevista al director interino de Informática del DRNA.
3. Análisis de información obtenida en respuesta a tres (3) Requerimientos de Información cursados por la OIG al DRNA.
4. Análisis y evaluación de información oficial publicada por DRNA para aclarar y desmentir alegado incendio, en conjunto con cualquier orden o aclaración que surgiera del expediente del proceso de enmiendas propuestas al *Reglamento para el Control de la Contaminación Atmosférica y la adopción del Plan de Implementación Estatal para las Áreas de No Logro con el Estándar Nacional de Calidad de Aire Ambiental de Dióxido de Azufre* del DRNA.
5. Análisis y evaluación de la Ley Orgánica del DRNA y de la reglamentación y normativas publicadas por la agencia.
6. Análisis y evaluación de la Ley Núm. 75-2019, mejor conocida como *Ley de la Puerto Rico Innovation and Technology Service* (PRITS) y normativas aplicables al uso y manejo de sistemas de información del Gobierno de Puerto Rico.

7. Entrevistas a personal del DRNA.
8. Inspección del área del Centro de Cómputos.
9. Otros documentos, leyes y referencias según fuera necesario.

En algunos aspectos, se examinaron transacciones, documentos y operaciones, sin consideración a sus fechas o vigencia.

HECHOS DETERMINADOS

Como parte de una investigación que se realizó en el DRNA, surgen posibles situaciones que podrían representar falta de atención y descuido en la planificación, uso y manejo de sistemas de información, ante casos fortuitos o de emergencia, así como en el resguardo de información de la entidad. Lo anterior, en posible contravención con la política pública del Gobierno de Puerto Rico, sobre controles internos y sana administración de los sistemas de información y tecnología.

Conforme al análisis realizado por un equipo especial asignado al Área de QI de la OIG, se detallan los siguientes hechos:

1. El **29 de septiembre de 2022,** la OIG advino en conocimiento de información que trascendió públicamente, en la cual se identificaba un alegado incidente en el Centro de Cómputos de las oficinas del DRNA, del cual no surgía certeza sobre la causa, no obstante, tuvo un impacto negativo en las operaciones y los sistemas de información de la entidad.
2. En la información se destacó que en esos momentos el DRNA se encontraba en el proceso de recibir comentarios para la adopción de cambios a la reglamentación. Surge que en ese momento había vigente una Orden de un Oficial Examinador a cargo de un proceso de enmiendas y adopción de reglamentos del DRNA, con fecha del **23 de septiembre de 2022**, que establecía la extensión de término para ofrecer comentarios sobre los trámites reglamentarios propuestos y que se debía publicar un nuevo anuncio al respecto, junto con un portal web alterno para colocar y hacer disponibles los documentos a los ciudadanos.
3. Según la Orden e información que trascendió el **12 de septiembre de 2022**, la página *web* del DRNA colapsó debido a una fluctuación de voltaje que ocasionó un incendio y destruyó los discos duros del sistema de información del DRNA. En el reporte de prensa surge que, una empleada del DRNA relató que ese día sonaron las alarmas contra incendios en la sede de la agencia.
4. Por otra parte, de una nota de prensa publicada el **29 de septiembre de 2022,** surgió que el DRNA, a través de su secretaria, había desmentido los hechos indicando que "*en ningún momento ha surgido incendio alguno en el centro de cómputos ni se han quemado los discos duros en el sistema informático.*" Más bien se alegó que, debido a fluctuaciones eléctricas antes y después del huracán Fiona, los sistemas de control

del sistema de almacenaje de datos sufrieron desperfectos que no permitían la sincronización de los sistemas. Al respecto, se indicó que, la causa establecida mediante Orden sería corregida y que el DRNA había estado en comunicación tanto con la compañía *Dell* como con el personal de la PRITS para corregir la situación.

5. A raíz de las versiones internas del DRNA sobre lo acontecido, el Área de QI de la OIG, inició un proceso investigativo al amparo de la Ley Núm. 15-2017, para validar o descartar los señalamientos, identificar las posibles razones que pudieron generar los acontecimientos reseñados y evaluar los efectos en la entidad, así como el posible impacto en los servicios esenciales a la ciudadanía, que pudieron haberse afectado.

6. El **30 de septiembre de 2022**, el Área de QI de la OIG, diligenció una comunicación dirigida al DRNA, sobre Notificación de Visita, Inspección y Requerimiento Información para la investigación QI-050-23-005, con el propósito de examinar métodos de manejo y control de seguridad en los de sistemas de información del DRNA.

7. En igual fecha, se llevó a cabo una entrevista por personal de la OIG al director interino de Informática, desde donde opera la Oficina de Informática del DRNA, con el propósito de obtener respuestas, mediante un cuestionario relacionado al alegado incendio reportado el 12 de septiembre de 2022, y sobre los controles y procesos internos que mantiene la entidad, sobre los sistemas de información. En la entrevista se obtuvo información certera del funcionario con mayor conocimiento sobre los sistemas de información y que, proveyó un panorama del funcionamiento de los sistemas de información del DRNA, así como de sus controles internos. Luego de obtener las respuestas solicitadas, mediante cuestionario, se llevó a cabo un proceso de retención de archivos digitales sujetos a litigio (denominados *litigation hold*, en inglés).

8. Personal de la OIG visitó e inspeccionó el área conocida como Centro de Cómputos, donde ubica el cuarto de servidores del DRNA, junto al director interino de Informática de la agencia, luego de culminado el proceso de entrevista. El Director Interino hizo un recorrido por el área explicando el uso de los servidores y los equipos allí instalados. Personal de la OIG examinaron visualmente y tomaron fotografías.

Como resultado de la investigación realizada y el análisis de los documentos entregados por el DRNA, la OIG concluyó que existe incumplimiento por parte de la agencia en cuanto a las normas y la política pública establecida por el Gobierno de Puerto Rico sobre el control y manejo de tecnologías y sistemas de información. Las posibles situaciones, a su vez, podrían representar falta de atención y cuidado en la planificación para el manejo de riesgos, en casos fortuitos o de emergencia, así como un impacto en los servicios ofrecidos a la ciudadanía, y a entidades estatales y federales.

HALLAZGOS DE LA INVESTIGACIÓN

Al amparo de las disposiciones legales antes citadas, a continuación se detallan los hallazgos relacionados a situaciones detectadas durante el transcurso de la presente investigación.

Hallazgo 1 – Deficiencias en el manejo preventivo de fallas en los sistemas de información, afectan servicios esenciales provistos por DRNA a la ciudadanía.

El 6 de octubre de 2022, la OIG realizó un requerimiento de información al DRNA para solicitar entre otras cosas, certificación sobre entidades y servicios que requieren de la conectividad de los sistemas de información del DRNA, para ser provistos. En respuesta a dicho requerimiento el DRNA certificó a través del director Interino de Informática que, al 12 de octubre de 2022, todas las áreas de servicio del DRNA se vieron parcial o totalmente afectadas, así como los servicios de las entidades que dependen directa o indirectamente de la funcionalidad de los sistemas del DRNA. Se identificaron unas diecinueve (19) entidades relacionadas:

- Customs and Border Protection
- Departamento de Hacienda
- Departamento de Justicia
- Departamento de Salud
- Drug EnforcementAdministration
- Federal Bureau of Investigations
- High Intensity Drug Trafficking Area
- Homeland Security Investigation
- Immigration and Customs Enforcement
- Negociado de la Policía de Puerto Rico
- Oficina del Contralor
- Oficina de Ética Gubernamental
- US Coast Guard
- US Department of Justice
- US Department of Commerce
- Fish and Wildlife Service
- Environmental Protection Agency
- National Oceanic and Atmospheric Administration
- US Forest Service

A esa misma fecha, el DRNA certificó a través del mismo funcionario que las entidades, departamentos y dependencias anteriores y cualesquiera otra que hubiesen requerido la conectividad a los sistemas del DRNA, para sus operaciones, se encontraban sin los siguientes servicios:

- Acceso a los datos de las embarcaciones registradas y nautas autorizados.
- Los datos que se utilizan en gestiones y procesos de investigación tanto criminal como civil. También se utilizan para procesos de fiscalización.
- Acceso a los datos de las acciones administrativas tales como: permisos, endosos y certificaciones. También se provee acceso a los productos de ciertos permisos tales como licencias de cacería, tenencia y portación de armas de caza, pesca, recolección de especies y otros.
- Portal DRNA-Portal oficial del DRNA en internet que provee información diversa que, entre otras, incluye análisis de medio ambiente, contaminación de playas y otros.

Por su parte, la Oficina de Recursos Humanos del DRNA, a través de su Sub Directora, certificó que, alrededor de 1,000 empleados se vieron afectados por los incidentes ocurridos en los sistemas de información luego del 12 de septiembre de 2022, en cuanto a su registro de asistencia en Kronos del Sistema RHUM y detalle de tiempo. A su vez, el director interino de Informática, certificó que la División de Infraestructura, donde a su vez opera la Oficina de Informática unos 963 empleados del DRNA, no podían ofrecer la totalidad de los servicios, por los problemas con los sistemas de información.

Previo a las certificaciones obtenidas con los resultados y el efecto en los servicios de las fallas, en respuesta a requerimientos de la OIG, el director interino de la División de Infraestructura, donde opera la Oficina de Informática del DRNA, había ofrecido respuestas a un cuestionario relacionado al control y manejo de los sistemas de información del DRNA.[2] A su vez, proveyó detalles de otras situaciones ocurridas, durante los meses de agosto y septiembre de 2022, previo al incidente del 12 de septiembre, que tuvo un impacto mayor, que dio lugar a la noticia reportada el 29 de septiembre de 2022.

De las respuestas obtenidas durante el transcurso de la investigación y brindados por el funcionario, y que la OIG pudo validar que, el 12 de septiembre de 2022:

- No hubo un incendio en el Centro de Cómputos del DRNA y que los incidentes que afectaron los sistemas de información fueron a raíz de fluctuaciones de voltajes.
- Desde el mes de agosto de 2022, personal del DRNA identificó fallas eléctricas en el sistema.

De la entrevista realizada, se mencionó que:

- El 10 de agosto de 2022, hubo un apagón que ocasionó alertas en los discos duros.

[2] Mediante entrevista llevada a cabo por personal de la OIG el 30 de septiembre de 2022.

- Los servicios de mantenimiento se encontraban vencidos al momento de los incidentes y que ha habido comunicaciones al respecto, pero no se ha podido atender el asunto por falta de presupuesto.
- Al 17 de octubre de 2022, aún quedaban pendiente de recibir o adquirir servicios o equipos necesarios, a raíz de los incidentes mencionados.
- Que el trámite de aprobación de órdenes de compra sobre reparación, mantenimiento o adquisición de discos duros había demorado.

De la información obtenida mediante la entrevista, surge que, el DRNA no estuvo preparado, de manera adecuada y suficiente, para mantener y garantizar el funcionamiento de los sistemas de información y proteger los mismos ante interrupciones y fluctuaciones imprevistas de energía eléctrica. Sobre esto, se destaca que, los incidentes de fluctuaciones eléctricas, precisamente estuvieron atados a problemas con los generadores del edificio. Es decir, los componentes de energía suplemente no respondieron de manera adecuada. Ello provocó que la operación de los sistemas de información se viera afectada.

El director interino de Informática del DRNA, indicó en respuesta al cuestionario provisto por la OIG que, al momento de la investigación, el DRNA contaba con 2 suplentes de energía , los *uninterruptible power supplies* conocidos como (UPS, por sus siglas en inglés) que mantienen un máximo de duración de solo 20 minutos, luego de cualquier falla o cese de electricidad.

De otra parte, éste informó que los contratos de mantenimiento se encuentran vencidos, pero que el personal del DRNA brinda mantenimiento a los equipos, sistemas y servidores de datos de manera periódica, con frecuencia semanal. No obstante, como parte de la información solicitada por la OIG, no se recibió copia o declaración certificada de los registros o bitácoras de mantenimiento a los sistemas y equipos de información por los pasados doce (12) meses, proveyendo mediante certificación negativa, a los efectos de indicar que no existen registros ni bitácoras del mantenimiento a éstos.

En cuanto a situaciones de alerta previa, no se desprendió información indicativa de que el DRNA llevara a cabo un análisis de riesgos, producto de las fallas y alertas ocurridas durante el mes de agosto, para evaluar la magnitud e impacto del daño que podría causar un evento mayor en cuanto al acceso, interrupción o destrucción de datos en los sistemas de información que respaldan sus operaciones. Hubo gestiones reactivas y comunicaciones con PRITS, y con una compañía privada. Pero, aun así, no se identificaron controles futuros certeros y confiables para manejar una situación similar, a base de los resultados o las vulnerabilidades reflejadas en algún análisis preventivo de riesgos que se haya realizado. Esto, a falta de informes preventivos detallados, como parte de planes o protocolos establecidos.

En torno a los trámites de mitigación llevados a cabo por el DRNA, se obtuvo copia de solicitudes y aprobaciones de PRITS sobre órdenes de compra y asistencia en la creación de un nuevo portal *web*, luego del colapso de los sistemas. También hubo trámites para recibir servicios tecnológicos y adquisiciones de equipo. Sin embargo, se identificaron fallas desde el mes de agosto, mas no surgen reportes de incidentes previos o periódicos desde el inicio de las mismas, cursadas al

personal de la Oficina de PRITS relacionados a las situaciones con los sistemas de información, incumpliendo con el proceso establecido por las normativas para el reporte de incidencias.

El director interino de Informática proveyó copia de una declaración cronológica interna tipo informe, dirigida a la secretaria del DRNA, para constatar alegadas situaciones con los resguardos, portales, discos duros, o cualquier otro incidente relacionado a los sistemas de información ocurridos desde agosto. No obstante, a pesar de que hubo situaciones recurrentes desde el mes de agosto, el documento titulado: *Informe sobre Incidente con "Data Center"- agosto a septiembre de 2022*, que fue provisto a la OIG, y enviado por parte del director interino de Informática a la atención de la secretaria del DRNA, tiene fecha del 4 de octubre de 2022, la cual es posterior a nuestra notificación de intervención en el DRNA. Esta acción surge casi dos (2) meses después de las alertas de eventos previos y luego del inicio de la gestión investigativa de la OIG.

Efecto

Las situaciones comentadas tienen el siguiente efecto:

1. No haber salvaguardado los mejores intereses para el Gobierno de Puerto Rico y la ciudadanía, mediante acciones preventivas.
2. Ser contrarias a las normativas aplicables para el manejo preventivo y oportuno de riesgos, ante incidentes de impacto en los sistemas de información.
3. Mantener riesgo considerable de pérdida irreparable de información esencial o privilegiada por no llevar a cabo análisis y acciones preventivas suficientes, ante alertas y amenazas.
4. Impacto negativo en las operaciones y los sistemas de información de la entidad.
5. Contribuir a la interrupción de servicios derivados esenciales provistos al ciudadano, y utilizado por entidades estatales y federales en el transcurso de sus funciones.
6. Contribuir a la interrupción del sistema de registro de asistencias digital, y posible riesgo de errores por ajuste de asistencia sin corroborar.
7. Posible pago de nómina a recursos humanos que no pudieron cumplir con labores regulares de servicios, por problemas en los sistemas y herramientas de trabajo.

Otras situaciones identificadas fueron:

La situación con los sistemas de información provocó que se extendiera el término para ofrecer comentarios a trámites reglamentarios en curso sobre el Reglamento para el Control de la Contaminación Atmosférica (Reglamento) y la adopción del Plan de Implementación Estatal para las Áreas de No Logro con el Estándar Nacional de Calidad de Aire Ambiental de Dióxido de Azufre del DRNA (Plan). Para ello, se solicitó la publicación de un nuevo anuncio, junto con un portal *web* alterno para colocar y hacer disponibles los reglamentos propuestos a los ciudadanos, para observaciones y comentarios.

La evaluación realizada al expediente de los trámites reglamentarios reflejó que fue necesario emitir dos (2) Órdenes del Oficial Examinador a cargo, con fecha del 23 de septiembre de 2022, para extender los términos de presentación de comentarios para los procesos relacionados al Plan y Reglamento.

Del análisis investigativo de la OIG surge que, pese a que no hubo incendio en los predios del DRNA, esto no eliminó la seriedad del asunto ni las deficiencias en el manejo de los sistemas de información. Los efectos provocados mantuvieron su esencia, y ello tuvo un impacto en las funciones de la entidad.

Hallazgo 2 – Deficiencias en los controles internos para el manejo de los sistemas de información del DRNA y la protección adecuada de equipos.

De las respuestas obtenidas el 30 de septiembre de 2022, por parte del director interino de la Oficina de Informática del DRNA, al cuestionario relacionado al control y manejo de los sistemas de información provisto por la OIG, surgieron asuntos indicativos de que el DRNA podría no estar implementando controles internos adecuados y suficientes para el manejo de los sistemas de información y la protección adecuada de equipos, programas y datos. Algunas de las situaciones relevantes han sido expuestas en el hallazgo 1 del presente informe. Por su parte, el impacto de los incidentes de fluctuaciones eléctricas pudo haber guardado una estrecha relación con controles internos de contingencia, tales como un mantenimiento adecuado de los generadores eléctricos del edificio. De ahí, a que la operación de los sistemas de información se viera afectada al no contar con generadores de energía operando adecuadamente.

a. Problemas con el mantenimiento de los discos duros y equipo

Sobre los discos duros de almacenaje del centro de datos (*data center*) del DRNA, se indicó que los mismos son marca *Dell* y que el servicio de mantenimiento se encontraba vencido al momento de la intervención, sin haberse podido atender previamente, por falta de "presupuesto". De la información obtenida sobre el inventario de equipos y programas, provistos por el DRNA, se pudo constatar que dichos servicios habían vencido, algunos en el 2018 y otros en el 2019. El director interino de Informática indicó que se brinda mantenimiento a los sistemas y a los equipos semanalmente. El mismo funcionario certificó el 7 de octubre de 2022, que no existen registros ni bitácoras sobre el mantenimiento periódico brindado a los sistemas.

b. Falta de normativas y procedimientos para la disposición de equipo no utilizado

De la información obtenida por la OIG, se observó que el DRNA no cuenta con normativas o procedimientos específicos para la disposición de equipos electrónicos, medios de almacenamiento externos y licencias de aplicaciones. La Oficina de Informática indicó que mantiene un registro de equipo a disponerse o declarado excedente. Sin embargo, no mantienen controles para la custodia o almacenamiento y la disposición confiable de los medios de almacenamiento electrónico. Más bien dependen de que vayan a la agencia a descartarlos, ya que el DRNA se encuentra desarrollando protocolos y manuales de instrucciones al respecto. Al

momento, trabajan a través de instrucciones del director interino de Informática previo a disponer de los equipos.

c. Falta de control y manejo de inventario de los sistemas de información.

Sobre el control y manejo de inventario se explicó que se realizan procesos de inventario de equipo periódicamente y se actualizan diariamente. A esos efectos, la OIG llevó a cabo un requerimiento de información en el cual solicitó una lista de inventario de equipos tecnológicos instalados, localizados o asignados al Centro de Cómputos del DRNA, que incluyera: modelo, fecha de adquisición, capacidad, nombre manufacturero e identificar cuáles de estos están bajo garantía o contrato mantenimiento. Se proveyeron 3 listados diferentes, sin uniformidad en la presentación de la información ni detalles explicativos para la falta de detalles sin incluir. Para algunos programas o equipos, no se incluyó detalles de su fecha de adquisición, modelo o su capacidad o si existía garantía o mantenimiento vigente.

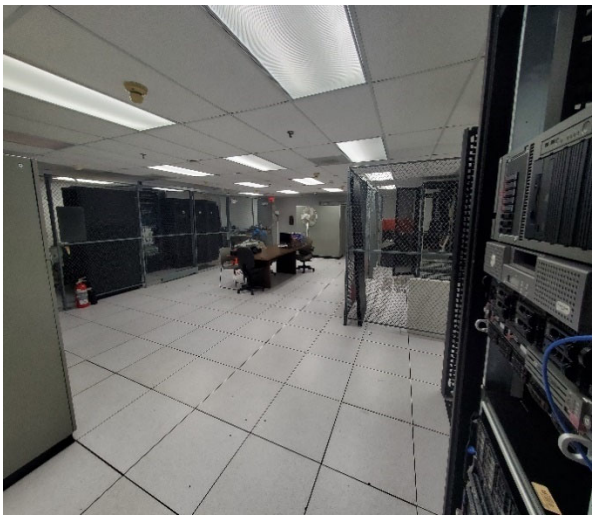
d. Equipos sin garantías vigentes

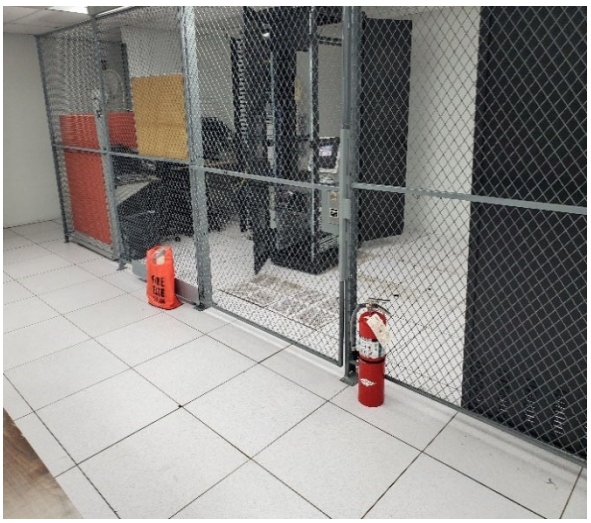
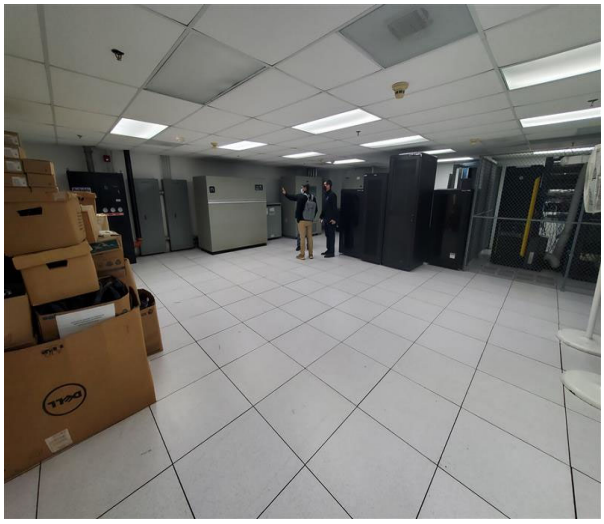
En cuanto a las fechas de mantenimiento o garantías que sí fueron incluidas, algunas habían vencido en el año 2018 y otras vencieron en el 2019. Se incluyeron 2 fechas referentes al año 2023, pero no estaban atadas a ningún equipo o programa en particular por lo que se desconoce el equipo o programa al que pertenecen o si, por el contrario, fueron incluidas por error.

e. Desperfectos y deficiencias en sistema y controles necesarios contra incendios

Luego de la entrevista, llevada a cabo el 30 de septiembre de 2022, se llevó a cabo una inspección ocular del Centro de Cómputos del DRNA (*data center*), también conocido como cuarto de servidores. De la visita, surgió lo siguiente:

Existía un extintor de incendio de uso manual tipo rociador, ubicado en el suelo y disponible. No obstante, el sistema de supresión de incendios mostraba desperfectos y el área no tiene sensores para detectar presencia de agua. De otra parte, se pudo observar una acumulación de cajas de cartón ubicadas en el lugar que podrían acelerar o agravar los efectos de cualquier incendio de origen externo o interno, provocando un riesgo de seguridad.



Luego de evaluar el lugar donde ocurrió el alegado incidente, la OIG no encontró señales visibles o evidencia de un incendio en los sistemas del DRNA. No obstante, de la inspección realizada se pudo observar lo siguiente:

1. No contaba con un sistema automático de supresión de incendios, esto es esencial e indispensable en un cuarto de servidores.
2. El UPS de 150 KW no estaba funcionando y no contaba con el mantenimiento adecuado para estos dispositivos.
3. Los resguardos de los servidores virtuales, debido a su configuración, se estaban grabando en los mismos discos donde estaba el sistema de producción afectado, lo que imposibilita recuperase del incidente mediante resguardos.
4. El generador eléctrico de la agencia tenía problemas para encender.
5. Falta de mantenimiento o contrato de servicios para los servidores principales de una agencia.
6. Cajas de cartón que pueden ser un acelerante en un incendio.

Los sistemas de información son parte esencial de las operaciones diarias de una agencia el no cumplir con las mejores prácticas y recomendaciones ponen en peligro las funciones de los que laboran en ella y de agencias, ciudadanos o entidades que dependen de sus datos para tomar decisiones. Los efectos y repercusiones de este incidente en los sistemas del DRNA pudieron ser contenidos si hubieran trabajado ágilmente en establecer las recomendaciones del informe de la Oficina del Contralor publicado el 14 de abril del 2021, llamado Informe de Auditoría TI-21-11.

Efecto

Las situaciones comentadas tienen el siguiente efecto:

1. Fomentar acciones contrarias a las mejores prácticas de control interno para la protección adecuada de programas y equipo tecnológico.
2. No salvaguardar los mejores intereses del Gobierno de Puerto Rico, en cuanto al cuidado y la atención preventiva de equipos y sistemas.
3. Carecer de registros o bitácoras útiles sobre el mantenimiento periódico brindado a los sistemas, como método de control futuro.
4. Crear vulnerabilidad sobre manejo y protección de data, a falta de normativas o procedimientos específicos para la disposición adecuada de equipos electrónicos o programas sensitivos que necesiten ser reemplazados.
5. Mantener un posible registro de inventario incompleto o sin datos actualizados para uso futuro.
6. Provocar vulnerabilidades en centro de datos o cuarto de servidores que podrían exacerbar el efecto de un incidente o fallar en prevenirlo.

Hallazgo 3 – Ausencia de nombramientos y designaciones oficiales para la atención y el manejo de los sistemas de información y la seguridad cibernética.

La Ley Núm. 75-2019 (en adelante, Ley Núm. 75-2019), conocida como *Ley de la Puerto Rico Innovation and Technology Service* (en adelante, PRITS), del 25 de julio de 2019, se promulgó con el propósito de establecer y promover la política pública sobre la elaboración, manejo, desarrollo, coordinación e integración efectiva de la infraestructura tecnológica e informática del Gobierno de Puerto Rico.[3] Establece, además, una serie de funciones, facultades y deberes tanto de PRITS, el Principal Ejecutivo de Innovación e Información (en adelante, PEII) del gobierno, así como de todas las entidades públicas. Dicha política pública del Gobierno de Puerto Rico, sobre el uso y manejo de los Sistemas de Información, persigue lograr que se cumpla con todos los estándares y procedimientos asociados a los controles y la seguridad cibernética, definidos por el PRITS para la operación y manejo de los activos de información. Pero, sobre todo, que los empleados o funcionarios gerenciales de esas materias mantengan roles y responsabilidades específicas por las cuales responder (*accountability*). Todo ello, para evitar, en el mayor grado posible, que surjan desviaciones y excepciones a la política pública uniforme que dio paso a la Ley Núm. 75-2019.[4]

A esos efectos, se crea la figura del PEII encargado, entre otras cosas, de evaluar y emitir recomendaciones finales sobre los nombramientos de los Principales Oficiales de Informática (en adelante, OPI) de las agencias[5] , las cuales, a su vez, deberán cumplir con todas las políticas de manejo de información y los estándares tecnológicos adoptados por el PRITS.[6] Parte de esto consiste en que las agencias deben notificar los nombramiento de sus Principales Oficiales de Informática (OPI) al PEII para su evaluación y recomendación final.[7] No podría hacerse nombramiento, transferencia o destaque de ninguna persona como OPI sin la previa autorización de PRITS. De lo contrario, estos podrán declararse nulos. Para ello, las agencias utilizarán un formulario único y exclusivo establecido por PRITS como "Formulario PRITS-002-Nombramientos de OPI".

Para propósitos del PRITS, el término OPI incluye al Oficial Principal de Informática de la agencia o en su defecto, el director o directores de información y tecnología que ejerzan funciones equivalentes. Incluso, se aclara que la ausencia de un OPI debidamente nombrado y en funciones no constituiría justificación para el incumplimiento con la Ley Núm.75-2019 y/o cualquier opinión o normativa derivada.[9]

En adición a la figura del OPI o, en su defecto, el director de información y tecnología (o quien ejerza su equivalencia en funciones), las entidades de gobierno deberán designar a una persona o

---

[3] Véase, Exposición de Motivos de Ley Núm. 75-2019.
[4] Véase, el Punto 2, titulado "Propósito", Incisos (3) y (4) de la Política para la Seguridad Cibernética, del 29 de octubre de 2021 y la Carta Circular Núm. 2021-007 del 6 de diciembre de 2021, publicadas por PRITS.
[5] véase, Art. 6(ee) d la Ley Núm.75-2019.
[6] Art 12 b y d de Ley Núm. 75-2019
[7] Art 12 j. de Ley Núm. 75-2019 y Orden Administrativa PRITS 2021-003 del 12 de abril de 2021.
[9] Id.

equipo que será responsable de la seguridad cibernética y el manejo de riesgos de la agencia. Dicha persona o equipo deberá, entre otras cosas:

- Evaluar el riesgo y el impacto que podría resultar del acceso no autorizado, la utilización, la divulgación, la interrupción, la modificación o la destrucción de la información o los sistemas de información.
- Determinar los niveles de seguridad cibernética apropiados para proteger la información y sus sistemas mediante la implementación de políticas, procedimientos, estándares y controles promulgados por el PRITS.
- Realizar pruebas y evaluaciones periódicas de la efectividad de las medidas, procedimientos y prácticas de seguridad cibernética, que se realizarán en función del riesgo, **no menos de una vez al año**. Las pruebas deben incluir controles de manejo, operacionales y técnicos para cada sistema de información identificado.
- Desarrollar procedimientos para detectar, reportar y responder a incidentes de seguridad cibernética, que deberán (i) ser consistentes con las políticas, guías y estándares establecidos por el PRITS; (ii) incluir la mitigación de los riesgos asociados con tales incidentes antes de que se produzcan daños sustanciales; (iii) notificar y consultar al PRITS; y (iv) notificar y consultar, según corresponda, con los organismos encargados de hacer cumplir la ley y otras oficinas pertinentes.
- Diseñar e implementar planes y procedimientos para la recuperación tras desastres y asegurar la continuidad de las operaciones de los sistemas de información que apoyen las actividades de la agencia.[10]

En la referida entrevista, surgió que, el funcionario designado no tenía detalles sobre si el DRNA había realizado gestiones con PRITS para obtener la aprobación de su puesto como OPI o director interino de informática de la agencia. Indicó, sin embargo, que contaba con una designación oficial por parte de la agencia. A esos efectos, el DRNA proveyó 2 comunicaciones con fechas del 29 de agosto de 2019 y 27 de mayo de 2022, respectivamente, en las que el entrevistado fue designado interinamente como director de la Oficina de Informática por la autoridad nominadora, para los referidos periodos, al momento de tales designaciones. En cuanto a las autorizaciones externas requeridas, la Oficina de Recursos Humanos certificó el 11 de octubre de 2022, que el DRNA no cuenta con un documento de autorización emitido por PRITS sobre las designaciones interinas para dirigir la Oficina a de Informática, según lo exige la Orden Administrativa PRITS 2021-003.

Del mismo modo, surgió que, el DRNA no cuenta con una persona o equipo de trabajo específicamente designado como responsable del manejo de riesgos y la seguridad cibernética de la agencia. En lo pertinente, la OIG obtuvo un organigrama de puestos con nombres de funcionarios y empleados de la Oficina de Sistemas de Información del DRNA. El mismo tenía fecha del 16 de abril de 2019, por lo que no estaba actualizado, según fue solicitado. Además, de

[10] 7.2.2, 7.2.3, 7.2.7, 7.2.9, 7.2.10 de la Política para la Seguridad Cibernética, publicada el 29 de octubre de 2021, publicadas por PRITS.

un directorio de recursos humanos provisto, no surgen designaciones específicas alusivas al manejo de riesgos y la seguridad cibernética de la agencia.

Efecto

Las situaciones comentadas tienen el siguiente efecto:

1. Impide lograr que se cumpla con todas las políticas, estándares y procedimientos asociados a los controles y seguridad cibernética, establecidos para la operación y manejo adecuado de los sistemas y activos de información.
2. Impide lograr que los empleados o funcionarios gerenciales de informática cumplan con los roles y responsabilidades específicas sobre riesgos y seguridad cibernética, dispuestos por política pública.
3. No se previene, en el mayor grado posible, que surjan desviaciones y excepciones a la política pública uniforme que dio paso a la Ley Núm. 75-2019.
4. No le permite a la agencia con el *expertise* y la facultad legislada, cumplir con su función de evaluar y autorizar los nombramientos, de manera formal, previo al comienzo de funciones.
5. Incide sobre la nulidad de nombramientos, creando un riesgo de cese forzoso de funciones en puestos esenciales.

Hallazgo 4 – Ausencia de planes, procedimientos y políticas de análisis preventivo para el manejo de riesgos y contingencias en los sistemas de información.

A partir del 2019 la política pública legislada sobre infraestructura tecnológica e informática del Gobierno de Puerto Rico persigue promover y establecer, de manera coherente e integrada, el manejo y la regulación efectiva de la infraestructura tecnológica e informática del Gobierno de Puerto Rico.[11] Es por esto que, según mencionado, las entidades públicas cobijadas deberán cumplir con todas las políticas de manejo, elaboración, desarrollo de sistemas y estándares tecnológicos adoptados por PRITS.[12] Hemos destacado la importancia de que las entidades de gobierno implementen las medidas y controles de seguridad que sean necesarios para trabajar de forma correcta y, sobre todo, se cumpla con las normativas vigentes sobre la protección de datos, equipos y programas. Tanto de la entrevista realizada al director interino de Informática, como de las respuestas a los requerimientos de información diligenciados por la OIG durante la investigación, surge que, el DRNA **no cuenta** con las siguientes normas, planes o procedimientos requeridos:

[11] Ref. #2.
[12] Ref. #5.

- Normas o procedimientos de planes de acción detallados y específicos para la recuperación de data (resguardo o *back-up*) tras eventos imprevistos o desastres y asegurar la continuidad de las operaciones de los sistemas.[13]
- Normas, procedimientos, planes o protocolos de acción seguros, detallados y específicos para el manejo y la recuperación de datos tras situaciones de accesos no autorizados, divulgación, utilización, interrupción o destrucción de datos por parte de un usuario, empleado o contratista de la entidad.[14]
- Normas y procedimientos detallados que cumplan con la CC Núm. 2020-05 de PRITS y que garanticen la confiabilidad y confidencialidad de la información, la protección de datos y la seguridad de los sistemas de información.[15]
- Normativas o procedimientos específicos para la disposición de los equipos electrónicos, discos duros, medios de almacenamiento externos y licencias de aplicaciones no desarrolladas internamente.

En cuanto a las medidas requeridas para el manejo adecuado de riesgos y contingencias, el DRNA no realiza análisis de riesgos, de manera periódica, para evaluar la magnitud o impacto del daño que podría causar el acceso, divulgación, interrupción, modificación o destrucción no autorizada a los sistemas de información que respaldan las operaciones de la agencia.[17] Tampoco existen controles para manejar los resultados y las vulnerabilidades producto de los análisis de riesgos realizados.[18]

Efecto

Las situaciones comentadas tienen el siguiente efecto:

1. No se contribuye, de manera coherente e integrada, al manejo y la regulación efectiva de la infraestructura tecnológica del Gobierno de Puerto Rico.
2. Falta de normas, procedimientos o planes de acción detallados para la recuperación de data tras eventos imprevistos o desastres.
3. Falta de normas, procedimientos o planes acción seguros y detallados ante situaciones de accesos no autorizados y la divulgación, interrupción o destrucción de datos por parte de un usuario, empleado o contratista de la entidad.
4. Falta de normas y procedimientos detallados que garanticen la confidencialidad de la información y la protección de datos de los sistemas de información.
5. Falta de normativas o procedimientos específicos para la disposición de los equipos electrónicos y medios de almacenamiento externos no desarrolladas internamente.

---

[13] Inciso 7.2.10 de la Política para la Seguridad Cibernética, del 29 de octubre de 2021, publicada por PRJTS.
[14] Véase, Inciso 7.3.2 de la Política para la Seguridad Cibernética, del 29 de octubre de 2021, publicada por PRITS.
[15] Véase, la Carta Circular Núm. 2020-05 sobre teletrabajo, del 30 de diciembre de 2020, publicadas por la PRITS.
[17] Incisos 6.1.8 y 7.2.7 de la Política para la Seguridad Cibernética, publicada el 29 de octubre de 2021, por PRITS.
[18] Incisos 6.1.9 y 7.2.8 de la Política para la Seguridad Cibernética, publicada el 29 de octubre de 2021 por PRITS.

6. Falta de protocolos para llevar a cabo análisis de riesgos tecnológicos, de manera periódica, sobre las operaciones de la agencia.
7. Falta de controles para manejar los resultados y las vulnerabilidades producto de los análisis de riesgos realizados
8. Inhabilidad para asegurar la continuidad de las operaciones de los sistemas del DRNA, en caso de contingencias.

POSIBLES DISPOSICIONES LEGALES INFRINGIDAS

Los hechos y hallazgos previamente determinados pudieran representar incumplimientos, por parte del Departamento de Recursos Naturales y Ambientales (DRNA), con las siguientes disposiciones legales:

A. Ley Núm. 75-2019, conocida como *Ley de la Puerto Rico Innovation and Technology Service (PRITS)*

a. Artículo 6 (ee)- El Principal Ejecutivo de Innovación e Información del Gobierno (PEII) será quien evaluará y emitirá recomendación final en los nombramientos de los Principales Oficiales de Informática de las Agencias.

b. Artículo 12 (b) y (d) y (j) - Dispone que las agencias tienen el deber de proveer y divulgar a la PRITS, en el tiempo requerido toda la información, datos, documentos y servicios necesarios y esenciales que les sean requeridos. También, deberán cumplir con las políticas de manejo de información y los estándares tecnológicos promulgados. Parte de los deberes es notificar todo nombramiento de principales oficiales de informática al Principal Ejecutivo de Innovación e Información del Gobierno (PEII) para su evaluación y recomendación final.

B. Ley Núm. 16 de 5 de agosto de 1975, según enmendada, conocida como *Ley de Seguridad y Salud en el Trabajo*

a. Se establece para garantizar condiciones de trabajo seguras y saludables a cada empleado autorizando al Secretario del Trabajo a prescribir y poner en vigor las normas, reglas y reglamentos de seguridad y salud desarrolladas o adoptadas bajo esta ley; asistiendo y estimulando a patronos y empleados en sus esfuerzos por garantizar condiciones de trabajo seguras y saludables.

b. Sección 2. Es su propósito y política garantizar, tanto como sea posible, a cada empleado en el Estado Libre Asociado de Puerto Rico condiciones de trabajo seguras y saludables y preservar nuestros recursos humanos y de esa manera minimizar las desgracias familiares y personales y las pérdidas económicas resultantes de las lesiones y enfermedades del trabajo. Se le confiere al Secretario del Trabajo y Recursos Humanos la responsabilidad y autoridad para poner en

vigor todas las disposiciones de esta ley y todas las normas de seguridad y salud ocupacionales, reglas, reglamentos y órdenes promulgadas bajo las mismas.

c. Sección 4. Esta ley aplicará a todo empleo realizado en cualquier sitio de empleo en el Estado Libre Asociado de Puerto Rico.

d. Sección 6. Cada patrono, como parte de sus deberes, tendrá que proveer a cada uno de sus empleados, un empleo y lugar libre de riesgos reconocidos que estén causando o que puedan causar muerte o daño físico a sus empleados. Además, cada patrono deberá cumplir con las normas de seguridad y salud ocupacionales promulgadas bajo esta ley y con las reglas, reglamentos y órdenes emitidas de acuerdo a las mismas.

C. Orden Administrativa PRITS 2021-003 del 12 de abril de 2021

a. Establece el requisito de uso del Formulario PRITS-002, dentro de un término no mayor de diez (10) días, desde la publicación de la Orden, para todo aquel que ejerza como Oficial Principal de Informática (OPI), o su equivalente. Se deberá proveer al PRITS: Resume o *curriculum* e indicar si el OPI es empleado de carrera en dicha plaza o si es objeto de algún destaque, licencia, etc.

b. No podrá hacerse nombramiento, transferencia o destaque de ninguna persona como OPI sin la previa autorización de PRITS. De lo contrario, estos podrán declararse nulos.

D. *Política para la Seguridad Cibernética*, publicada el 29 de octubre de 2021, por PRITS

a. Incisos 7.2.2, 7.2.3, 7.2.7, 7.2.9 y 7.2.10 - Cada jefe de agencia debe designar un equipo de manejo de riesgos y seguridad cibernética que será responsable de la seguridad cibernética y el manejo de riesgos de la agencia. Las responsabilidades de este equipo incluyen, entre otras, las siguientes:

- Evaluar el riesgo y el impacto que podría resultar del acceso no autorizado, la utilización, divulgación o destrucción de la información o los sistemas de información.
- Determinar los niveles de seguridad cibernética apropiados para proteger la información y sus sistemas mediante las políticas y controles promulgados por el PRITS.
- Realizar pruebas y evaluaciones periódicas de la efectividad de las medidas, procedimientos y prácticas de seguridad cibernética, no menos de una vez al año.
- Desarrollar procedimientos para detectar, reportar y responder a incidentes de seguridad cibernética, que deberán ser consistentes con las políticas, guías y

estándares establecidos por PRITS e incluir la mitigación de los riesgos asociados con tales incidentes, antes de que se produzcan daños sustanciales.

- Diseñar e implementar planes y procedimientos para la recuperación tras desastres y asegurar la continuidad de las operaciones de los sistemas de información que apoyan las operaciones.[19]

b. Inciso 6.1.8 - Cada agencia deberá realizar evaluaciones periódicas del riesgo y la magnitud del daño que podría resultar del acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados de la información y los sistemas que respaldan las operaciones y los activos de la agencia.

c. Incisos 6.1.9 y 7.2.8 - Cada agencia debe establecer controles para prevenir el inicio de ataques cibernéticos desde sus redes internas a otros sistemas de información externos. También, deben desarrollar un proceso para planificar, implementar, evaluar y documentar acciones correctivas que aborden los riesgos a los activos de TI y cualquier deficiencia en las políticas, procedimientos y prácticas de seguridad cibernética de la agencia.

E. Carta Circular Núm. 2020-05 (*Guías para el Programa de Teletrabajo)* del 30 de diciembre de 2020, publicada por la PRITS.

a. Establece que cada Agencia, y su Oficial Principal de Informática (OPI), será responsable de la implementación del Programa de Teletrabajo mediante un plan que considere las exigencias operacionales de la Agencia y de cada empleado participante del Programa. Deberán establecer normas, procedimientos y protocolos detallados que cumplan con la CC Núm. 2020-05 de la PRITS y que garanticen la confiabilidad, seguridad y confidencialidad de la información.

F. Carta Circular Núm. 2021-007 (*Establecimiento de la Política para la Seguridad Cibernética)* del 6 de diciembre de 2021, publicada por la PRITS

a. Una vez que se descubre un incidente o amenaza de seguridad de la información, la agencia deberá notificar inmediatamente al PRITS y enviará un Informe de Incidente de Ciberseguridad que incluirá la información descrita en la *Guía para informar incidentes de ciberseguridad*. De igual forma, las agencias que no son monitoreadas por PRITS deberán enviar informes mensuales de ciberseguridad, con la información requerida en el Acápite 3.8.2 de los Estándares.

G. *Guía para informar incidentes de Ciberseguridad*, publicada por PRITS el 30 de agosto de 2021.

a. Provee instrucciones específicas a seguir para reportar asuntos relacionados con incidentes de ciberseguridad. PRITS ha desarrollado una sección para informar

[19] Incisos 7.2.2, 7.2.3, 7.2.7, 7.2.9 y 7.2.10 de la Política para la Seguridad Cibernética, publicada el 29 de octubre de 2021 por PRITS.

incidentes de ciberseguridad en la herramienta PRITS *Service Desk*. Esto permitirá notificar y documentar todos los eventos de ciberseguridad que hayan resultado en un incidente que represente una violación de las leyes, procedimientos y políticas de seguridad, o que sea una amenaza a los sistemas de información del Gobierno. Este informe será esencial para recopilar información relevante para un posterior análisis basado en los datos históricos proporcionados.

H. Estándares para la Seguridad Cibernética, publicados por PRITS el 29 de octubre de 2021.

a. Incisos 3.8.1.- La agencia notificará a PRITS inmediatamente luego de descubrir un incidente o una amenaza de seguridad y enviará un informe de incidente de ciberseguridad, a tono con la *Guía para informar incidentes de Ciberseguridad.*

CONCLUSIÓN

La evaluación realizada a los documentos y la información recopilada durante la investigación, fue relevante, significativa y suficiente para fundamentar los hallazgos contenidos en el presente informe.

Los controles internos de tecnología son el conjunto de procedimientos y herramientas que se implementan para proteger la información que se genera y procesa a través de servidores, dispositivos, redes y otros sistemas electrónicos. Sirven como una capa de protección para los archivos de información, ante sucesos imprevistos y contingencias. A mayor volumen de actividades producidas a través de redes y dispositivos electrónicos, mayores garantías de seguridad requieren las operaciones. Precisamente, la protección de la infraestructura de la tecnología de la información (*Information Technology* o IT, por sus siglas en inglés) es el proceso de implementar medidas para salvaguardar el entorno tecnológico de una entidad. Es por eso que, la sana y adecuada infraestructura de IT abarca todos los aspectos tecnológicos incluyendo programas (*softwares*) y componentes (*hardware*).

Como resultado de la investigación realizada y de los hallazgos expuestos, la OIG concluye que, no ocurrió un evento o incidente de incendio en el Centro de Cómputos del DRNA, y que las fallas identificadas en los sistemas de información de la entidad fueron como consecuencia de fluctuaciones de voltajes. No obstante, pese a no haber ocurrido el incidente de incendio, la OIG identificó que existe incumplimiento por parte del DRNA, en cuanto al fiel y estricto cumplimiento con las normas y la política pública establecida por el Gobierno de Puerto Rico sobre controles internos y medidas preventivas de seguridad cibernética.

Las situaciones encontradas pudieron, a su vez, haber contribuido a que, posterior al 12 de septiembre de 2022, se hayan interrumpido servicios esenciales dependientes del DRNA provistos al ciudadano, así como a entidades estatales y federales. Esto, provocó un riesgo

considerable de pérdida irreparable de información esencial o privilegiada por no haber desarrollado planes y protocolos sobre mantenimiento preventivo y respuesta, ante riesgos y amenazas.

Esta determinación no limita las prerrogativas de la OIG, de poder realizar referidos a otras agencias fiscalizadoras, así como requerir de cualquier entidad sujeta a nuestra jurisdicción cualquier acción correctiva o de cumplimiento.

RECOMENDACIONES

A la secretaria del Departamento de Recursos Naturales y Ambientales:

1. Hacer los trámites de solicitud presupuestaria para que se restauren los servicios de mantenimiento de equipos y sistemas de información o, en la alternativa, se desarrollen protocolos para proveer mantenimiento estable y periódico, que incluya registros y bitácoras históricas. La alternativa deberá ser la que mejor responda a la austeridad fiscal, sin sacrificar la calidad del servicio.
2. Hacer los trámites de seguimiento suficientes para que las órdenes de compra sobre reparación, mantenimiento o adquisición de equipos o sistemas de información afectados del DRNA puedan ser aprobadas con la mayor celeridad posible.
3. Hacer los trámites necesarios para que se resuelvan los problemas con los generadores del edificio ante fallas eléctricas y se mantengan generadores alternos adecuados. La alternativa deberá ser la que mejor responda a la austeridad fiscal, sin sacrificar la calidad del servicio.
4. Hacer los trámites para que, en un término no mayor de **120 días**, el DRNA cumpla con lo siguiente:
    a. Diseñar e implementar planes y procedimientos para la recuperación tras desastres y asegurar la continuidad de las operaciones de los sistemas de información que apoyen las operaciones y los activos de la agencia.
    b. Diseñar e implementar normas o procedimientos de planes de acción detallados y específicos para la recuperación de data (resguardo o *back-up*) tras eventos imprevistos o desastres y se asegure la continuidad de las operaciones de los sistemas.
    c. Diseñar e implementar normas, procedimientos, planes o protocolos de acción seguros, detallados y específicos para el manejo y la recuperación de datos tras situaciones de accesos no autorizados, divulgación, utilización, interrupción o destrucción de datos por parte de un usuario, empleado o contratista de la entidad.

d. Diseñar e implementar normas y procedimientos detallados que cumplan con la CC Núm. 2020-05 de la PRITS y que garanticen la confiabilidad y confidencialidad de la información, la protección de datos y la seguridad de los sistemas de información.

e. Diseñar e implementar normativas o procedimientos específicos para la disposición de los equipos electrónicos, discos duros, medios de almacenamiento externos y licencias de aplicaciones no desarrolladas internamente.

5. Comenzar gestiones, dentro de un término de 10 días laborables, para que se resuelva cualquier desperfecto en los generadores eléctricos de la agencia para que mantengan un óptimo funcionamiento.

6. Asegurarse de implementar o establecer las medidas necesarias para garantizar condiciones de trabajo seguras y saludables a cada empleado y visitante. Todo ello al amparo y en cumplimiento con todas las normas, reglas y reglamentos de seguridad y salud, estatales o federales, que sean desarrolladas o adoptadas por el secretario del Departamento del Trabajo y Recursos Humanos.

7. Asegurarse de que el director interino de Informática cuente con los recursos o herramientas necesarias para el buen funcionamiento de los sistemas de información y que se garantice la continuidad de las operaciones.

8. Velar por el cumplimiento del director interino en torno a las recomendaciones 9-19 del presente informe.

Al director interino de la Oficina de Informática del Departamento de Recursos Naturales y Ambientales:

9. Asegurarse de cumplir e implementar todas las políticas, procedimientos, estándares y controles promulgados por el PRITS, sin desviaciones a las mismas.

10. Establecer protocolos detallados y por escrito para bridar mantenimiento a los sistemas, equipos y servidores de datos de manera periódica. Asegurarse de que parte de los protocolos consista en que se lleve a cabo un registro histórico de los servicios de mantenimiento llevados a cabo.

11. Asegurarse de que se lleven a cabo análisis de riesgos periódicos, no menos de una vez al año, sobre los sistemas de información que incluyan planes detallados para el manejo de los resultados o las vulnerabilidades producto de los análisis.

12. Realizar pruebas y evaluaciones periódicas de la efectividad de las medidas implementadas, para la protección y seguridad de la infraestructura tecnológica del DRNA, en función del riesgo, no menos de una vez al año.

13. Asegurarse de cumplir con los reportes de incidentes al PRITS inmediatamente se perciba un incidente que pueda representar riesgo a los sistemas de información.

14. Revisar el inventario de equipos, programas y componentes de información del DRNA para crear registros uniformes y detallados que incluyan modelos, fechas de adquisición, capacidad, nombres de manufactureros por cada equipo e identificar cuáles de estos están bajo garantía o contrato mantenimiento.

15. Asesorar al secretario e implementar todas las normativas o procedimientos específicos que sean adoptados por el DRNA para la disposición adecuada de equipos electrónicos, medios de almacenamiento externos y licencias de aplicaciones y para cumplir con las normativas de PRITS, referentes a los sistemas de información.

16. Comenzar gestiones, dentro de un término de 5 días laborables, para corregir cualquier desperfecto existente en el Centro de Cómputos del DRNA (*data center*), también conocido como cuarto de servidores, relacionado al sistema de supresión de incendios.

17. Comenzar gestiones, dentro de un término de 5 días laborables, para evaluar la instalación de sensores para detectar presencia de agua en el "data center".

18. Remover o corregir, dentro de un término de 5 días laborables, todo material o componente que pueda acelerar o agravar los efectos de cualquier falla eléctrica o incendio, de origen externo o interno, provocando un riesgo de seguridad en el "data center", tales como acumulación de cajas de cartón o almacenaje peligroso.

19. Asistir a la secretaria en todo lo relacionado a equipos o sistemas de información para la implementación de las medidas necesarias que garanticen condiciones de trabajo seguras y saludables para cada empleado o visitante. En cumplimiento con todas las normas, reglas y reglamentos de seguridad y salud, estatales o federales, que sean desarrolladas o adoptadas por el secretario del Departamento del Trabajo y Recursos Humanos.

APROBACIÓN

El presente informe es aprobado en virtud de los poderes conferidos por la Ley Núm. 15-2017, antes citada. Será responsabilidad de los funcionarios, empleados o del cuerpo rector del gobierno de cada entidad, observar y procurar que se cumpla cabalmente con la política pública. De la misma manera, establecer los controles y mecanismos adecuados para garantizar su cumplimiento. Además, será el deber de cada uno de estos y de los demás funcionarios y servidores públicos, el poner en vigor las normas, prácticas y estándares que promulgue la OIG, así como de las recomendaciones, medidas y planes de acción correctiva que surjan de las evaluaciones.

Hoy, 19 de diciembre de 2022, en San Juan, Puerto Rico.

Ivelisse Torres Rivera, CFE, CIG
Inspectora General

Lcdo. Francisco J. Rodríguez Pina
Director Interino Área de Querellas e Investigación

INFORMACIÓN GENERAL

Misión

Consolidar los recursos y esfuerzos del Gobierno de Puerto Rico, para promover una sana administración pública y mediante una pre intervención efectiva, el óptimo funcionamiento de sus instituciones.

Visión

Servir como entidad gubernamental reconocida a nivel local e internacional y lograr a través de auditorías internas y acciones preventivas, el funcionamiento efectivo y eficiente d ellos fondos y de la propiedad pública del Gobierno de Puerto Rico.

Confidencias

La Oficina del Inspector General tiene el compromiso de promover una sana administración pública. Por lo que, cualquier persona que tenga información sobre un acto irregular o falta de controles internos en las operaciones de la rama ejecutiva, puede comunicarse a la OIG a través de:

- Línea de Consultas: 787-679-7979
- Correo Electrónico: informa@oig.pr.gov
- Página Electrónica: www.oig.pr.gov/informa

Contactos


PO Box 191733 San Juan, Puerto Rico 00919-1733


Ave. Arterial Hostos 249 Esquina Chardón Edificio ACAA Piso 7, San Juan, Puerto Rico 00918


787-679-7997


consultas@oig.pr.gov


www.oig.pr.gov