CÁMARA DE CUENTAS
DE LA REPÚBLICA DOMINICANA

INFORME DE EVALUACIÓN AL DEPARTAMENTO DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN Y RECURSOS TECNOLÓGICOS DE LA DIRECCIÓN GENERAL DE CONTRATACIONES PÚBLICAS (DGCP)

Por el período comprendido entre el 1. ° de enero de 2017 y el 31 de diciembre de 2020

(OP N.° 003106/2021)

CCRD
CÁMARA DE CUENTAS
DE LA REPÚBLICA DOMINICANA

CÁMARA DE CUENTAS DE LA REPÚBLICA DOMINICANA

INFORME DE EVALUACIÓN AL DEPARTAMENTO DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN Y RECURSOS TECNOLÓGICOS DE LA DIRECCIÓN GENERAL DE CONTRATACIONES PÚBLICAS (DGCP)

Índice de Contenido

CÁMARA DE CUENTAS DE LA REPÚBLICA DOMINICANA

INFORME DE EVALUACIÓN AL DEPARTAMENTO DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN Y RECURSOS TECNOLÓGICOS DE LA DIRECCIÓN GENERAL DE CONTRATACIONES PÚBLICAS (DGCP)

SIGLAS Y ABREVIATURAS

Cámara de Cuentas de la República Dominicana	CCRD
Dirección General de Contrataciones Públicas	DGCP
Dirección de Auditoría de la Cámara de Cuentas	DACC
Tecnología de la Información y Comunicación	TIC
Tecnología de la Información	TI
Objetivos de Control para la Información y Tecnologías Relacionadas	COBIT
Marco Integrado de Control Interno	COSO
Asociación de Auditoría y Control de Sistemas de Información	ISACA
Normas de Tecnología de la Información y Comunicación	NORTIC

INFORME DE EVALUACIÓN AL DEPARTAMENTO DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN Y RECURSOS TECNOLÓGICOS DE LA DIRECCIÓN GENERAL DE CONTRATACIONES PÚBLICAS (DGCP)

Por el período comprendido entre el 1.° de enero de 2017 y el 31 de diciembre de 2020

I. INFORMACIÓN INTRODUCTORIA

1. Antecedentes

La evaluación efectuada al Departamento de Tecnología de la Información y Comunicación y recursos tecnológicos de la **Dirección General de Contrataciones Públicas (DGCP)**, como apoyo a la auditoría financiera se realizó acogiendo las instrucciones dispuestas por la Cámara de Cuentas de la República Dominicana, a través del oficio de la presidencia n.° 003106/2021 de fecha 12 de marzo de 2021, cumpliendo con el Plan Anual de Auditoría, aprobado por el Pleno de Miembros, según decisión n.° DEC-2020-130, de fecha 8 de septiembre de 2020, amparados en el artículo 33 de la Ley 10-04, de fecha 20 de enero de 2004.

2. Objetivos de la evaluación

2.1 Objetivo general

Evaluar los procesos, controles, funcionalidad y seguridad del Departamento de Tecnología de la Información y Comunicación y los recursos tecnológicos de la Dirección General de Contrataciones Públicas (DGCP) y los controles de TI que permitan garantizar la integridad, confidencialidad y disponibilidad de la Información Financiera de la DGCP.

2.2 Objetivos específicos

a) Evaluar el Control Interno de Tecnologías de la Información y Comunicación de las operaciones de la Dirección General de Contrataciones Públicas (DGCP).
b) Verificar las políticas y procedimientos del Departamento de TIC.
c) Verificar los procesos utilizados del aplicativo o Sistema Administrativo Financiero de la entidad.
d) Identificar oportunidades de mejoras en los componentes y características del área de TIC.

3. Alcance de la evaluación

Las consideraciones contenidas en el presente informe se limitan a los procesos, recursos y controles generales del área de TI relacionadas con el Sistema Financiero y Administrativo, los procesos de auditoría realizados por la Cámara de Cuentas abarcaron el período comprendido entre el l. ° de enero de 2017 y el 31 de diciembre de 2020, basada en la facultad que le otorga la Ley n.° 10-04, de fecha 20 de enero de 2004, a la Cámara de Cuentas de la República Dominicana.

3.1. Limitación al alcance

Durante los procedimientos ejecutados en la DGCP no se pudieron completar los procesos iniciados los cuales tuvieron resistencia por el encargado del Departamento de Tecnología de la Información y Comunicación con el apoyo de la Dirección General.

A continuación, detalles de los procedimientos incompletos por la retención de información:

Procedimiento	Fecha	Detalles
Verificación de adquisición de hardware y software para el portal.	16/07/2021	Verificación de los recursos tecnológicos adquiridos para el fortalecimiento del portal de compras y contrataciones públicas en los siguientes contratos anexos. • Contrato de Ejecución de Bienes y Servicios entre MULTICOMPUTOS S.R.L. y la Dirección General de Contrataciones Públicas (SNCC.C.024) • Contrato de Suministro de Bienes y Servicios Conexos entre MULTICOMPUTOS S.R.L. y la Dirección General de Contrataciones Públicas (DGCP-CCC-PEEX-2019-0003 / DGCP-2019-00186) • Contrato de Suministro de Bienes y Servicios Conexos MULTICOMPUTOS S.R.L. y la Dirección General de Contrataciones Públicas (SNCC.C.024 / DGCP-CCC-PEPU-2019-0003 / DGCP-2019-00118)

		• Contrato de Suministro de Bienes y Servicios Conexos MULTICOMPUTOS S.R.L. y la Dirección General de Contrataciones Públicas (DGCP-CCC-PEPU-2020-0002 / DGCP-2020-00075) • Contrato de Suministro de Bienes y Servicios Conexos MULTICOMPUTOS S.R.L. y la Dirección General de Contrataciones Públicas (DGCP-CCC-PEPU-2020-0001 / DGCP-2020-00125) • Contrato de Suministro de Bienes y Servicios Conexos IQTEK SOLUTIONS, S.R.L. y la Dirección General de Contrataciones Públicas (DGCP-CCC-PEPU-2020-0001 / DGCP-2020-00082) • Contrato de Suministro de Bienes y Servicios Conexos IQTEK SOLUTIONS, S.R.L. y la Dirección General de Contrataciones Públicas (DGCP-CCC-PEPU-2019-0002 / DGCP-2019-00127) • Contrato de Suministro de Bienes y Servicios Conexos IQTEK SOLUTIONS, S.R.L. y la Dirección General de Contrataciones Públicas (SNCC.C.024 / DGCP-2018-00112) En el procedimiento de levantamiento de información se realizó una inspección en las instalaciones del 911 en donde la Dirección General de Contrataciones Públicas tiene hospedado el Portal de Compras y Contrataciones Públicas. Se procedió a realizar un levantamiento de evidencia, que incluyen fotografías de los equipos en cuestión.
Entrevista de Entendimiento con el Encargado de Tecnología de la Información y Comunicación	28/07/2021	Procedimiento realizado para detallar el conocimiento general del Departamento de Tecnología de la Información y Comunicación DTIC de la Dirección General de Contrataciones

		Públicas (DGCP) como parte del proceso de evaluaciones sustantivas.
Inspección Física al Centro de Procesamiento de Datos (Data Center)	29/07/2021	Evaluación de las políticas, procedimientos y componentes que conforman el Centro de Datos o Data Center de la Dirección de Contrataciones Públicas (DGCP). Aplicación de Check List (Lista de Chequeo) de los componentes que conforma e integran al centro de datos o Data Center. Fotografías de centro de datos o Data Center
Gestión de las Cuentas Usuarios del Active Directory	29/07/2021	Evaluación de los procedimientos de administración y gestión de los usuarios de Active Directory. Evaluación de las políticas, procedimientos y parametrización de las cuentas de usuarios en el Active Directory
Extracción de Logs de Servidor que hospeda el servicio de Active Directory	29/07/2021	Procedimiento con la herramienta DUMPSEC de extracción de logs del servidor de Active Directory (AD) de Grupos, Políticas, Servicios y Usuarios para el análisis y evaluación del mismo

4. Definición y objetivos específicos del control interno

La Ley n.° 10-07 artículo 24 y su reglamento de implementación n.° 491-07, exigen a las entidades públicas aplicar los lineamientos del marco integrado de Control interno del COSO (Committee of Sponsoring Organizations of the Treadway Commission).

Dicho marco, define el Control Interno como un proceso efectuado por el Consejo de Administración, la Dirección y el resto del personal de una empresa, diseñado para proporcionar una razonable seguridad respecto al logro de objetivos, dentro de las siguientes categorías:

a) Eficiencia y eficacia de las operaciones.
b) Confiabilidad de la información financiera.
c) Cumplimiento con las leyes y normas aplicables.

El marco "Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT), Control Objectives for Information and Related Technology por sus siglas en inglés, alineado al marco COSO, permite cumplir de manera integral con las exigencias de la Ley.

Esta convergencia COBIT-COSO no solo agrega valor en lo relativo a Gestión de las Tecnologías de la Información y las Comunicaciones, sino también en torno a las prácticas de planeación estratégica, estructura organizacional, cultura de control, seguridad, gestión presupuestal, gestión de personal, gestión de la calidad, gestión de los riesgos, gestión de los servicios, entre otros.

De manera específica, el propósito de las prácticas de COBIT es ser habilitadoras para la planificación, adquisición, administración, soporte y monitoreo de la Tecnología de la Información que sostienen los procesos de la entidad.

5. Componentes del control interno

A partir de la alineación COBIT-COSO elaborada por la Asociación de Auditoría y Control de Sistemas de Información (ISACA) por sus siglas en inglés *"Information Systems Audit and Control Association"*, mostramos en detalle las prácticas comunes con cada uno de los componentes del marco COSO.

1. Componente de Ambiente de Control:

a) Plan estratégico y operativo de informática.
b) Estructura organizacional de informática.
c) Segregación de funciones de las áreas críticas de Informática.
d) Ambiente de control y administración de políticas informáticas.
e) Reclutamiento y retención del personal.
f) Entrenamiento del personal.
g) Evaluación del desempeño.
h) Evaluación de la gestión informática.
i) Monitoreo y evaluación del control interno informático.
j) Administración de la calidad.
k) Administración de los proyectos.

2. **Componente de Valoración y administración de Riesgos:**

a) Evaluación de riesgos tecnológicos.
b) Respuestas a los riesgos.
c) Plan de acción de tratamiento de los riesgos.

3. **Componente de Actividades de Control:**

a) Administración de los usuarios que ingresan a la red de datos y a los sistemas de la entidad.
b) Pruebas, vigilancia y monitoreo de la seguridad de los equipos e informaciones.
c) Administración de documentos sensitivos y dispositivos de salida.
d) Prevención, detección y corrección de software malicioso y virus en las redes.
e) Seguridad de la red de datos, detección y prevención de intrusos.
f) Seguridad física de los centros de datos y áreas críticas.
g) El monitoreo, medición y reporte del desempeño y la capacidad tecnológica.

4. **Componente de Información y Comunicación:**

a) Mesa de ayuda de los servicios tecnológicos.
b) Acuerdos de niveles de servicios tecnológicos.
c) Administración de integridad de la información.
d) Almacenamiento, respaldo y conservación de la información.
e) Administración de incidentes de seguridad de la información.
f) Administración de problemas tecnológicos.
g) Administración de la continuidad de las operaciones y la recuperación de desastres.
h) Administración de las operaciones.

6. Marcos y estándares de control interno informático aplicados en la auditoría de TI

La evaluación al Departamento de Tecnología de la Información y Comunicación y recursos tecnológicos de la Dirección General de Contrataciones Públicas (DGCP), como apoyo a la auditoría financiera se efectuó considerando los marcos de control y estándares de buenas prácticas reconocidos a nivel nacional e internacional como:

- ***COBIT*** *(Objetivos de Control para Información y Tecnologías Relacionadas, en inglés: Control Objectives for Information and related Technology).*
- ***ITIL*** *(Biblioteca de Infraestructura de Tecnología de Información, en inglés: Information Technology Infrastructure Library).*
- ***ISO*** *(Organización Internacional de Normalización, en inglés: International Standarization Organization).*
- **ANSI/TIA-942-A** *(La Asociación de la Industria de Telecomunicaciones, Norma de Infraestructura de Telecomunicaciones para Centros de Datos, en inglés: (The Telecommunications Industry Association (TIA) Telecommunications Infrastructure Standard for Data Centers is an American National Standard (ANS)*
- **NORTIC** *(Normas de Tecnologías de la Información y Comunicación, creadas en el año 2013 por el Departamento de Estandarización, Normativa y Auditoria Técnica (ENAT).*

II. RESULTADOS DE LA EVALUACIÓN

2.1 Debilidades y vulnerabilidades de gestión del Departamento TIC

Al momento de la fiscalización y mediante la aplicación del cuestionario de Evaluación de Gestión TI, de fecha 5 de octubre de 2021, en el Departamento de TIC se comprobó que existen debilidades y vulnerabilidades de gestión, citadas a continuación:

a. Ausencia de un mecanismo para evaluar la situación actual tecnológica de la DGCP.
b. No se cuenta con los planes de contingencia, continuidad de negocio y recuperación de desastres acorde con la situación actual de la DGCP.
c. El departamento de TIC no cuenta con los recursos necesario para el desarrollo e implementación de proyecto (s) acorde con una metodología basadas en buenas prácticas.
d. El departamento de TIC no cuenta con un área para evaluar la calidad (QA) de los proyectos tecnológicos llevados a cabo en la DGCP.
e. El departamento de TIC no ha creado e implementado los mecanismos que le permitan desplegar una gestión de cambio en las contraseñas de las cuentas de servicios que afectan las áreas sensitivas y críticas de la DGCP.
f. El departamento de TIC no ha creado e implementados los mecanismos para garantizar una efectiva segregación de las funciones entre las áreas que conforman el departamento TIC.

El marco de evaluación de Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT 2019), en el proceso APO01. Gestionar el Marco de Gestión de la TI, expresa:

"Aclarar y mantener el gobierno de la misión y la visión corporativa de TI. Implementar y mantener mecanismos y autoridades para la gestión de la información y el uso de TI en la empresa para apoyar los objetivos de gobierno en consonancia con las políticas y los principios rectores".

Además, en la práctica de gestión APO01.03 Mantener los elementos catalizadores del sistema de gestión, y sus actividades respectivamente expresan:

"Mantener los elementos catalizadores del sistema de gestión y del entorno de control de la TI de la empresa y garantizar que están integrados y alineados con la filosofía y el estilo operativo de gobierno y de gestión de la empresa. Estos elementos catalizadores incluyen una comunicación clara de expectativas/requisitos. El sistema de gestión debería fomentar la cooperación interdepartamental y el trabajo en equipo, promover el cumplimiento y la mejora continua y tratar las desviaciones en el proceso (incluidos los fallos)".

"1. Adquirir comprensión de la visión, la dirección y la estrategia corporativas.
3. Inferir e integrar los principios de TI con los principios de negocio.
4. Alinear el entorno de control con el entorno de políticas de TI, con los marcos de trabajo generales de gobierno de TI y procesos de TI y los marcos de trabajo existentes a nivel corporativo en cuanto a riesgo y control. Evaluar las buenas prácticas o los requisitos específicos del sector (p. ej., normativa específica del sector) e integrarlos donde corresponda.
6. Crear un conjunto de políticas para conducir las expectativas de control de TI en temas clave relevantes, como calidad, seguridad, confidencialidad, controles internos, uso de activos de TI, ética y derecho de propiedad intelectual.
7. Evaluar y actualizar las políticas, como mínimo una vez al año, para ajustarlas a los cambiantes entornos operativo o de negocio.
8. Implantar y aplicar las políticas de TI a todo el personal relevante, de forma que estén incorporadas y sean parte integral de las operaciones empresariales.
9. Asegurarse de que los procedimientos estén en funcionamiento para realizar un seguimiento del cumplimiento con las políticas y definir las consecuencias de la no conformidad".

Así mismo en la práctica de gestión APO01.05 Optimizar la ubicación de la función TI y sus actividades, expresa:

"Posicionar la capacidad de TI en la estructura organizativa global para reflejar en el modelo de empresa la importancia de TI en la organización, especialmente su criticidad para la estrategia empresarial y el nivel de dependencia de TI. La línea de reporte de CIO debe ser proporcional a la importancia de las TI en la empresa".

1. *"Entender el contexto de la función de TI, incluyendo una evaluación de la estrategia empresarial y el modelo operativo (centralizado, federado, descentralizado, híbrido), importancia de TI, la situación y opciones para la provisión.*
2. *Identificar, evaluar y priorizar las opciones para la ubicación en la organización, los modelos operativos y de aprovisionamiento.*
3. *Definir la ubicación de la función de TI y obtener aprobación".*

También, en la práctica de gestión APO01.07 Gestionar la mejora continua de los procesos y sus actividades expresa:

"Evaluar, planificar y ejecutar la mejora continua de procesos y su madurez para asegurar que son capaces de entregarse conforme a los objetivos de la empresa, de gobierno, de gestión y de control. Considerar las directrices de la implementación de procesos de COBIT, estándares emergentes, requerimientos de cumplimiento, oportunidades de automatización y la realimentación de los usuarios de los procesos, el equipo del proceso y otras partes interesadas. Actualizar los procesos y considerar el impacto en los catalizadores del proceso".

1. *"Identificar los procesos críticos de negocio basándose en el rendimiento, cumplimiento y los riesgos relacionados. Evaluar la capacidad del proceso e identificar objetivos de mejora. Analizar las diferencias en la capacidad y control del proceso. Identificar las opciones de mejora y rediseño de procesos. Priorizar iniciativas para la mejora de procesos basadas en el potencial coste-beneficio.*
2. *Implementar las mejores acordadas, funcionando como una práctica normal del negocio y establecer objetivos y métricas de rendimiento que permitan el seguimiento de las mejoras del proceso.*
3. *Considerar las maneras de mejorar la eficiencia y eficacia (p. eje., mediante formación, documentación, estandarización y automatización de procesos).*
4. *Aplicar prácticas de gestión de calidad para la actualización de procesos.*
5. *Retirar procesos, componentes o catalizadores desactualizados".*

En adición, en la práctica de gestión APO01.08 Mantener el cumplimiento con las políticas y procedimientos y sus actividades, expresa:

"Poner en marcha procedimientos para mantener el cumplimiento y medición del funcionamiento de las políticas y otros catalizadores del marco de referencia; hacer cumplir las consecuencias del no cumplimiento o del desempeño inadecuado. Seguir las tendencias y el rendimiento y considerarlos en el diseño futuro y la mejora del marco control".

1. *"Hacer un seguimiento del cumplimiento con políticas y procedimientos.*
2. *Analizar los incumplimientos y adoptar las acciones apropiadas (puede incluir cambio de requerimientos).*
3. *Integrar rendimiento y cumplimiento dentro de los objetivos individuales del personal.*

4. *Evaluar periódicamente el desempeño de los catalizadores del marco de referencia y adoptar las acciones necesarias.*

5. *Analizar las tendencias en el funcionamiento y cumplimiento y adoptar las acciones apropiadas ".*

El encargado de TIC vía correo electrónico de fecha 22 de octubre de 2021 con el título: Acceso | Auditoría Cámara de Cuenta - Solicitud de datos y comprobantes, solicitud n.° 45 - Informaciones varias, nos responde:

"Existe una iniciativa mediante el Plan de recuperación de desastres del año 2016, aunque no existe un marco institucional establecido". Ver documento "DRP-TIC-V05.pdf"

La DGCP no cuenta con planes de contingencia, recuperación de desastres y continuidad de negocio, metodología o plan de desarrollo de proyecto, evaluación de la calidad de los proyectos tecnológicos en general y segregación de las diferente divisiones o departamento que conforman la Dirección de Tecnología de la Información y Comunicación.

Recomendaciones:

Al director general le corresponde,

1. Garantizar la gestión eficiente de la Dirección de Tecnología de la Información y Comunicación basada en buenas prácticas y normativas.

2. Instruir al director de TIC a la creación de un plan que le permita a la Dirección de Tecnología de la Información y Comunicación identificar los riesgos tecnológicos que pudieran afectar a la DGCP.

3. Exigir a la Dirección de Tecnología de la Información y Comunicación la correcta segregación de funciones y la calidad de los procedimientos realizados.

4. Garantizar la disponibilidad de los servicios críticos gestionado desde la Dirección de Tecnología de la Información y Comunicación.

Reacción de la ex administración de la entidad:

Mediante comunicación de réplica de fecha 16 de septiembre de 2022, Yokasta Altagracia Guzmán, cédula de identidad y electoral, n.° 001-0081375-7, exdirectora general de la Dirección General de Contrataciones Públicas, expresa:

"Es importante destacar que en agosto del año 2012 no existía un departamento, unidad o área de Tecnología de la Información. Es por ello que desde el año 2013 se iniciaron los trabajos necesarios para la creación del Departamento TIC, realizando las siguientes actividades incluidas de manera histórica para que las autoridades cuenten con toda la información relativa a este punto:

1) *Se contrató un auditor informático certificado que realizó lo siguiente:*
   a. *Diagnóstico en mayo del 2013.*
   b. *Evaluación inicial de la gobernabilidad de las Tecnologías de la Información, diciembre 2013.*
   c. *Análisis de Brechas entre COBIT 5 y la situación actual, enero 2014.*
   d. *Evaluación Final de la gobernabilidad de TI, julio 2014*
   e. *Análisis de Brechas entre COBIT 5 y la situación actual, octubre 2015.*
   f. *Análisis de Brechas entre COBIT 5 y la situación actual, marzo 2016.*
   g. *Evaluación sobre la aceptación y puesta en funcionamiento de la plataforma tecnológica del Portal Transaccional, abril 2016.*
2) *Se contrató un Auditor de Sistemas a tiempo completo en el 2015 (Alexander Luna – Ver perfil de puesto).*
3) *Se contrató a la firma ARGENTUM para realizar una auditoría al Portal Transaccional, incluyendo sus códigos fuentes de 2018 a 2019.*
4) *Con recursos del BID se contrató un consultor (Licdo. Alejandro Barros) para evaluar el Portal Transaccional, julio 2019.*
5) *Se creó un Comité de Tecnología, 2020. Favor ver informe de los procesos y servicios internos de Tecnología, que incluyen recomendaciones de mejoras en el flujo de los distintos procesos (realizado por el Consultor Ing. Juan Díaz).*

Los documentos y los informes relativos a la contratación de estos consultores se encuentran en los archivos institucionales.

1. *Durante el período enero – abril del 2016, se elaboró un Plan de Continuidad Servicios de la institución, el cual hasta agosto de 2020 se mantenía actualizado por el personal del Departamento Tecnología de la Información.*
2. *Previo al cambio de Administración se elaboraron ocho Términos de Referencia para que las nuevas autoridades contrataran equipos adicionales para la continuidad de operaciones.*

EL
ES

a) *DGCP – TDRs – Portal Transaccional – 01 Dimensionamiento Equipamiento y Replicación.*
b) *DGCP – TDRs – Portal Transaccional – 02 Adquisición Equipamiento.*
c) *DGCP – TDRs – Portal Transaccional – 03 Renta Alojamiento.*
d) *DGCP – TDRs – Portal Transaccional – 04 Implementación de la replicación en tiempo real.*
e) *DGCP – TDRs – Interno – 01 Dimensionamiento equipamiento y replicación.*
f) *DGCP – TDRs – Interno – 02 Adquisición equipamiento.*
g) *DGCP – TDRs – Interno – 03 Renta Alojamiento.*
h) *DGCP – TDRs – Interno – 04 implementación de la replicación en tiempo real.*

Ver Términos de Referencia del Plan de Continuidad Tecnológico y Sostenibilidad del Portal Transaccional y TIC (realizado por el Consultor Ing. Juan Díaz). La consultoría finalizo en Julio 2020 y se tenía planificado ejecutarlo con presupuesto de TIC del 2021.
Los mencionados documentos reposan en el archivo institucional.

1) *El Gobierno y Gestión de TIC se realizó de acuerdo con los lineamientos de COBIT.*
2) *Hasta agosto de 2020 se disponía de un Gerente de Proyectos (Leandro Altuzarra) a tiempo completo.*
3) *Hasta agosto de 2019 se disponía de un Auditor de Tecnología (Alexander Luna) a tiempo completo.*

Ver "Informe referente a la carga operativa y dimensionamiento de TIC", que incluye las mejores prácticas. De igual forma, el mencionado documento contiene un levantamiento de puestos y manual de funciones de los distintos colaboradores y áreas necesarias para llevar adelante la operación de TIC y del Portal Transaccional como Sistema de Emisión Crítica, con el fin de dimensionar el departamento de TIC (realizado por el Consultor Ing. Juan Díaz). Adicional a esto, el departamento contaba con la posición de Gerente de Proyecto (Anteriormente función que llevaba a cabo el Licdo. Leandro Altuzarra y posteriormente se sumó como Analista de Proyecto la Licda. Anllelina Familia).
Los mencionados documentos reposan en el archivo institucional.

1. *El Gobierno y Gestión de TIC se realizó de acuerdo con los lineamientos de COBIT.*
2. *Hasta agosto de 2020 se disponía de un Gerente de Proyectos (Leandro Altuzarra) a tiempo completo.*

3. *Hasta agosto de 2019 se disponía de un Auditor de Tecnología (Alexander Luna) a tiempo completo.*

4. *Hasta agosto de 2020 se disponía de una unidad para controlar la calidad de los sistemas y un Líder de Control de Calidad de Software.*
5. *Hasta agosto de 2020 se disponía de Procedimientos y Esquemas de pruebas minuciosos para el pase a producción de los sistemas.*

El Departamento de TIC cuenta con un área de QA, liderado por el Ing. Erasmo Aquino. Contratado originalmente como Líder de QA (Coordinador) del Portal Transaccional y luego se le incorporaron funciones de Calidad en TIC.

Los mencionados documentos reposan en el archivo institucional.

1. *Se crearon Procedimientos de Tecnología, 2014. (Ver repositorio de origen documental en el Departamento de TIC, ubicación donde reposan todas las políticas, procedimientos, reglamentos y manuales del Departamento de Tecnología de la Información de la institución. En adición, el Departamento de Planificación y Desarrollo tiene evidencias de toda las políticas, procedimientos y reglamentos vigentes, firmados por la máxima autoridad de la institución).*

2. *Se actualizaron los Procedimientos de Tecnología, incluyendo los de Seguridad, 2019. (Ver repositorio de origen documental en el Departamento de TIC, ubicación donde reposan todas las políticas, procedimientos, reglamentos y manuales del Departamento de Tecnología de la Información de la institución. En adición, el Departamento de Planificación y Desarrollo tiene evidencias de toda las políticas, procedimientos y reglamentos vigentes, firmados por la máxima autoridad de la institución).*

3. *Se disponía en la estructura de TIC de un Coordinador de Seguridad Informática (Ing. Eddy Acevedo).*

El área de Seguridad TIC, liderado por Ing. Eddy Acevedo, tenía las funciones de velar por la Seguridad TIC tanto del Portal Transaccional como de la Plataforma Institucional.

Los mencionados documentos reposan en el archivo institucional.

1. *Se definió una estructura funcional para Tecnología, alineada con los requerimientos del Ministerio de Administración Pública (MAP), la Oficina Presidencial de Tecnología de la Información y Comunicaciones (OPTIC) y COBIT, 2014.*

2. *Se actualizaron las descripciones de puesto, 2016. Ver repositorio de origen documental en el Departamento de TIC, ubicación donde reposan todas las políticas, procedimientos, reglamentos y manuales del Departamento de Tecnología de la Información de la institución. En adición, el Departamento de Planificación y Desarrollo tiene evidencias de toda las políticas, procedimientos y reglamentos vigentes, firmados por la máxima autoridad de la institución).*

3. *Se definió una estructura funcional para Tecnología, alineada con los requerimientos del Ministerio de Administración Pública (MAP), la Oficina Presidencial de Tecnología de la Información y Comunicaciones (OPTIC) y COBIT, 2019.*

4. *Se elaboró una matriz de comparación de funciones entre áreas comparado con los lineamientos de COBIT 2019, 2019.*

5. *Se actualizó la matriz de comparación de funciones entre áreas comparado con los lineamientos de COBIT 2019, 2020.*

6. *La estructura aprobada mediante Resolución Núm. 1084-2020 contempla las estructuras del Departamento TIC, separadas de las del Portal Transaccional.*

Ver informe de procesos y funciones de las distintas áreas de TIC (realizado por el Ing. Juan Díaz).

Los mencionados documentos reposan en el archivo institucional".

Comentarios y conclusiones de los auditores de la CCRD

Luego de una revisión exhaustiva y en vista a la carencia de información necesaria en la que se pudiera ver la subsanación se mantiene la observación en el informe.

2.2 Revisión y/o actualización de las políticas y procedimientos de TIC

Durante los procedimientos realizados en la DGCP al Departamento de TIC, comprobamos que las políticas y procedimientos generales de TIC, al momento de la auditoría, se

encuentran desactualizadas, realizándose la última revisión y/o creación en el año 2015. A continuación, se cita el listado de las políticas encontradas en esa condición:

a. DGCP.POL-DTI-GT01-Política General de Gestión de Tecnología V33 - JT-AOR (14/08/2015).
b. DGCP.POL-DTI-IF02-Política de Uso Aceptable Infraestructura para Usuarios V33 - JT-AOB (14/08/2015).
c. DGCP POL-DTI-CE03-Política de Uso Aceptable para Correo Electrónico V26 – JT (03/06/2015).
d. DGCP.POL-DTI-AI04-Política de Uso Aceptable para Internet V32 – JT (14/08/2015).
e. DGCP.POL-DTI-RI08-Política sobre las copias resguardo de la Información V22-AOR (03/07/2015).
f. DGCP.POL-DTI-MA07-Política de la Mesa de Servicios V32-AOR (14/08/2015).
g. DGCP.POL-DTI-UA06-Política de Uso de Antivirus V31 (14/08/2015).
h. DGCP-POL-DTI-091-Políticas de Contraseñas v21 (03/07/2015).
i. DGCP.POL-DTI-RT05-Política de Propiedad de los Recursos Tecnológicos V32-AOR (14/08/2015).
j. DGCP.POL-DTI-CS10-Política de Control de Acceso al Cuarto de Servidores V22-AOR (03/07/2015).
k. DGCP-POL-DTI-061-Política sobre dispositivos móviles y teletrabajo V31 (14/08/2015).
l. DGCP-POL-DTI-111-Política de Eliminación y Destrucción V21 (03/07/2015).
m. DGCP-POL-DTI-171-Política de la Continuidad del Negocio V21 (03/07/2015).
n. DGCP.POL-DTI-SA09-Política Desarrollo e Implementación de Sistemas y Aplicativo V31 (22/09/2015).
o. DGCP-POL-DTI-151-Política de Seguridad para Proveedores V21 (03/07/2015).

Las políticas en su mayoría no cuentan con un procedimiento que indique como deben de ser ejecutadas las políticas concebidas en el departamento de TIC para la DGCP.

El marco de evaluación de Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT 4.1), en los procedimientos PO6.1 Ambiente de Políticas y de Control, PO6.3 Administración de Políticas para TI, PO6.4 Implantación de Políticas de TI, PO6.5 Comunicación de los Objetivos y la Dirección de TI establecen:

"PO6.1 Ambiente de Políticas y de Control. - Definir los elementos de un ambiente de control para TI, alineados con la filosofía administrativa y el estilo operativo de la empresa. Estos elementos incluyen las expectativas / requerimientos respecto a la entrega de valor proveniente de las inversiones en TI, el apetito de riesgo, la integridad, los valores éticos, la competencia del personal, la rendición de cuentas y la responsabilidad. El ambiente de control se basa en una cultura que apoya la entrega de valor, mientras administra riesgos significativos, fomenta la colaboración entre divisiones y el trabajo en equipo, promueve el cumplimiento y la mejora continua de procesos, y maneja las desviaciones (incluyendo las fallas) de forma adecuada".

"PO6.3 Administración de Políticas para TI.- Elaborar y dar mantenimiento a un conjunto de políticas que apoyen la estrategia de TI. Estas políticas deben incluir su intención, roles y responsabilidades, procesos de excepción, enfoque de cumplimiento y referencias a procedimientos, estándares y directrices. Su relevancia se debe confirmar y aprobar en forma regular".

"PO6.4 Implantación de Políticas de TI.- Asegurarse de que las políticas de TI se implantan y se comunican a todo el personal relevante, y se refuerzan, de tal forma que estén incluidas y sean parte integral de las operaciones empresariales".

"PO6.5 Comunicación de los Objetivos y la Dirección de TI.- Asegurarse de que la conciencia y el entendimiento de los objetivos y la dirección del negocio y de TI se comunican a los interesados apropiados y a los usuarios de toda la organización".

La Dirección de Tecnología de la Información y Comunicación no cuenta con un plan de revisión de las políticas y procedimiento TIC que le permita estar acordes a las necesidades actuales de la DGCP.

Recomendaciones:

Al director general le corresponde,

1. Garantizar desde la Dirección de Tecnología de la Información y Comunicación el análisis, diseño e implementación de los controles que le permita la gestión y gobernabilidad de los recursos tecnológicos basados en buenas prácticas.

2. Instruir a las diferentes direcciones en combinación con la Dirección de Tecnología de la Información y Comunicación a diseñar, crear e implementar las políticas y procedimientos que le permitan el crecimiento y fortalecimiento institucional.

3. Aprobar las políticas de TICs e instruir al Comité de TICs a la revisión, aprobación y difusión de las mismas en la entidad.

Reacción de la ex administración de la entidad:

Mediante comunicación de réplica de fecha 16 de septiembre de 2022, Yokasta Altagracia Guzmán, cédula de identidad y electoral, n.° 001-0081375-7, exdirectora general de la Dirección General de Contrataciones Públicas, expresa:

1. *Se elaboraron un conjunto de políticas para TIC en el 2015, las cuales se mantuvieron en uso, debido a que fueron elaboradas alineadas con COBIT y se mantuvo su pertinencia.*
2. *Se crearon los Procedimientos de Tecnología, 2014.*
3. *Se actualizaron los Procedimientos de Tecnología, incluyendo los de Seguridad, 2019.*

Las Políticas fueron creadas en el año 2015, actualizadas y socializadas por el Consultor Ing. Juan Díaz a las áreas internas de la Institución. También se habilitó el espacio de "Gobierno TIC" para tratar estos temas y todo lo referente" a Tecnología de la Información que afecte a la Institución. Ver acuerdo firmado por la Dirección General en Julio 2020 y que debe dársele continuidad en la nueva gestión.

Los mencionados documentos reposan en el archivo institucional".

Comentarios y conclusiones de los auditores de la CCRD

Luego de una revisión exhaustiva y en vista a la carencia de información necesaria en la que se pudiera ver la subsanación se mantiene la observación en el informe.

2.3 El Departamento de TIC no cuenta con una herramienta o matriz de riesgo

En la realización de procedimientos aplicados en el mes de octubre de 2021 al Departamento TIC de la DGCP, se verificó que no cuentan con una herramienta o matriz que le permita identificar cuáles son los riesgos a los que están expuestos y el grado en que afectarían las

operaciones del Departamento TIC y la DGCP a nivel general. De igual manera no tienen identificadas cuales son las áreas más sensitivas e incidencias más comunes que se presenta en la entidad.

La Norma para la Seguridad de las Tecnologías de la Información y Comunicación en el Estado Dominicano NORTIC A7 de 2016, en su sección 4.02 Plan de continuidad, literal j y su sub-literal (iv), establece:

"(j) Debe tomarse en cuenta los siguiente para la prueba, mantenimiento y re-evaluación del plan de continuidad del organismo:

(iv) Deben verificarse las siguientes informaciones del plan al momento de su revisión:

- *Personal responsable del plan y personal alternativo.*
- *Direcciones y números de contacto.*
- *Alineación del plan con la estrategia organizacional.*
- *Locales y/o sucursales.*
- *Proveedores de servicios y clientes.*
- *Procesos, tanto nuevos como actualizados o eliminados.*
- *Evaluación de riesgo".*

La referida Norma NORTIC A7 de 2016, en su sección 4.02.3 Pruebas y simulacros, literales y sub-literales, establece:

"(a) El CONTI solo debe ser considerado como completado cuando se ha realizado una prueba funcional del mismo, se han validado los resultados y realizados los ajustes necesarios a fin de que cumpla con los objetivos identificados durante su fase de diseño.

(b) La forma de medir que el plan ha sido completado es mediante el informe del comité del CONTI informando a la máxima autoridad, la cual, luego de revisarla hará las observaciones de lugar y dará por completado el proceso de implantación inicial mediante firma de que los objetivos han sido logrados.

(c) Los organismos gubernamentales deben generar periódicamente informes sobre la ejecución y estado de su plan de continuidad.

(i) *Los organismos gubernamentales deben tomar en cuenta lo siguiente para sus evaluaciones periódicas del plan de continuidad:*

- *Análisis sobre nuevos riesgos y los impactos de los mismos.*
- *Revisión del impacto económico asociado al plan de continuidad.*
- *Evaluación sobre los simulacros del plan de continuidad.*
- *Capacitación del personal del departamento de TIC para llevar a cabo el plan de continuidad.*

El marco de evaluación de Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT 2019), en el proceso APO12 Gestionar el Riesgo, en la práctica de gestión APO12.06 Responder al riesgo y sus actividades, en el proceso DSS04 Gestionar la Continuidad, práctica de gestión DSS04.04 Ejercitar, probar y revisar el BCP y sus actividades expresan:

"APO12 Gestionar el Riesgo. - Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de los niveles de tolerancia establecidos por la dirección ejecutiva de la empresa".

APO12.06 Responder al riesgo, y sus actividades expresan respectivamente:

"Responder de una forma oportuna con medidas efectivas que limiten la magnitud de pérdida por eventos relacionados con TI".

1. *"Preparar, mantener y probar planes que documenten los pasos específicos a tomar cuando un evento de riesgo pueda causar un incidente significativo operativo o evolucionar en un incidente con un impacto de negocio grave. Asegurar que los planes incluyan vías de escalado a través de la empresa.*
2. *Categorizar los incidentes y comparar las exposiciones reales con los umbrales de la tolerancia al riesgo. Comunicar los impactos en el negocio a los responsables de toma de decisiones como parte de la notificación y actualizar el perfil de riesgo.*
3. *Aplicar el plan de respuesta apropiado para minimizar el impacto cuando ocurren incidentes de riesgo.*
4. *Examinar eventos, adversos/pérdidas del pasado y oportunidades perdidas y determinar sus causas raíz. Comunicar la causa raíz, requerimientos de respuesta adicionales para el riesgo y mejoras de proceso a los responsables de toma de decisiones apropiados y asegurarse de que la causa, los requerimientos de respuesta y la mejora del proceso se incluyan en los procesos de gobierno del riesgo".*

DSS04 Gestionar la Continuidad, práctica de gestión DSS04.04 Ejercitar, probar y revisar el BCP y sus atividades expresan:

"DSS04 Gestionar la Continuidad, práctica de gestión. - Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa".

"DSS04.04 Ejercitar, probar y revisar el BCP. - Probar los acuerdos de continuidad regularmente para ejercitar los planes de recuperación respecto a unos resultados predeterminados, para permitir el desarrollo de soluciones innovadoras y para ayudar a verificar que el plan funcionará, en el tiempo, como se espera".

1. *"Definir los objetivos para ejercitar y probar los sistemas del plan (de negocio, técnicos, logísticos, administrativos, procedimentales y operacionales) para verificar la completitud del plan de continuidad de negocio (BCP) para enfrentarse a los riesgos de negocio.*
2. *Definir y acordar ejercicios que sean razonables con las partes interesadas, validar los procedimientos de continuidad, e incluir roles y responsabilidades y acuerdos de retención de datos que ocasionen la mínima disrupción en los procesos de negocio.*
3. *Asignar roles y responsabilidades para realizar ejercicios y pruebas del plan de continuidad.*
4. *Planificar ejercicios y actividades de prueba tal como esté definido en el plan de continuidad.*
5. *Realizar un análisis y revisión post-ejercicio para considerar el logro.*
6. *Desarrollar recomendaciones para mejorar el plan de continuidad actual en base a los resultados de revisión".*

El Estándar para la Seguridad de la Información de la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional ISO/IEC 27002, en el dominio 17, sobre Seguridad de la Información en la Gestión de la Continuidad del Negocio en los diferentes Objetivos de Control y Controles, establece:

"Analizar las consecuencias de los desastres, falla de seguridad, perdidas de servicio y la disponibilidad del servicio y desarrollar e implantar planes de contingencia para asegurar que los procesos del negocio se pueden restaurar en los plazos requeridos las operaciones esenciales, manteniendo las consideraciones en seguridad de la información utilizada en los planes de continuidad y función de los resultados del análisis de riesgos.

EL
ES

17.1 Continuidad de la seguridad de la información: El objetivo es que la seguridad de la información sea integrada en los sistemas de gestión de la continuidad del negocio de la organización.

17.1.1 Planificación de la continuidad de la seguridad de la información: La organización debería determinar los requisitos para la seguridad de la información y su gestión durante situaciones adversas como situaciones de crisis o de desastre".

El encargado de TIC vía correo electrónico de fecha 22 de octubre de 2021 con el título: Acceso | Auditoría Cámara de Cuenta - Solicitud de datos y comprobantes Solicitud n.° 45 - Información varias, nos responde:

"Existe una iniciativa mediante el Plan de recuperación de desastres del año 2016, aunque no existe un marco institucional establecido".

La DGCP no cuenta con un control, mecanismo o plan que identifique los riesgos tecnológicos a los que se exponen a nivel general e incluyendo los servicios ofrecidos desde el portal transaccional.

Recomendaciones:

1. Al director general le corresponde, garantizar a través de la Dirección de Tecnología de la Información y Comunicación a:

   - Desarrollar un plan de Análisis de Riesgos Tecnológicos basado en una metodología formal en el que se incluya la mayoría de los puntos mencionados anteriormente. Como sugerencia, las metodologías de TI *(Ej. MAGERIT, NIST, ISO 27005*) incluyen esos aspectos.
   - Realizar en la DGCP el Análisis de Riesgos para establecer los parámetros para implementar la Seguridad de TIC y mitigación de Riegos Tecnológicos.
   - Determinar el calendario periódico con el que se debe realizar el Análisis de Riesgo de TI a fin de verificar que los riesgos tecnológicos están siendo mitigados.

2. Al director general le corresponde, garantizar para que se gestionen los controles y herramientas de forma efectiva, que se minimicen los riesgos tecnológicos que pudieran afectar los procesos, servicios y actividades de la DGCP.

Es

Reacción de la ex administración de la entidad:

Mediante comunicación de réplica de fecha 16 de septiembre de 2022, Yokasta Altagracia Guzmán, cédula de identidad y electoral, n.° 001-0081375-7, exdirectora general de la Dirección General de Contrataciones Públicas, expresa:

1. *"Se elaboraron Matrices de Riesgo por área, 2015.*
2. *Se actualizó la Matriz de Riesgos, 2016.*
3. *Se actualizó la Matriz de Riesgos, 2018.*

Recomendamos buscar evidencia en las implementaciones de NOBACI. Ver informe de los procesos y servicios internos de Tecnología, que incluyen recomendaciones de mejoras en el flujo de los distintos procesos (realizado por el Consultor Ing. Juan Díaz).

Los mencionados documentos reposan en el archivo institucional".

Comentarios y conclusiones de los auditores de la CCRD

Luego de una revisión exhaustiva y en vista a la carencia de información necesaria en la que se pudiera ver la subsanación se mantiene la observación en el informe.

2.4 Vulnerabilidades del centro de datos (Data Center).

1) En fecha 29 de julio de 2021, se realizó una inspección física al centro de datos (Data Center) de la Dirección General de Contrataciones Públicas, se encontraron las siguientes debilidades en los subsistemas mecánicos, arquitectura y eléctrico:

   a. Sistemas de refrigeración, en la actualidad la DGCP cuenta con dos aires tipo central de cinco (5) toneladas que trabajan configurado uno como respaldo del otro.
   b. Sistema de respaldo UPS, se comprobó que la unidad de UPS EATON POWERWARE 9355 funciona como respaldo general en las instalaciones de la DGCP.
   c. El sistema de supresión de incendio automático no cuenta con los detectores de humos que en caso de un incendio fuera del perímetro en el mismo centro de datos active la alarma de la existencia de un siniestro o humo.
   d. Extintor manual dentro del centro de datos (Data Center) y señalización suelta.

ES

e. No se cuenta con un estudio o plano que determine que la ubicación actual del centro de datos (Data Center) sea la más idónea y favorable a la DGCP estando este en un perímetro de acceso general para los colaboradores y personal de visita con un acceso más allá de la recepción.
f. Las puertas de acceso al centro de datos (Data Center) no cumplen con las buenas prácticas por las siguientes condiciones detalladas:
   i. Puertas de vidrios solo con el marco en aluminio.
   ii. Puertas sin sensores de rupturas de Vidrios.
   iii. Puertas con llavines y cerraduras mecánicas.
   iv. Ausencia de sensores que notifique la apertura de las puertas.
   v. Puertas en la cara frontal y lateral del centro de datos (Data Center).
g. No se cuenta con un falso piso.
h. El falso techo de material inflamable.
   i. El cableado de data y el cableado eléctrico pasando por el mismo conducto para llegar a los RACKs.
   j. Una sola cámara de circuito cerrado (CCTV) la cual no cubre todos los ángulos del centro de datos (Data Center) permitiendo puntos ciegos.
   k. Sistema eléctrico de la DGCP no aísla el sistema eléctrico del centro de datos (Data Center) para proteger los equipos de este frente a caída, picos o incidentes eléctricos.

2) Durante los procedimientos de inspección realizados al centro de datos (Data Center) se encontraron las siguientes debilidades de gestión de control:
   a. No se cuenta con una bitácora de visitas.
   b. No existen políticas y procedimientos actualizados relativos a los controles y mecanismo del sistema eléctrico y respaldo.
   c. No se cuenta con políticas y procedimientos para asegurar el adecuado diseño del centro de datos (Data Center).
   d. No se cuenta con políticas y procedimientos actualizados para los accesos temporales de personal al centro de datos (Data Center).

El marco de evaluación de Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT 4.1), en los procedimientos DS12.1 Selección y Diseño del Centro de Datos, DS12.2 Medidas de Seguridad Física, DS12.3 Acceso Físico, DS12.4 Protección Contra Factores Ambientales y DS12.5 Administración de Instalaciones Físicas expresan:

"DS12.1 Selección y Diseño del Centro de Datos. - Definir y seleccionar los centros de datos físicos para el equipo de TI para soportar la estrategia de tecnología ligada a la estrategia del negocio. Esta selección y diseño del esquema de un centro de datos debe tomar en cuenta el riesgo asociado con desastres naturales y los causados por el hombre. También debe

considerar las leyes y regulaciones correspondientes, tales como regulaciones de seguridad y de salud de trabajo.

DS12.2 Medidas de Seguridad Física. - Definir e implementar medidas de seguridad físicas alineadas con los requerimientos del negocio. Las medidas deben incluir, pero no limitarse al esquema de perímetro de seguridad, de las zonas de seguridad, la ubicación del equipo crítico y de las áreas de envío y recepción. En particular, mantenga un perfil bajo respecto a la presencia de operaciones críticas de TI. Deben establecerse las responsabilidades sobre el monitoreo y los procedimientos de reporte y de resolución de incidentes de seguridad física.

DS12.3 Acceso Físico. - Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a locales y áreas de acuerdo con las necesidades del negocio, incluyendo las emergencias. El acceso a locales, edificios, áreas debe justificarse, autorizarse, registrarse y monitorearse. Esto aplica para todas las personas que accedan a las instalaciones, incluyendo personal, clientes, proveedores, visitantes o cualquier tercera persona.

DS12.4 Protección Contra Factores Ambientales. -Diseñar e implementar medidas de protección contra factores ambientales. Deben instalase dispositivos y equipo especializado para monitorear y controlar el ambiente".

DS12.5 Administración de Instalaciones Físicas. -Administrar las instalaciones, incluyendo el equipo de comunicaciones y de suministro de energía, de acuerdo con las leyes y los reglamentos, los requerimientos técnicos y del negocio, las especificaciones del proveedor y los lineamientos de seguridad y salud".

La Norma para la Seguridad de las Tecnologías de la Información y Comunicación en el Estado Dominicano NORTIC A7 de 2016, en su sección 3.01 Control de acceso de usuario, literal a y sus sub-literales, establece:

"(a) Los organismos gubernamentales deben tener procedimientos establecidos para la gestión de accesos de sus empleados, estos procedimientos deben contemplar:

(i) Accesos de entrada y salida al organismo gubernamental.

a) El sistema de acceso al organismo gubernamental debe cumplir las directrices establecidas en la sección 3.02 Controles de acceso a la infraestructura.

(ii) Controles de accesos a la información del organismo gubernamental.

a) Estos controles deben contemplar las directrices establecidas en la sección 2.02 Políticas para la administración de la información.

(iii) Controles de accesos a estaciones de trabajo.
(iv) Controles de accesos a áreas restringidas.
(v) Controles de accesos a áreas de servidores.
(vi) Controles de accesos a software del organismo gubernamental."

La referida Norma NORTIC B1 de 2016, en su sección 5.02 Gestión del centro de datos y Servidores, literales y sub-literales, establece:

"(a) Para la correcta administración de los centros de datos, deben seguirse las directrices a continuación:

(i) El personal de la unidad TIC debe tener contratos de confidencialidad sobre los datos o información que estos manipulen.
(ii) En caso de que el organismo opte por la contratación de terceros para el almacenamiento de la información, el proveedor debe entregar un SLA, el cual debe especificar su compromiso con salvaguardar la información.
(iii) La unidad de TIC debe asegurar la redundancia de su infraestructura para eventualidades o catástrofes. Ver NORTIC A7:2016, Capitulo IV. Plan de disponibilidad y continuidad.
(iv) Deben existir políticas de privilegios dentro del departamento de TIC, específicamente el área de operaciones TIC, para que solo el personal autorizado pueda acceder a la infraestructura del organismo. Ver NORTIC A7:2016, sección 3.02 controles de acceso a la infraestructura.

(b) Para la correcta administración de los servidores dentro del centro de datos, deben seguirse las directrices a continuación:

- *Debe darse soporte y mantenimiento al sistema operativo y el software utilitario instalado.*
- *Deben crearse políticas de respaldo y restauración.*
- *Deben gestionarse todas las licencias para los sistemas instalados en los servidores, especialmente sistemas operativos, utilidades y cualquier software de aplicación.*

a) Para los temas sobre el licenciamiento el organismo debe cumplir con las directrices especificadas en la NORTIC A1, subsección 1.05.2 Licenciamiento.

- *Deben aplicarse medidas de seguridad, incluyendo la identificación y aplicación de parches de seguridad, gestión de acceso y detección de intrusiones.*
- *Debe realizarse un mantenimiento continuo, el cual incluya la sustitución de servidores antes de estos ser obsoletos para apoyar la evolución de los servicios.*
- *Los servidores deben tener el cifrado de unidad activado desde el Sistema Básico de Entrada/Salida (BIOS, por sus siglas en inglés) para la encriptación de sus datos.*
- *Los servidores de dominio deben tener habilitado el protocolo LDAPS.*
- *Todas las estaciones de trabajo deben estar protegidas por políticas para ser accedidas solo por el personal autorizado.*

- *Los servidores de la infraestructura deben tener las últimas actualizaciones y parches de seguridad.*
  a) Antes de la implementación en ambientes de producción, esto debe pasar por un ambiente de pruebas.
- *Todos los servidores deben tener una solución de antivirus actualizada que aseguren la protección de la red, así como las estaciones de trabajo.*
- *Los controles de acceso biométricos o de tarjetas de código que estén conectados a la infraestructura de la red, deben estar conectados mediante una VLAN separada del tráfico de usuarios".*

ANSI/TIA-942-A (La Asociación de la Industria de Telecomunicaciones, Norma de Infraestructura de Telecomunicaciones para Centros de Datos, en inglés: (The Telecommunications Industry Association (TIA) Telecommunications Infrastructure Standard for Data Centers is an American National Standard (ANS), el documento TIA ESTANDAR aprobado el 12 de abril de 2005 sobre las Normas de infraestructuras de telecomunicaciones para centros de datos expresa, en la descripción generales de diseño de centro de datos cuales son los elementos y factores necesario para el diseño del mismo los cuales enumeramos:

a) Estimación de equipos de telecomunicaciones, espacio, energía y demanda de refrigeración del centro de datos a plena capacidad. Anticipar futuras telecomunicaciones, el poder y las tendencias de enfriamiento durante la ida útil del centro de datos.

b) Proporcionar espacio, energía, refrigeración, seguridad, carga sobre el suelo, tierra, protección eléctrica, y otros requisitos de las instalaciones a los arquitectos e

ingenieros. Proporcionar los requisitos para el centro de operaciones, muelle de carga, sala de almacenamiento, áreas de almacenamiento y otras áreas de apoyo.

c) Coordinar los planes de centros de datos espaciales preliminares de arquitectos e ingenieros. Sugerir cambios según sea necesario.
d) Crear un plan de equipamiento para el salón incluyendo la colocación de las principales salas y espacios para salas de ingreso, principales áreas de distribución, áreas de distribución horizontal, zonas de distribución de zonas y áreas de distribución de equipos. Proporcionar energía esperada, la refrigeración, y el piso cargado requisitos para el equipo de ingenieros. Proporcionar los requisitos para las vías de telecomunicaciones.
e) Obtener un plan actualizado de los ingenieros de telecomunicaciones con las vías, equipos eléctricos, equipos mecánicos y añadido a la planta del centro de datos a plena capacidad.

f) Sistema de cableado de telecomunicaciones Diseño basado en las necesidades del equipo que se encuentra en el centro de datos.

La DGCP no cuenta con un diseño y gestión adecuado en el centro de datos, el cual le permita certificar un ambiente físico y seguro en el desarrollo de las operaciones de la tecnología de la información.

Recomendación:

Al director general le corresponde, gestionar a través de las áreas técnicas correspondientes, la readecuación del Centro de Datos (Data Center), la adquisición de los elementos faltantes, la actualización de elementos existentes y la implementación de las mejores prácticas, para elevar el nivel de madurez del Centro de Datos (Data Center), implementación de procedimientos y herramientas que aseguren el acceso a las áreas restringidas y asegurar las operaciones de la DGCP en la plataforma e infraestructura tecnológica.

Reacción de la ex administración de la entidad:

Mediante comunicación de réplica de fecha 16 de septiembre de 2022, Yokasta Altagracia Guzmán, cédula de identidad y electoral, n.° 001-0081375-7, exdirectora general de la Dirección General de Contrataciones Públicas, expresa:

a. *"Respecto estos hallazgos, favor de tomar en cuenta, que para agosto del año 2020 el Data Center se encontraba ubicado en las instalaciones del Data Center del Sistema de Emergencias 911 y en la institución solo existe un Cuarto de Equipos que no califica para ser denominado Centro de Datos (Data Center) pues en el mismo solo se encuentra un servidor de dominio y un servidor de correos que requieren encontrarse físicamente en la DGCP.*

Los mencionados documentos reposan en el archivo institucional".

b. *Respecto a su señalamiento, favor de tomar en cuenta, que para agosto del año 2020 el Data Center se encontraba ubicado en las instalaciones del Data Center del Sistema de Emergencias 911 y en la institución solo existe un Cuarto de Equipos que no califica para ser denominado Centro de Datos (Data Center) pues en el mismo solo se encuentra un servidor de dominio y un servidor de correos que requieren encontrarse físicamente en la DGCP.*

Dentro de los Planes de Continuidad de Servicio, se tenía contemplado el traslado del Centro de Datos de la institución del Sistema de Emergencias 911 al Centro de Datos de la OPTIC, lo que no pudo ser ejecutado debido a las situaciones originadas por la pandemia del COVID-19 y la posterior entrada de nuevas autoridades.

Verificar bien que se contaba con procedimientos de accesos al datacenter, las mismas tienen evidencia y fueron parte de las auditorías de las Nortic (certificadas).

Los mencionados documentos reposan en el archivo institucional".

Comentarios y conclusiones de los auditores de la CCRD

Luego de una revisión exhaustiva y en vista a la carencia de información necesaria en la que se pudiera ver la subsanación se mantiene la observación en el informe.

2.5 Ausencia de controles en el servidor de dominio.

Durante los procedimientos de extracción de logs y revisión del servidor de active directory, practicado en el mes de julio de 2021, se detectaron que existen vulnerabilidades y falta de control detalladas a continuación:

1-Logs o pistas de auditorías deshabilitadas como se detallan a continuación:

i. Reinicio y apagado: Sin auditoría (Restart and Shutdown: No auditing).
ii. Inicio y cierre de sesión: Sin auditoría (Logon and Logoff: No auditing).
iii. Archivo / Acceso a objetos: Sin auditoría (File/Object Access: No auditing).
iv. Uso del derecho de usuario: Sin auditoría (Use of User Right: No auditing).
v. Proceso de seguimiento: Sin auditoría (Process Tracking: No auditing).
vi. Cambios en la política de seguridad: Sin auditoría (Security Policy Changes: No auditing).
vii. Gestión de Usuarios / Grupos: Sin auditoría (User / Group Managenment: No auditing).
viii. Acceso al servicio de directorio: Sin auditoría (Directory Service Access: No auditing).
ix. Inicio de sesión de cuenta privilegiada: Sin auditoría (Privileged Account Logon: No auditing).
x. Cuentas de usuarios activas en el active directory con acceso mediante VPN que las contraseñas no expiran o caducan
xi. Cuentas de servicios activas, en el active directory, con dos años o más tiempo sin cambio de contraseñas
xii. Cuentas de usuarios del active directory con privilegios y pertenecen al grupo de Administradores en la que no expira o caduca la contraseña.
xiii. Cuentas de usuarios en el active directory con privilegios de administración de esquemas (Schema Admin).
xiv. Cuentas de usuarios de active directory con privilegios de administradores de empresas (Enterprise Admin).
xv. Cuentas de usuarios para pruebas activas en el active directory sin uso.

La Norma para la Seguridad de las Tecnologías de la Información y Comunicación en el Estado Dominicano NORTIC A7 de 2016, en su sección 3.03 Control de acceso al sistema operativo, literal h y sus sub-literales, establece:

"(h) Todas las estaciones de trabajo de los organismos gubernamentales deben estar protegidas por contraseña que cumplan las siguientes características:

i. Las contraseñas deben tener un mínimo de ocho (8) caracteres.
ii. Las contraseñas deben tener al menos una letra mayúscula.
iii. Las contraseñas deben tener letras minúsculas.
iv. Las contraseñas deben tener al menos un número.

v. *Las contraseñas deben ser renovadas cada cuarenta y cinco (45) días.*
vi. *Las contraseñas personales no deben ser compartidas para no comprometer información sensible que resida en las estaciones de trabajo.*
vii. *Las contraseñas definidas por el empleado no deben ser comunes.*
viii. *Las contraseñas no se pueden reutilizar en diferentes sistemas a menos que se esté utilizando un sistema de autenticación centralizado o de Autentificación Sencilla."*

El marco de evaluación de Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT 4.1), en el procedimiento DS5.4 "Administración de Cuentas del Usuario, expresa:

"Garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, sean tomados en cuenta por un conjunto de procedimientos de la gerencia de cuentas de usuario. Debe incluirse un procedimiento de aprobación que describa al responsable de los datos o del sistema otorgando los privilegios de acceso. Estos procedimientos deben aplicarse a todos los usuarios, incluyendo administradores (usuarios privilegiados), usuarios externos e internos, para casos normales y de emergencia. Los derechos y obligaciones relativos al acceso a los sistemas e información de la empresa deben acordarse contractualmente para todos los tipos de usuarios. Realizar revisiones regulares de la gestión de todas las cuentas y los privilegios asociados".

En el referido marco COBIT 4.1, en el procedimiento DS10.2 Rastreo y Resolución de Problemas, expresa:

"El sistema de administración de problemas debe mantener pistas de auditoría adecuadas que permitan rastrear, analizar y determinar la causa raíz de todos los problemas reportados considerando:

- *Todos los elementos de configuración asociados*
- *Problemas e incidentes sobresalientes*
- *Errores conocidos y sospechados*
- *Seguimiento de las tendencias de los problemas.*

Identificar e iniciar soluciones sostenibles indicando la causa raíz, incrementando las solicitudes de cambio por medio del proceso de administración de cambios establecido. En todo el proceso de resolución, la administración de problemas debe obtener reportes regulares de la administración de cambios sobre el progreso en la resolución de problemas o errores. La administración de problemas debe monitorear el continuo impacto de los problemas y errores conocidos en los servicios a los usuarios. En caso de que el impacto se vuelva severo, la administración de problemas debe escalar el problema, tal vez refiriéndolo a un comité determinado para incrementar la prioridad de la solicitud del cambio (RFC) o para implementar un cambio urgente, lo que resulte más pertinente. El avance de la resolución de un problema debe ser monitoreado contra los SLAs".

El Estándar para la Seguridad de la Información de la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional ISO/IEC 27002, en el dominio 9 sobre el Control de Acceso en los diferentes Objetivos de Control y Controles, establece:

"9.2 Gestión de acceso de usuario: Garantizar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información y servicios.

9.2.2 Gestión de los derechos de acceso asignados a usuarios: Se debería de implantar un proceso formal de aprovisionamiento de acceso a los usuarios para asignar y revoca derechos de acceso a todos los tipos usuarios y para todos los sistemas y servicios.
9.2.3 Gestión de los derechos de acceso con privilegios especiales: La asignación y uso de los derechos de acceso con privilegios especiales debería ser restringido y controlado.
9.2.5 Revisión de los derechos de acceso de los usuarios: Los propietarios de los activos deberían revisar con regularidad los derechos de acceso de los usuarios.
9.2.6 Retirada o adaptación de los derechos de acceso: Se deberían retirar los derechos de acceso para todos los empleados, contratista o usuarios de terceros a la información y a las instalaciones del procesamiento de información a la finalización del empleo, contrato o acuerdo, o ser revisados en caso de cambio.

9.4 Control de acceso a sistemas y aplicaciones: Impedir el acceso no autorizado a la información mantenida por los sistemas y aplicaciones.

9.4.2 Gestión de contraseñas de usuario: Los sistemas de gestión de contraseñas deberían ser interactivos y asegurar contraseñas de calidad".

El encargado de TIC vía correo electrónico de fecha 22 de octubre de 2021 con el título: Acceso | Auditoría Cámara de Cuenta - Solicitud de datos y comprobantes, solicitud n.° 45 - Información varias, nos responde:

"Actualmente se encuentran activas las políticas de auditoría de eventos de autenticación y bloqueo de cuentas a nivel de dominio general, sin embargo, en los servidores de AD se detectó con este proceso de auditoría que las auditorias locales de los servidores no estaban habilitadas, esto se atribuye a que no fue considerado en la instalación original del dominio, sin embargo, serán activadas producto de este hallazgo".

"Existe una iniciativa pendiente de ejecución sobre la implementación de un criterio de menor privilegio para los usuarios administrativos donde se separarían los roles administrativos de los permisos comunes del usuario, sin embargo, la misma no se ejecutado por lo tanto por razones culturares hay usuarios con permisos similares asociados al mismo administrador". SIC

"No están documentados estos casos".

"Estas cuentas en muchas ocasiones son creadas sin el conocimiento de la división de ciberseguridad y al no existir un procedimiento oficial documentado sobre el trato de este tipo de cuentas las mismas no son inhabilitadas en su debido momento".

"Por la falta de un procedimiento que indique a los colaboradores técnicos de las diferentes áreas a solicitar y validar estos accesos con la división de ciberseguridad antes de modificar estas opciones en la configuración de los usuarios finales".

"Por la falta de un procedimiento que inste a los colaboradores técnicos de las diferentes áreas a solicitar y validar estos accesos con la división de ciberseguridad antes de modificar estas opciones y por falta de capacidades de monitoreo/auditoria de los diversos sistemas institucionales".

"Por la falta de un procedimiento que indique a los colaboradores técnicos de las diferentes áreas a solicitar y validar estos accesos con la división de ciberseguridad antes de modificar estas opciones en la configuración de los usuarios finales".

"por la falta de un procedimiento de validación periódica de cuentas en uso en el dominio".

ES

"Por motivos históricos culturares no se ha permitido llevar a cabo la auditoria de accesos administrativos donde se determinaría la necesidad real de la asignación de estos permisos solo en los casos donde sea requerido".

"No existe un procedimiento oficial aprobado para la ejecución de esta tarea".

Durante los procedimientos y levantamientos de información realizados en la DGCP se evidencio ausencia de controles en los recursos que se gestionan desde el servidor de dominio de Active Directory.

Recomendaciones:

Al director general le corresponde,

1. Garantizar vía la Dirección de Tecnología de la Información y Comunicación la revisión y saneamiento de los perfiles y roles de las cuentas en el active directory para determinar cuáles cuentas de usuarios realmente necesitan privilegios o excepciones para el desarrollo de sus tareas diarias.

2. Instruir a la Dirección de Tecnología de la Información y Comunicación a realizar el procedimiento necesario para activar las directivas o pistas de auditorías en el servidor de active directory para contar con los logs en caso de alguna eventualidad.

3. Garantizar el apoyo total a las políticas y procedimientos generales de TICs y en especial a las correspondientes a la administración y gestión del servidor del Active Directory ejecutadas por la Dirección de Tecnología de la Información y Comunicación.

Reacción de la ex administración de la entidad:

Mediante comunicación de réplica de fecha 16 de septiembre de 2022, Yokasta Altagracia Guzmán, cédula de identidad y electoral, n.° 001-0081375-7, exdirectora general de la Dirección General de Contrataciones Públicas, expresa:

1) Documentación de la solución Vortal para el Portal Transaccional (solución "llave en mano"). 2) Las políticas y la administración las llevaba a cabo el Líder de Seguridad TIC (Ing. Eddy Acevedo). 3) También se pueden validar las evidencias e informes en la auditoría realizada al sistema por la empresa ARGENTUM, que incluye el período comprendido entre 2017 – 2020.

Los mencionados documentos reposan en el archivo institucional".

Comentarios y conclusiones de los auditores de la CCRD

Luego de una revisión exhaustiva y en vista a la carencia de información necesaria en la que se pudiera ver la subsanación se mantiene la observación en el informe.

2.6 Estructura organizativa del departamento de TIC no alineada a Órganos rectores

En indagaciones realizadas mediante el mes de octubre de 2021 al Departamento de Tecnología de la Información y Comunicación, se constató que actualmente no cuentan con una estructura alineada a las posiciones o cargos existentes en la resolución 51-2013 de fecha 3 de diciembre de 2013, que aprueba los modelos de estructura organizativa de las unidades de Tecnologías de la Información y Comunicación (TIC), aprobada por los órganos rectores: Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC) y el Ministerio de Administración Pública (MAP).

La Norma General Sobre el Uso e Implementación de las Tecnologías de la Información y Comunicación en el Estado Dominicano. NORTIC A1 de 2014, en el capítulo 2 Gestión del Departamento de TIC, en las secciones que lo componen 2.01 Estructura del departamento TIC, 2.02 Políticas generales del departamento de TIC, 2.03 Servicios TIC, 2.04 Inventario general de TIC y 2.05 Recomendaciones para las políticas del departamento TIC C, en la sub-secciones, literales y sub-literales que la conforman, establece:

CAPÍTULO II
GESTIÓN DEL DEPARTAMENTO DE TIC

"En este capítulo se establecen las directrices para la gestión del departamento de TIC, especificando cómo este debe estar estructurado organizacionalmente, las políticas departamentales para una gestión efectiva, como debe gestionar los servicios de TIC y cómo llevar el control de los activos que están bajo la responsabilidad del departamento".

SECCIÓN 2.01. Estructura del departamento de TIC

Se ha dispuesto una estructura organizacional que consta de 5 áreas básicas, las cuales deben cumplir con los roles establecidos para cada una de estas áreas, así como 3 modelos

de estructura organizacional y dos formas para la selección de uno de estos modelos basado en una serie de criterios y tablas de ponderaciones.

Sub-sección 2.01.1. Estructura organizacional

(a) *Todo organismo gubernamental debe organizar la estructura departamental de TIC, de acuerdo con todas las directrices especificadas en la resolución 51-2013 elaborada entre la OPTIC y el MAP.*

(b) *La gestión del departamento de TIC debe agruparse en 6 grandes áreas básicas y cumplir con los roles asignados a cada una:*

(i) Unidad TIC: *Tiene bajo su cargo las responsabilidades indicadas en la sección 2.02. Políticas generales del departamento TIC.*

(ii) Desarrollo e implementación de sistemas: *Debe responsabilizarse de todas las actividades relacionadas con el diseño, desarrollo, implementación y soporte de los programas y sistemas que apoyan los procesos esenciales de los organismos.*

(iii) Operaciones de TIC: *Debe responsabilizarse de todas las actividades relacionadas con la operación y administración de la infraestructura tecnológica (servidores, bases de datos, redes, entre otros), así como el aseguramiento de la continuidad de las operaciones.*

(iv) Administración del servicio de TIC: *Debe responsabilizarse de todas las actividades de soporte técnico a la infraestructura tecnológica, incluyendo el soporte funcional y mesa de ayuda a los usuarios de los servicios de TIC.*

(v) Seguridad y monitoreo: *Debe responsabilizarse de todas las actividades relacionadas con la definición e implementación de políticas de seguridad de la información, control y monitoreo de los accesos a los sistemas de información.*

(vi) Administración de proyectos de TIC: *Debe responsabilizarse de todas las actividades relacionadas con la administración y coordinación de la implementación de proyectos de TIC.*

SECCIÓN 2.02. Políticas generales del departamento de TIC

Una buena gestión del departamento de TIC incrementa la efectividad y productividad del departamento, y permite lograr los objetivos establecidos previamente, haciendo un mejor uso de la tecnología y la estructura organizacional. Para lograrlo, todo organismo gubernamental debe cumplir con las siguientes directrices:

***(a)** La máxima autoridad del departamento de TIC debe cumplir con las siguientes responsabilidades, apoyándose en todos los miembros pertenecientes al departamento:*

***(i)** Evaluar y monitorear el cumplimiento de normas, políticas y leyes por parte de todos los miembros del departamento.*

***(ii)** Dirigir la preparación y la implementación de planes y políticas.*

***(iii)** Gestionar y administrar eficientemente las fuentes y activos de información del organismo, disponiendo de controles la calidad y seguridad de los sistemas.*

***(iv)** Gestionar y administrar las licencias de software y realizar su distribución entre las unidades administrativas que las requieran.*

***(v)** Administrar y coordinar todas las actividades relacionadas con la implementación de proyectos de TIC de impacto interno o externo del organismo.*

***(vi)** Administrar y gestionar los servicios del centro de datos, garantizando la tecnología que soporte las actividades de TIC del organismo, así como el aseguramiento de la redundancia y balanceo de los servicios, monitorear el óptimo estado de los sistemas y plataformas alojadas.*

***(vii)** Desarrollar y administrar aplicaciones de TIC que contribuyan al logro de las metas del organismo, asegurando la calidad de la plataforma y el cumplimiento de los estándares especificados en las NORTIC.*

***(viii)** Disponer de los servicios informáticos y de telecomunicaciones que soliciten las diferentes unidades administrativas del organismo.*

***(ix)** Fomentar la integración a diferentes redes de informaciones nacionales e internacionales mediante Internet, para permitir el acceso a distintas bases de datos en línea.*

ES

(x) Implantar y mantener actualizado un sistema de información integral que automatice las operaciones y procesos del organismo fomentando la comunicación interna, mediante el uso intensivo de las TIC.

(xi) Implementar y mantener la infraestructura de TIC que permita al organismo alcanzar sus metas estratégicas y promover el Gobierno Electrónico, mediante el intercambio, acceso y uso de la información por los usuarios internos y externos.

(xii) Participar en la elaboración, ejecución y seguimiento, de acuerdos y protocolos de intercambios de información por medios electrónicos que realice el organismo con otras instituciones públicas y privadas.

(xiii) Proveer soporte técnico a los usuarios de las aplicaciones, así como a la información y la infraestructura del organismo.

(xiv) Realizar la planificación estratégica y presupuestaria de las soluciones de TIC del organismo. (xv) Revisar periódicamente el funcionamiento de la red, el desempeño de los sistemas en operación y el de las bases de datos del organismo para identificar desviaciones respecto a los objetivos y formular recomendaciones que optimicen los recursos y procesos operativos, propiciando el incremento de la productividad y la eficiencia.

(b) De acuerdo con la naturaleza de cada organismo gubernamental, debe crearse políticas de documentación para cada procedimiento, resolución de incidentes, software desarrollado internamente, y cualquier otra información relevante que manipule el departamento.

(i) La documentación debe realizarse de manera minuciosa, explicando todos los detalles de la información a documentar.

(ii) En caso de prescindir de un recurso, debe utilizarse la documentación realizada previamente, de manera que se pueda continuar brindando los servicios que se ofrecen.

SECCIÓN 2.03. Servicios de TIC

En esta sección se establece el procedimiento a seguir en la prestación de servicios y la gestión de incidentes. Así como las especificaciones para la estructuración del catálogo de servicio y la elaboración de los Acuerdos de Nivel de Servicio (SLA, por sus siglas en inglés).

EA
ES

(a) La disponibilidad de los servicios debe contemplarse en el plan de disponibilidad y continuidad de cada organismo. Ver sección 6.05. Plan de disponibilidad y continuidad.

(b) Cualquier tarea que implique una degradación o interrupción del servicio debe realizarse en las horas de inactividad o de menor demanda de este, siempre que sea posible.

(c) Si el servicio debe estar disponible las 24 horas del día y la interrupción es necesaria:

(i) Debe consultarse con el cliente acerca de las horas en la que la interrupción del servicio afectará menos a sus actividades.

(ii) Debe informarse con antelación suficiente a todos los involucrados.

(iii) Debe incorporarse dicha información a los SLA.

(iv) Debe monitorizarse la disponibilidad del servicio y elaborarse informes con los resultados.

(v) Debe especificarse el tiempo de detección.

(vi) Debe especificarse el tiempo de respuesta.

(vii) Debe especificarse el tiempo de reparación/recuperación.

SECCIÓN 2.04. Inventario general de TIC

Se establece el procedimiento para el levantamiento, actualización y control de inventario que todos los organismos deben seguir para la gestión de los activos físicos y de información que se encuentren bajo la responsabilidad del departamento de TIC.

(a) Todo organismo debe realizar un inventario ordenado, completo y actualizado de todos los activos que estén bajo la responsabilidad del departamento de TIC.

(i) El inventario general de TIC debe estar organizado en dos secciones principales:

- ***Activos físicos:** Donde se registrarán todos los equipos de la infraestructura TI, estaciones de trabajo, portátiles y demás.*

- ***Activos de información:** Donde se registrará todo el software utilizado, sistemas operativos y demás.*

(ii) La unidad de operaciones de TIC debe tener un personal que asuma la función de llevar a cabo todo el proceso de inventario. Este tendrá a la responsabilidad de coordinar las tareas que deben desarrollarse:

*a) **Levantamiento de inventario:** Registrar todos los bienes que forman el equipamiento tecnológico bajo el control del departamento de TIC. Esta fase se realizará en caso de que el organismo no haya realizado un inventario anteriormente.*

*b) **Actualizaciones de inventario:** Agregar al inventario nuevos bienes adquiridos por el departamento de TIC, igualmente eliminar los bienes que han salido de la responsabilidad del organismo.*

*c) **Control de inventario:** Revisar físicamente los bienes que se encuentran en el inventario.*

SECCIÓN 2.05. Recomendaciones para las políticas del departamento de TIC

• Establecer responsabilidades claramente entendidas y aceptadas por todos los miembros del departamento de TIC.

• Para cumplir con los objetivos departamentales, antes de elaborar las estrategias de trabajo, es necesario tomar en cuenta las capacidades y recursos técnicos que posee el departamento de TIC.

• Que la estructura del departamento de TIC esté distribuida, tanto en recursos tecnológicos como en recursos humanos, de manera que pueda darse soporte al organismo y brindar los servicios con la calidad exigida.

El Decreto n.° 527-09, que establece el Reglamento Estructura Organizativa, Cargos y Política Salarial, de fecha 21 de julio de 2009, artículo 5, De las Estructuras Organizativas, expresa: *"La estructura organizativa es un instrumento fundamental para desarrollar una estrategia efectiva de gestión por tanto para su presentación y aprobación debe contener y reflejar todos los cargos clasificados valorados y presupuestados requeridos para el cumplimiento de los objetivos y proyección estratégica de cada institución así como su realidad".*

ES

El Decreto n.° 491-07, del 30 de agosto de 2007, que aprueba el Reglamento de Aplicación de la Ley n.° 10-07, del 8 de enero de 2007, que Instituye el Sistema Nacional de Control Interno y de la Contraloría General de la República, título IV Del Desarrollo y Aplicación del Control Interno y Auditoría Interna, capítulo II De los Componentes del Proceso de Control Interno, artículo 47, numeral 1 Ambiente de control, literales f y h, respectivamente, establece:

"La administración activa, principalmente el titular de cada entidad y organismo público del ámbito de la Ley, debe fomentar un ambiente propicio para la operación del control interno, mediante la generación de una cultura de administración y control que promueva, entre el personal de la institución, el reconocimiento del control como parte integrante de los sistemas institucionales. En su calidad de responsable por el proceso de control interno debe mostrar constantemente una actitud de apoyo a las medidas de control implantadas en la institución, mediante la divulgación de éstas y un ejemplo continuo de apego a ellas en el desarrollo de las labores cotidianas. Los elementos principales en que descansa el componente son:

(...) f) Estructura organizacional.
(...) h) Asignación de responsabilidad".

El encargado de TIC vía correo electrónico de fecha 22 de octubre de 2021 con el título: Acceso | Auditoría Cámara de Cuentas - Solicitud de datos y comprobantes, solicitud n.° 45 - Información varias, nos responde:

"Documento colocado en la carpeta Anexos [ORGANIGRAMA TIC]"

La Dirección de Tecnología de la Información y Comunicación de la DGCP, no cuenta con una infraestructura organizacional alineada a las recomendaciones del MAP en la resolución n.° 51-2013 y la OPTIC en la NORTIC A1 del 2014.

Recomendación:

Al director general le corresponde, gestionar la realización de estudio o evaluación, diseño, creación e implementación de la estructura organizativa de la Dirección de Tecnología de la Información y Comunicación de la Dirección General de Contrataciones Públicas (DGCP) basadas en las estructuras recomendadas por el Ministerio de Administración Pública (MAP) y la Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC) en la Resolución n.° 53-2013 y la NORTIC A1 2014, Norma General Sobre el Uso e

Implementación de las Tecnologías de la Información y Comunicación en el Estado dominicano.

Reacción de la ex administración de la entidad:

Mediante comunicación de réplica de fecha 16 de septiembre de 2022, Yokasta Altagracia Guzmán, cédula de identidad y electoral, n.° 001-0081375-7, exdirectora general de la Dirección General de Contrataciones Públicas, expresa:

1. *"Se definió una estructura funcional para Tecnología, alineada con los requerimientos del Ministerio de Administración Pública (MAP), la Oficina Presidencial de Tecnología de la Información y Comunicaciones (OPTIC) y COBIT, 2014.*
2. *Se actualizaron las descripciones de puesto, 2016.*
3. *Se definió una estructura funcional para Tecnología, alineada con los requerimientos del Ministerio de Administración Pública (MAP), la Oficina Presidencial de Tecnología de la Información y Comunicaciones (OPTIC) y COBIT, 2019.*
4. *La referida estructura fue aprobada mediante Resolución Núm. 1084-2020 del Ministerio de Administración Pública (MAP).*

Como se indica la estructura de TIC aprobada no era acorde al dimensionamiento necesario y requerido para llevar adelante la Plataforma de Emisión Critica del Portal Transaccional (+ de 2,000 usuarios externos e internos, + de 40 servidores, etc). El consultor Ing. Juan Díaz, confeccionó un documento con una propuesta acorde a la realidad de las necesidades de la Institución, la cual debería presentarse al MAP para su aprobación. La pandemia del COVID19 y el cambio de gobierno hizo que esta propuesta no se llevara a cabo, pero se presentó a la nueva Dirección que asumió en agosto 2020 para continuar con la gestión en el MAP (Órgano Rector de Función Pública).

Los mencionados documentos reposan en el archivo institucional".

Comentarios y conclusiones de los auditores de la CCRD

Luego de una revisión exhaustiva y en vista a la carencia de información necesaria en la que se pudiera ver la subsanación se mantiene la observación en el informe.

EL
ES

2.7 Falta de control y monitoreo en los accesos a los sistemas de información.

Verificamos que en los procedimientos aplicados en los meses de septiembre y octubre de 2021, el área de seguridad y monitoreo del departamento de TIC, no ha sido responsable del control y monitoreo de algunos de los accesos a los sistemas de información de la entidad. Se comprobó, las siguientes áreas ejerciendo dicha función:

a. División de operaciones TIC (Infraestructura).
b. División de administración de servicios TIC.
c. Departamento de Recursos Humanos.

El marco de evaluación de Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT 4.1), en los procedimientos PO4.11 Segregación de funciones, PO4.13 Personal clave de TI y PO7.5 Dependencia Sobre los Individuos, expresa:

"PO4.11 Segregación de funciones. - Implementar una división de roles y responsabilidades que reduzca la posibilidad de que un solo individuo afecte negativamente un proceso crítico. La gerencia también se asegura de que el personal realice sólo las tareas autorizadas, relevantes a sus puestos y posiciones respectivas.

PO4.13 Personal clave de TI.- Definir e identificar al personal clave de TI y minimizar la dependencia en un solo individuo desempeñando una función de trabajo crítica.

PO7.5 Dependencia Sobre los Individuos. - Minimizar la exposición a dependencias críticas sobre individuos clave por medio de la captura del conocimiento (documentación), compartir el conocimiento, planeación de la sucesión y respaldos de personal".

La Dirección de Tecnología de la Información y Comunicación ha delegado funciones o permitido que otras áreas realicen funciones propias de la División de Seguridad y Monitoreo TIC.

Recomendaciones:

Al director general le corresponde,

1. Gestionar la revisión de las funciones a desempeñar por la división/departamento/sección/unidad de monitoreo y seguridad TIC para diseñar un

plan para segregar las tareas según el puesto y función que le corresponde desempeñar a cada colaborador.

2. Garantizar que desde la Dirección de Tecnología de la Información y Comunicación la división/departamento/sección/unidad de monitoreo y seguridad TIC cumplan con funciones de asegurar la confidencialidad, disponibilidad e integridad de las informaciones procesadas por los sistemas internos y externos manteniendo una conectividad a los mismos.

Reacción de la ex administración de la entidad:

Mediante comunicación de réplica de fecha 16 de septiembre de 2022, Yokasta Altagracia Guzmán, cédula de identidad y electoral, n.° 001-0081375-7, exdirectora general de la Dirección General de Contrataciones Públicas, expresa:

1. *"Se elaboraron un conjunto de políticas para TIC en el 2015, las cuales se mantuvieron en uso debido a que estaban elaboradas alineadas con COBIT.*
2. *Se crearon los procedimientos de tecnología, 2014.*
3. *Se actualizaron los Procedimientos de Tecnología, incluyendo los de Seguridad, 2019.*

Los procesos definidos y existentes indican que el control de Asistencia (poncheo en relojes) es responsabilidad del Departamento de RRHH y el soporte y mantenimiento de los biométricos es responsabilidad de TIC.

El sistema de Cámaras de CCTV de la institución, a nivel gestión y supervisión fue entregado al área de seguridad física (militar) en el período septiembre 2020 (Ver con el Capitán Rizik).

Los accesos remotos a los sistemas, que se realizan mediante clientes VPN, se encuentran documentados y bajo procedimiento definidos a cargo del área de Seguridad TIC (Líder Eddy Acevedo).

Los mencionados documentos reposan en el archivo institucional".

Comentarios y conclusiones de los auditores de la CCRD

Luego de una revisión exhaustiva y en vista a la carencia de información necesaria en la que se pudiera ver la subsanación se mantiene la observación en el informe.

2.8 Falta de un aplicativo para monitoreo de los controles de TIC.

En el levantamiento de informaciones en el departamento de TIC (el área de seguridad y monitoreo TIC), realizados en los meses de septiembre y octubre de 2021, se verificó que la entidad no cuenta con un aplicativo y/o software de monitoreo que permita alertar e identificar de forma oportuna y efectiva cualquier cambio accidental o intencional en los sistemas de información, base de datos, servidor de archivo, respaldo en disco o portal transaccional.

La Norma para la Implementación y Gestión de la Conectividad en el Estado Dominicano NORTIC B1 de 2016, en su sección 5.04 Herramientas y Sistemas de Monitoreo, literales, establece:

"(a) Todos los componentes de la infraestructura de TIC deben ser monitoreados continuamente en conjunción con la gestión de eventos, de modo que los posibles problemas o las tendencias pueden ser identificadas antes de que se produzcan un fallo o cualquier evento de degradación de rendimiento.

(b) La vigilancia debe ser automatizada y la misma debe tener alertas periódicas con las acciones correctivas que permitan evitar que ocurra un impacto adverso en la infraestructura.

(c) El departamento de TIC debe tener un Software de Gestión de la Infraestructura del Centro de Datos (DCIM, por sus siglas en inglés) para su monitoreo y gestión.

(d) El departamento de TIC debe disponer de un Centro de Control de la Red (NOC, por sus siglas en inglés), y que el mismo brinde servicios las 24 horas, 7 días de la semana, los 365 días del año.

(e) Los componentes y elementos identificados por el organismo que deben de ser objeto de seguimiento y monitoreo, como mínimo debe evaluarse lo siguiente:

- *La utilización de la Unidad Central de Procesamiento (CPU, por sus siglas en inglés).*
- *La utilización del almacén de archivos, tales como:*
  - *Discos duros.*
  - *Particiones.*
  - *Segmentos.*

EL
ES

- *El uso de las aplicaciones.*
- *La utilización de bases de datos.*
- *Tasas de transacción, tasas de error y reintentos.*
- *Los números de sistemas/aplicación inicios de sesión y usuarios concurrentes.*
- *Los números de nodos de red en uso, y los niveles de utilización.*

El encargado de TIC vía correo electrónico de fecha 22 de octubre de 2021 con el título: Acceso | Auditoría Cámara de Cuentas - Solicitud de datos y comprobantes, solicitud n.° 45 - Información varias, nos responde:

"Por la falta de un procedimiento que inste a los colaboradores técnicos de las diferentes áreas a solicitar y validar estos accesos con la división de ciberseguridad antes de modificar estas opciones y por falta de capacidades de monitoreo/auditoria de los diversos sistemas institucionales".

La Dirección de Tecnología de la Información y Comunicación no posee un control o herramienta con la cual se pueda monitorear de forma oportuna la base de datos, servidores de archivos, recursos tecnológicos de la entidad.

Recomendación:

Al director general le corresponde, instruir a la Dirección de Tecnología de la Información y Comunicación a los fines de evaluar las herramientas necesarias para el monitoreo oportuno de la Base de Datos y la gestión de usuario en el Directorio Activo, para someterlo luego al proceso de adquisición de este para la implementación en la Dirección General de Contrataciones Públicas (DGCP).

Reacción de la ex administración de la entidad:

Mediante comunicación de réplica de fecha 16 de septiembre de 2022, Yokasta Altagracia Guzmán, cédula de identidad y electoral, n.° 001-0081375-7, exdirectora general de la Dirección General de Contrataciones Públicas, expresa:

"Tanto la plataforma del Portal Transaccional como la Institucional cuentan herramientas de monitoreo como el NAGIOS y System Center (de Microsoft) y herramientas propias desarrolladas por el propietario de la solución del Portal Transaccional Vortal.Biz. Adicional a estas y debido a la necesidad de poder contar con una herramienta que pueda consolidar el monitoreo temprano, incluyendo comportamiento utilizando Inteligencia Artificial (IA), la institución lanzó una manifestación de interés y posteriormente la

ES

Licitación Pública Nacional DGCP-CCCLPN-2020-0001, la cual arrojó como resultado de la evaluación técnica que ningún proveedor de los que presentaron propuestas cumplía con las especificaciones técnicas requeridas, declarándose el proceso desierto. Se tenía planificado en el presupuesto y objetivo del Departamento TIC, volver a lanzar el proceso en el año 2021, ya que en el año 2020 no fue posible por la situación de emergencia generada por la pandemia. Debido a lo anterior, en la documentación institucional puede encontrarse la publicación de la manifestación de interés, la convocatoria a la Licitación Pública Nacional y los demás documentos del proceso, incluyendo las funcionalidades necesarias para realizar el monitoreo.

Destacamos que durante el año 2020 la institución enfocó sus esfuerzos y recursos a través de la herramienta de teletrabajo para dar soporte a las instituciones, los proveedores y responder consultas de la sociedad. También a asistir técnicamente a la Comisión de Veeduría creada mediante Decreto Núm. 145-20 y a dar seguimiento a que los procesos declarados de Emergencia cumplieran con los requisitos establecidos en el Decreto Núm. 543-12 (Art. 3.2, 4.8, 4.9 y 4.10) del 6 de septiembre del año 2012 que aprueba el Reglamento de aplicación de la Ley Núm. 340-06 y sus modificaciones, los Decretos Núm. 133-20 y 144-20 sobre Declaratoria de Emergencia (instituciones incluidas en la declaratoria y obligatoriedad de publicidad de todos los procesos de Emergencia aún en COVID19), en la "Guía para las Compras y Contrataciones Declaradas de Emergencia" elaborada por la institución y aprobada mediante Decreto Núm. 401-20 (la que tuvo cinco versiones por ser la primera vez que estaba funcionando el Portal Transaccional bajo una Emergencia como el COVID y tras solicitar la Comisión de Veeduría que los documentos que respaldaban cada etapa de cada proceso de Emergencia convocado se publicaran de inmediato y no a los 15 días de concluida la Emergencia como establece el Reglamento de la Ley) y las Circulares DGCP-01-2020 y DGCP-02-2020 de marzo 2020 sobre la obligatoriedad de recibir ofertas en línea en procesos de contratación pública y recomendaciones para los actos de recepción y apertura de ofertas utilizando la tecnología como medida para mitigar la propagación del Coronavirus (COVD-19). Lo que permitió dar cumplimiento a lo establecido en el Decreto Núm. 543-12 que obliga a publicar las convocatorias en los declarados de Emergencia a que todo aquel que pueda y desee participar participe y a que sus ofertas fueran evaluadas.

República Dominicana es el único país que realizó convocatorias públicas a los procesos de emergencia, dando publicidad total y cooperando con los proveedores y mipymes para que pudieran participar. Todos los demás países que declararon emergencia por el COVID-19 realizaron compras directas.

ES

El informe final de la Comisión de Veeduría se encuentra disponible en https://conep.org.do/documentos.

Los mencionados documentos reposan en el archivo institucional".

Comentarios y conclusiones de los auditores de la CCRD

Luego de una revisión exhaustiva y en vista a la carencia de información necesaria en la que se pudiera ver la subsanación se mantiene la observación en el informe.

2.9 Falta de segregación de funciones

Durante los procedimientos de levantamiento de informaciones, aplicación de cuestionarios e indagaciones realizadas a las divisiones y áreas que conforman el departamento de TIC en los meses de septiembre y octubre de 2021, se comprobó que, al momento de los procedimientos, existen debilidades en la segregación de funciones, según describimos a continuación:

1-División de operaciones TIC (Infraestructura) actualmente ejerce las siguientes funciones no propias del área:

i) Implementación desde el área de infraestructura TIC de la DGCP de los controles y mecanismos de seguridad desarrollados que debieron ser implementados por el área de seguridad y monitoreo TIC.
ii) Gestión de los usuarios de las cuentas de usuarios destinados a los servicios, la cual le corresponde al área de seguridad y monitoreo TIC gestionar.

La división de desarrollo e implementación de sistemas realiza el proceso completo para el desarrollo de un sistema o aplicativo incluyendo el desarrollo de la base de datos, el cual se debería de realizar desde el área de infraestructura TIC.

Los analistas funcionales en la gestión de usuario del portal transaccional con la asignación de permisos a los usuarios administrativos roles, que solo debería de tener el área de seguridad y monitoreo TIC.

El administrador de base de datos no desarrolla en la actualidad las bases de datos utilizadas en los aplicativos desarrollados en la DGCP.

El marco de evaluación de Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT 4.1), en el procedimiento PO4.11 Segregación de funciones, PO4.13 Personal clave de TI y PO7.5 Dependencia Sobre los Individuos, expresan:

"PO4.11 Segregación de funciones. - Implementar una división de roles y responsabilidades que reduzca la posibilidad de que un solo individuo afecte negativamente un proceso crítico. La gerencia también se asegura de que el personal realice sólo las tareas autorizadas, relevantes a sus puestos y posiciones respectivas".

"PO4.13 Personal clave de TI.- Definir e identificar al personal clave de TI y minimizar la dependencia en un solo individuo desempeñando una función de trabajo crítica".

"PO7.5 Dependencia Sobre los Individuos. - Minimizar la exposición a dependencias críticas sobre individuos clave por medio de la captura del conocimiento (documentación), compartir el conocimiento, planeación de la sucesión y respaldos de personal".

El encargado de TIC vía correo electrónico de fecha 22 de octubre de 2021 con el título: Acceso | Auditoría Cámara de Cuenta - Solicitud de datos y comprobantes Solicitud n.° 45 - Información varias, nos responde:

"Documento colocado en la carpeta Anexos [ORGANIGRAMA TIC]".

Recomendación:

Al director general le corresponde, gestionar el diseño de un plan para segregar las tareas según el puesto y función que le corresponde desempeñar a cada colaborador y diseñar, crear e implementar los manuales que definan las funciones según el cargo a ocupar en la entidad por el servidor público en la Dirección de Tecnología de la Información y Comunicación.

Reacción de la ex administración de la entidad:

Mediante comunicación de réplica de fecha 16 de septiembre de 2022, Yokasta Altagracia Guzmán, cédula de identidad y electoral, n.° 001-0081375-7, exdirectora general de la Dirección General de Contrataciones Públicas, expresa:

"Ver "Informe referente a la carga operativa y dimensionamiento de TIC" que incluye las mejores prácticas, como un levantamiento de puesto y manual de funciones de los distintos colabores y áreas necesarias para llevar adelante la operación de Departamento TIC y del

Portal Transaccional, como sistema de misión crítica, con el fin de dimensionar el Departamento TIC. En dicho informe se detallan las funciones y responsabilidades de cada posición y se propone una estructura acorde a las necesidades de la institución. La consultoría concluyó en julio del 2020 y por la pandemia no pudo ser implementada. La propuesta fue presentada a las nuevas autoridades para su conocimiento y fines correspondientes.

Los mencionados documentos reposan en el archivo institucional".

Comentarios y conclusiones de los auditores de la CCRD

Luego de una revisión exhaustiva y en vista a la carencia de información necesaria en la que se pudiera ver la subsanación se mantiene la observación en el informe.

2.10 Debilidades de la gestión de respaldos de información (backups).

En cuestionario aplicado en fecha 19 de septiembre de 2021 al Departamento de TIC de la entidad, se verificaron que existen debilidades relacionadas con la gestión de respaldos de la información (backups), que se detallan a continuación:

a. Ausencia de almacenamiento externos de los respaldos de información realizados a la infraestructura interna (archivos, bases de datos de aplicaciones, correo electrónico, active directory, entre otros).
b. Los planes de respaldos y restauración, tanto de la infraestructura interna como del Portal Transaccional no aprobados por la dirección ejecutiva de la DGCP durante el procedimiento realizado.
c. Las pruebas de los respaldos de la información, no se documentan.
d. La herramienta utilizada para la automatización de los respaldos de información de su infraestructura interna (Veritas Backup Exec) sin licenciamiento durante el procedimiento realizado.
e. Usuarios no pertenecientes a la división de operaciones TIC (infraestructura), con accesos a la carpeta donde se encuentran los backups de las bases de datos.

La Norma para la Seguridad de las Tecnologías de la Información y Comunicación en el Estado Dominicano NORTIC A7 de 2016, en la sub-sección 2.03.3. Respaldo de la Información, en sus literales y sus sub-literales, establece:

"Por la naturaleza y alcance de la información generada por los organismos, los procesos de respaldo y restauración de la información son, quizás, los activos más importantes luego de la vida humana. De no disponer de los medios administrativos, procedimientos y recursos técnicos adecuados podría ser imposible llevar a cabo un proceso de continuidad exitoso.

(a) *Los organismos gubernamentales deben tener políticas, procedimientos y recursos tecnológicos para los sistemas de respaldo de la información.*

(i) Los organismos gubernamentales deben definir cuáles informaciones serán incluidas en el respaldo.

a) Las informaciones vitales para el correcto funcionamiento de los organismos deben ser incluidas dentro del programa de respaldo.

(ii) Los organismos gubernamentales deben disponer de un espacio físico y seguro para el almacenamiento de los respaldos.

a) Solo el personal autorizado podrá acceder y manipular los respaldos.

(iii)Los organismos gubernamentales deben asegurar que los datos respaldos están íntegros y libres de errores para su posterior uso.

a) Debe probarse periódicamente y aleatoriamente los respaldos realizados para garantizar su integridad.

(iv) Los organismos gubernamentales deben definir la vigencia que tendrá cada respaldo realizado.

(v) Debe realizarse una frecuencia de respaldo semanal, mensual y anual de todos los datos identificados como críticos para el organismo.

(b) *Los organismos deben presentar información verificable del cumplimiento y nivel de éxito de este proceso.*

(c) *(c) Los organismos deben hacer el aprovisionamiento necesario de medios de almacenamiento para poder cumplir con las demás directivas antes expuestas".*

ES

La referida Norma NORTIC A7 de 2016, en su sub-sección 2.03.3. Respaldo de la Información, Apartado 2.03.3.1 Almacenamiento fuera de sitio, en sus literales y sus sub-literales establece:

"(a) Debe mantener una copia fiel de la información respaldada en una localidad física diferente, fuera de las facilidades inmediatas donde se realiza respaldo.

(i) Esta localidad alternativa debe tener los controles de protección necesarios para que la información guardada no sea dañada tanto por factores ambientales, operacional o mal uso.

(ii) Los medios de respaldo móviles, tales como cintas, y otras unidades externas, deben ser almacenadas bajo llave o con un acceso controlado.

(b) Estos lugares de almacenamiento de los medios deben incluir no solo el control de acceso sino también la protección contra fuego, humedad, electricidad estática e influencia electromagnético, iluminación, entre otros controles de seguridad.

(c) La información respaldada fuera del sitio debe también estar fuera de línea, es decir, que utilice dispositivos discretos que no requieran ni estén conectados a otros sistemas para proteger la información.

(d) Los medios de almacenamiento utilizados deben estar capacitados para proteger la información que contienen, aun después de periodos prolongados, de hasta varios años, sin recibir electricidad.

También el Apartado 2.03.3.3 Confidencialidad de la información almacenada, en sus literales y sus sub-literales, establece:

"(a) Para fines de mantener la confidencialidad de la información respaldada los organismos deben:

(i) Cifrar la información que se encuentra en los medios de respaldo móviles, para lo cual deben hacer las previsiones necesarias para la gestión de las llaves, contraseñas o cualquier otro esquema de autorización.
(ii) No indicar cual información contienen estos medios, para lo cual deben elaborar un esquema de etiquetado que sea útil desde el punto administrativo pero que no revele la información que está respaldada.

(iii)En caso de transporte físico, fuera de las facilidades del organismo, estos medios deben ser transportados por un personal autorizado.

(b) Los medios a transportar no deben ser incluidos en las rutas de trabajo del personal que labora externamente evitando que el dispositivo este los menos posible en posesión de este personal y sean dejado en vehículos o en situaciones de riesgo en que puedan ser perdidos o sustraídos.

(c) El organismo debe disponer de mecanismos administrativos que permitan la rápida y correcta organización y acceso a los medios de almacenamiento externos.

(d) La pérdida de un dispositivo personal con información clasificada del organismo debe ser notificada y ser manejada como un incidente de seguridad de información para ser categorizado y planificar la respuesta correspondiente al nivel del impacto del mismo.

Así mismo, en la subsección 2.03.3. Respaldo de la Información, Apartado 2.03.4.2 Prueba de la recuperación, en sus literales, establece:

"(a) Los organismos deben de disponer de los procesos administrativos y recursos tecnológicos para la verificación de las facilidades de restauración, así como la integridad de la información respaldada.

(b) Los organismos deben disponer de los indicadores necesarios para poder confirmar cuando la prueba ha sido exitosa.

(c) En caso de que las pruebas no arrojen un resultado exitoso, debe abrirse un caso para la identificación y solución de la causa raíz del problema, realizando de nuevo el proceso de respaldo y restauración hasta que los resultados obtenidos sean satisfactorios.

(d) En caso de no poder disponer de los medios, recursos o cualquier otro factor crítico para las pruebas debe notificarse a la alta dirección con el más alto nivel de prioridad para la toma de acción correspondiente".

El encargado de TIC vía correo electrónico de fecha 22 de octubre de 2021 con el título: Acceso | Auditoría Cámara de Cuentas - Solicitud de datos y comprobantes Solicitud n.° 45 - Información varias, nos responde:

"No se tiene contratado un lugar externo para estos fines".

"Los respaldos de información de las bases de datos se realizan directamente desde el gestor de bases de datos debido a que, para el tamaño de nuestra data, resulta más eficiente de esta manera, logrando tiempos de ejecución hasta 5 veces menor que la herramienta de respaldo centralizada existente".

"Ver documentos anexos: Calendario_2019.msg, Calendario_2020.msg, | Restauracion_2019.msg, Restauracion_2020.msg".

"Infraestructura Interna: 60 días en cintas. Portal Transaccional: 14 días en Appliance, 45 días en cintas".

"¿Cuenta la División de Operaciones TIC (Infraestructura) con mecanismos oportunos de alerta para cuando un respaldo de la información, no se ejecute satisfactoriamente? Si".

"Las licencias que utiliza la herramienta son de uso perpetuo. No expiran. La información que se presenta en las imágenes hace referencia a la renovación del soporte y mantenimiento por parte del fabricante al software BackupExec. Esto no quiere decir que el software no esté licenciado, más bien, funciona como un indicador de la herramienta para que los administradores sepan cuando deben renovar el soporte de la misma

A pesar de que la imagen indica que el soporte estaba expirado, lo que el fabricante toma en cuenta a la hora de una solicitud de soporte, es el contrato de renovación que se realiza y este queda registrado en el mismo portal del fabricante de la herramienta como lo indican las siguientes imágenes anexas.

Informamos que, la renovación correspondiente al periodo 2021-2022 ya fue adjudicada en el proceso de compras DGCP-CCC-PEEX-2021-0004".

"Los accesos a esta carpeta han sido asignados por solicitud de las áreas involucradas y por configuración de herencia en los servidores de archivo institucionales, los cuales no son administrados 100% por la división de ciberseguridad, sino que las áreas de infraestructura, administración de servicios y Ciberseguridad otorgan permisos en este servidor. Se necesita un procedimiento oficial estandarizado para la correcta gestión y evaluación de permisos en el servidor de archivos y carpetas criticas como esta".

Recomendaciones:

Al director general le corresponde,

1. Gestionar realizar el análisis, diseño e implementación de un plan de respaldo o backup de las informaciones de la DGCP. También le corresponde al director general garantizar los medios y el cumplimiento del plan de respaldo de la información resguardada en diferente medios interno y externo a la DGCP.

2. Garantizar que se cumpla con los procedimientos establecidos desde el plan de respaldo en el cual se incluirían actividades como:
    - Análisis de las informaciones a incluir en los respaldos.
    - Ejecución del procedimiento de respaldo
    - Prueba de integridad de la información en los respaldos y documentación del proceso.
    - Resguardo interno en los medios destinados y el resguardo externo en una localización segura y accesible en caso de ser requeridos.
    - Pruebas periódicas y aleatoria de los respaldos realizados en la entidad.
    - Descarte y destrucción segura de la información y medios que la contienen.

3. Mantener las herramientas actualizadas y la segregación del personal con acceso a las informaciones contenidas en los respaldos realizados por la entidad.

Reacción de la ex administración de la entidad:

Mediante comunicación de réplica de fecha 16 de septiembre de 2022, Yokasta Altagracia Guzmán, cédula de identidad y electoral, n.° 001-0081375-7, exdirectora general de la Dirección General de Contrataciones Públicas, expresa:

1. *"Las cajas de almacenamiento de la plataforma del Portal Transaccional, como la plataforma institucional superaban los cinco años de obsolescencia. Para el año 2020 el Departamento tuvo como objetivo identificar soluciones que satisficieran la necesidad de almacenamiento y réplica de información en sitios diferentes.*
2. *En el 2020 no se contaba con el presupuesto para su implementación, pero se iniciaron los estudios de mercado de soluciones acorde a las necesidades, planificando lanzar el proceso de licitación en el año 2021.*

3. *"Respaldo de Base de Datos": La solución de respaldo para la plataforma del Portal Transaccional, fue aprobada y validada por el fabricante de la solución y las adecuaciones subsiguientes, con el aumento de capacidad, que cuentan también con este aval.*
4. *Los respaldos se realizan en discos y luego en cintas ubicadas en la Cintoteca del Data Center del Sistema de Emergencias 911.*
5. *Con relación a los correos electrónicos: Desde finales del 2019 y los primeros meses del 2020, se realizó una migración de las bases de datos de correos electrónicos en forma híbrida, con la solución de Office 365 de Microsoft, donde los backups se guardan en la nube de Microsoft. Todos los backups del Data Center de la institución, se guardan en cintas fuera del Data Center, según procedimientos definidos para iniciar las adecuaciones en 2021.*

Los mencionados documentos reposan en el archivo institucional".

Comentarios y conclusiones de los auditores de la CCRD

Luego de una revisión exhaustiva y en vista a la carencia de información necesaria en la que se pudiera ver la subsanación se mantiene la observación en el informe.

2.11 Debilidades de control en el área de desarrollo e implementación de sistemas

Al momento de la realización de los procedimientos de levantamiento, en el mes de septiembre de 2021 en la división de desarrollo e implementación de sistemas, comprobamos las siguientes debilidades en el desarrollo de los sistemas, según describimos a continuación:

a. No se rige por una metodología para el desarrollo de los sistemas.
b. No tienen los controles de las aplicaciones, considerados para el desarrollo de esta, consistentes con los estándares de seguridad de la organización.
c. No se realizan análisis funcional de las soluciones propuesta.
d. No cuenta con un control que les permita a los usuarios finales evaluar todas las etapas de los sistemas desarrollados.
e. No ha desarrollado un mecanismo para medir el grado de satisfacción de los usuarios finales.

La Norma sobre el Desarrollo y Gestión del Software en el Estado Dominicano NORTIC A6 de 2016, en su Sección 2.02 Desarrollo del software gubernamental, establece:

"En el Estado Dominicano son necesarias directrices y políticas para el correcto establecimiento de estándares sobre el software desarrollado en los organismos, para lo cual, en esta sección se establecen las pautas necesarias para lograr un desarrollo óptimo bajo las mejores metodologías y prácticas".

El marco de evaluación de Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT 4.1), en el procedimiento PO8.3 Estándares de Desarrollo y de Adquisición, establece:

"Adoptar y mantener estándares para todo desarrollo y adquisición que siga el ciclo de vida, hasta el último entregable e incluir la aprobación en puntos clave con base en criterios de aceptación acordados. Los temas a considerar incluyen estándares de codificación de software, normas de nomenclatura; formatos de archivos, estándares de diseño para esquemas y diccionario de datos; estándares para la interfaz de usuario; inter operabilidad; eficiencia de desempeño de sistemas; escalabilidad; estándares para desarrollo y pruebas; validación contra requerimientos; planes de pruebas; y pruebas unitarias, de regresión y de integración".

En el procedimiento realizado de fecha 22 de septiembre de 2021 el personal que desempeña las funciones de Encargado de Desarrollo expresó en el documento Evaluación del Área de Desarrollo que no poseen metodología de desarrollo en la Dirección de Tecnología de la Información y Comunicación de la DGCP.

Las debilidades y vulnerabilidades evidenciadas en el área de desarrollo e implementación de sistemas de la DGCP afectan significativamente el resultado de los productos. Las mismas se presentan por la ausencia de políticas, procedimientos, metodologías y controles que garanticen una madurez en el área de desarrollo e implementación.

Recomendaciones:

Al director general le corresponde,

1. Garantizar que la Dirección de Tecnología de la Información y Comunicación establezca y mantenga una metodología de desarrollo que le facilite el desarrollo de soluciones in-house, al igual que la adopción de métodos y estándares y normas que garanticen el ciclo de vida completo de las soluciones desarrolladas en la entidad.

ES

2. Garantizar que el software desarrollado cumpla con los estándares y normativas que garanticen la escalabilidad y permanencia de la inversión resguardando el código fuente para futuras actualizaciones o modificaciones.

Reacción de la ex administración de la entidad:

Mediante comunicación de réplica de fecha 16 de septiembre de 2022, Yokasta Altagracia Guzmán, cédula de identidad y electoral, n.° 001-0081375-7, exdirectora general de la Dirección General de Contrataciones Públicas, expresa:

"Para responder este hallazgo debe separarse el análisis de la siguiente forma:

a.1 En la migración del Sistema Operativo y Base de Datos que se llevó a cabo en el período comprendido entre septiembre - diciembre de 2019, se levantaron las vulnerabilidades detectadas las cuales fueron informadas al fabricante de la solución del Portal Transaccional (Vortal.Biz e INDRA Sistemas), indicando que con la configuración que tenían los equipos es cómo funciona y aprobando esta empresa la arquitectura que actualmente está montada en la plataforma tecnológica. Posteriormente, el fabricante recomendó migrar toda la solución a la versión NEXT VISION que es la evolución para el mercado de la plataforma de su propiedad, lo que fue analizado, pero no decidido, primero por la declaratoria de emergencia que provocó la pandemia y segundo, porque con posterioridad a las elecciones se consideró que era una decisión que correspondía a las autoridades entrantes. Todo lo anterior fue documentado en los informes resultantes de ese proyecto que reposan en los archivos de la institución.

b.1 En la migración del Sistema Operativo y Base de Datos que se llevó a cabo en el período comprendido entre septiembre - diciembre de 2019, se levantaron las vulnerabilidades detectadas las cuales fueron informadas al fabricante de la solución del Portal Transaccional (Vortal.Biz e INDRA Sistemas), indicando que la configuración que tenían los equipos es cómo funciona y aprobando esta empresa la arquitectura que actualmente está montada en la plataforma tecnológica. Posteriormente, el fabricante recomendó migrar toda la solución a la versión NEXT VISION que es la evolución para el mercado de la plataforma de su propiedad, lo que fue analizado pero no decidido, primero por la declaratoria de emergencia que provocó la pandemia y segundo, porque con posterioridad a las elecciones se consideró que era una decisión que correspondía a las autoridades entrantes. Todo lo anterior fue documentado en los informes resultantes de ese proyecto que reposan en los archivos de la institución.

c.1 La gestión de auditoría, control, validación y monitoreo de los accesos, usuarios y permisos a los sistemas, se encuentra documentada por el área de Seguridad TIC (Ing. Eddy Acevedo). Referirse a la documentación que respalda esta respuesta y que se encuentra en los archivos de la institución.

Los mencionados documentos reposan en el archivo institucional.

d, e, f.1 En el año 2020, la institución tenía planificado certificarse en la Norma Nortic A7 e ISO 27001, con relación a Seguridad Informática, para lo cual se publicó un proceso para contratar un consultor que ajustara los requerimientos de Seguridad alineados a las nuevas tecnologías del momento. Adicionalmente, el objetivo de la referida consultoría se extendía a obtener recomendaciones sobre especificaciones de equipos y herramientas de seguridad para mejorar en ese aspecto la Seguridad Informática de la institución. Dicho proceso fue declarado desierto porque el único proveedor que participó no cumplió con la presentación de la documentación técnica/credenciales requeridas. Se recomendó a la nueva gestión proceder al respecto. En el caso particular de la persona señalada que poseía usuario habilitado luego de haber dejado la institución, referimos que para agosto del 2020 la mencionada servidora pública aún prestaba servicios a la institución.

Los mencionados documentos reposan en el archivo institucional.

g.1 1) El código fuente se encuentra en los servidores de despliegue de la Plataforma. El procedimiento definido es que con cada versión que sale a producción del Portal Transaccional se guarda versionado con el código fuente original. El código fuente original de la versión puesta en producción fue depositado en manos de una Notaría Pública levantando un acta notarial que da fe de esta entrega (Recomendamos ver este tema con la Licda. Mercedes Eusebio, Directora de PN&P).

g.1 2) Se contrató a la firma Argentum para realizar una auditoría de calidad de software al Portal Transaccional (LPN2017-0002), incluyendo sus códigos fuentes en 2018 y 2019, encontrándose el informe en los archivos de la institución.

g.1 3) Se inició un proceso para implementar las recomendaciones de la auditoría.

g.1 4) El proveedor entregaba los códigos fuente con cada nueva versión y esta se custodiaba en servidores institucionales.

a) La versión de los códigos fuente se compilaba y desplegaba para prueba y luego en producción; como un mecanismo para asegurar que la institución siempre tuviera

la última versión de los códigos fuente que correspondiera a los programas en operación.

Los mencionados documentos reposan en el archivo institucional.

h.1 Mejora levantada como requerimiento para que el fabricante de la solución desarrolle la funcionalidad. Todos los requerimientos adicionales a la solución base (esa funcionalidad no la tenía definida para la versión contratada) se debe elevar para aprobación y posterior desarrollo en fases subsiguientes del proyecto.

Los mencionados documentos reposan en el archivo institucional".

Comentarios y conclusiones de los auditores de la CCRD

Luego de una revisión exhaustiva y en vista a la carencia de información necesaria en la que se pudiera ver la subsanación se mantiene la observación en el informe.

2.12 Debilidades y vulnerabilidades críticas generales del portal transaccional

Durante los procedimientos realizados en octubre de 2021 al área de seguridad y monitoreo TIC comprobamos que existen vulnerabilidades críticas, las cuales se detallan a continuación:

a. Los equipos FORTINET – FortiGate 500D y FortiGate 600C no se le realizaron actualizaciones al software de los equipos manteniendo la versión 5.2.6 y en la actualidad el proveedor va por la versión 5.2.10.
b. Equipo de balanceo de datos FORTINET – FortiADC 2000D con la configuración de seguridad que el equipo tiene por defecto.
c. Usuario ADMIN utilizado tanto por el área de seguridad y monitoreo TI como por el área de análisis funcional.
d. Usuario ADMIN, quien es utilizado por diferentes servidores públicos sin trazabilidad de eventos realizados (pistas de auditoría).
e. Usuarios no pertenecientes al área de seguridad y monitoreo TIC con acceso a los equipos (FortiGate 500D, frontend) y (FortiGate 600C, backend).
f. Excolaboradores con usuarios activos en el Portal Transaccional (Ejemplo: Aleida Batista - abatista@dgcp.gob.do).

g. El departamento de TIC no cuenta con los accesos al código fuente del Portal Transaccional.
h. Las contraseñas de los usuarios internos y externos del Portal Transaccional no caducan o expiran.

La Norma para la Implementación y Gestión de la Conectividad en el Estado Dominicano NORTIC B1 de 2016, en su sección 5.02 Gestión del centro de datos y Servidores, literal (b) y sub-literales (v, viii y ix), establece:

"(b) Para la correcta administración de los servidores dentro del centro de datos, deben seguirse las directrices a continuación:

(v) Deben realizarse un mantenimiento continuo, el cual incluya la sustitución de servidores antes de estos ser obsoletos para apoyar la evolución de los servicios.
(viii) Todas estaciones de trabajo deben estar protegidas por políticas para ser accedidas solo por el personal autorizado.
(ix) Los servidores de la infraestructura deben tener las últimas actualizaciones y parches de seguridad.

La Norma para la Seguridad de las Tecnologías de la Información y Comunicación en el Estado Dominicano NORTIC A7 de 2016, en la sección 2.02. Políticas para la administración de la información en la sub-sección 2.02.1. Responsabilidad del empleado, en el literal (a) y sus sub-literales (iv y v), establece:

"(a) Los empleados de los organismos gubernamentales deben cumplir con las siguientes responsabilidades:

(iv) El empleado no debe divulgar credenciales que utiliza dentro del organismo gubernamental.

(v) El empleado público no debe divulgar información confidencial a otra personal no autorizado para circular dicha información".

La Norma para la Seguridad de las Tecnologías de la Información y Comunicación en el Estado Dominicano NORTIC A7 de 2016, en la sección 3.01. Control de acceso de usuario en sus literales ((b) (c) (d) y (e)), establece:

ES

"(b) Los organismos gubernamentales deben hacer una revisión de los accesos de los usuarios anualmente. Esta revisión debe estar documentada.

(c) Los organismos gubernamentales deben hacer una revisión, modificación o eliminación de los accesos de los usuarios al momento que estos:

- *Sean cancelados.*
- *Sean promovidos.*
- *Sean transferidos a diferentes localidades.*
- *En caso de fallecimiento.*
- *Cambien de funciones dentro del mismo organismo.*

(d) La unidad de Seguridad y Monitoreo debe tener un personal asignado del área de Administración de accesos para la gestión de accesos de los empleados.

(e) Las aplicaciones deben disponer de un esquema de control de acceso que efectivamente controle la separación de roles de los usuarios administradores y diferentes grupos de usuarios según los perfiles de uso".

La Norma Sobre el Desarrollo y Gestión del Software en el Estado Dominicano NORTIC A6 de 2016, capítulo 2 Administración y Desarrollo de Software en la sección 2.01. Administración del software en la sub-sección 2.01.3. Adquisición del Software, literales ((a) y (d)), establece:

SECCIÓN 2.01. Administración del software

Los organismos gubernamentales requieren políticas y controles para una correcta administración del software, los cuales permitan un control sobre los mismos para asegurar el correcto funcionamiento y desempeño.

Sub-sección 2.01.3. Adquisición del Software

"(a) Los organismos gubernamentales que contraten servicios de desarrollo de aplicaciones, deben exigir a los desarrolladores la propiedad exclusiva de la aplicación y el código fuente desarrollado.

(d) El software de gestión de Servidores Web (http server y servicios relacionados) deben ser abierta".

El Estándar para la Seguridad de la Información de la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional ISO/IEC 27002, en el dominio 6 sobre el Aspecto Organizativo de la Seguridad de la Información Objetivo de Control 6.1 Organización Interna en su Control 6.1.2 Segregación de tareas, establece:

"6.1.2 Segregación de tareas: Se deberían segregar tareas y las áreas de responsabilidad ante posibles conflictos de interés con el fin de reducir las oportunidades de una modificación no autorizada o no intencionada, o el de un mal uso de los activos de la organización".

El Estándar para la Seguridad de la Información de la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional ISO/IEC 27002, en el dominio 9 sobre el Control de Acceso en su Objetivo de Control 9.1 Requisitos de negocio para el control de acceso en sus Controles 9.1.1 Política de control de accesos y 9.1.2 Control de acceso a las redes y servicios asociados, establece:

"9.1.1 Política de control de accesos: Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización.

9.1.2 Control de acceso a las redes y servicios asociados: Se debería proveer a los usuarios de los accesos a redes y los servicios de red para los que han sido expresamente autorizados a utilizar".

El Estándar para la Seguridad de la Información de la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional ISO/IEC 27002, en el dominio 9 sobre el Control de Acceso en su Objetivo de Control 9.2 Gestión de acceso de usuarios en sus Controles del 9.2.1 al 9.2.6, establece:

"9.2.1 Gestión de altas/bajas en el registro de usuarios: Debería existir un procedimiento formal de alta y baja de usuarios con objeto de habilitar la asignación de derechos de acceso.

9.2.2 Gestión de los derechos de acceso asignados a usuarios: Se debería de implantar un proceso formal de aprovisionamiento de accesos a los usuarios para asignar o revocar derechos de acceso a todos los tipos de usuarios y para todos los sistemas y servicios.

9.2.3 Gestión de los derechos de acceso con privilegios especiales: La asignación y uso de derechos de acceso con privilegios especiales debería ser restringido y controlado.

9.2.4 Gestión de información confidencial de autenticación de usuarios: La asignación de información confidencial para la autenticación debería ser controlada mediante un proceso de gestión controlado.

9.2.5 Revisión de los derechos de acceso de los usuarios: Los propietarios de los activos deberían revisar con regularidad los derechos de acceso de los usuarios.

9.2.6 Retirada o adaptación de los derechos de acceso: Se deberían retirar los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información a la finalización del empleo, contrato o acuerdo, o ser revisados en caso de cambio".

El Estándar para la Seguridad de la Información de la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional ISO/IEC 27002, en el dominio 9 sobre el Control de Acceso en su Objetivo de Control 9.4 Control de acceso a sistemas y aplicaciones en su Control 9.4.3 Gestión de contraseñas de usuario, establece:

"9.4.3 Gestión de contraseñas de usuario: Los sistemas de gestión de contraseñas deberían ser interactivos y asegurar contraseñas de calidad".

El Estándar para la Seguridad de la Información de la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional ISO/IEC 27002, en el dominio 12 sobre la Seguridad en la Operativa en su Objetivo de Control 12.4 Registro de actividad y supervisión en su Control 12.4.3 Registro de actividad del administrador y operador del sistema, establece:

"12.4.3 Registros de actividad del administrador y operador del sistema: Se deberían registrar las actividades del administrador y del operador del sistema y los registros asociados se deberían proteger y revisar de manera regular".

El Estándar para la Seguridad de la Información de la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional ISO/IEC 27002, en el dominio 12 sobre la Seguridad en la Operativa en su Objetivo de Control 12.6 Gestión de la vulnerabilidad técnica en su Control 12.6.1 Gestión de vulnerabilidades técnicas, establece:

"12.6.1 Gestión de las vulnerabilidades técnicas: Se debería obtener información sobre las vulnerabilidades técnicas de los sistemas de información de manera oportuna para

evaluar el grado de exposición de la organización y tomar las medidas necesarias para abordar los riesgos asociados".

El marco de evaluación de Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT 4.1), en los procedimientos AI2.3 Control y Posibilidad de Auditar las Aplicaciones, procedimiento, AI2.4 Seguridad y Disponibilidad de las Aplicaciones, AI3.2 Disponibilidad del Recurso de Infraestructura, AI3.3 Mantenimiento de la Infraestructura, y DS3.4 Disponibilidad de Recursos TI, expresa:

"AI2.3 Control y Posibilidad de Auditar las Aplicaciones. - Implementar controles de negocio, cuando aplique, en controles de aplicación automatizados tal que el procesamiento sea exacto, completo, oportuno, autorizado y auditable".

"AI2.4 Seguridad y Disponibilidad de las Aplicaciones. - Abordar la seguridad de las aplicaciones y los requerimientos de disponibilidad en respuesta a los riesgos identificados y en línea con la clasificación de datos, la arquitectura de la información, la arquitectura de seguridad de la seguridad de la información y la tolerancia a riesgos de la organización".

"AI3.2 Protección y Disponibilidad del Recurso de Infraestructura. - Implementar medidas de control interno, seguridad y auditabilidad durante la configuración, integración y mantenimiento del hardware y del software de la infraestructura para proteger los recursos y garantizar su disponibilidad e integridad. Se deben definir y comprender claramente las responsabilidades al utilizar componentes de infraestructura sensitivos por todos aquellos que desarrollan e integran los componentes de infraestructura. Se debe monitorear y evaluar su uso".

"AI3.3 Mantenimiento de la Infraestructura. -Desarrollar una estrategia y un plan de mantenimiento de la infraestructura y garantizar que se controlan los cambios, de acuerdo con el procedimiento de administración de cambios de la organización. Incluir una revisión periódica contra las necesidades del negocio, administración de parches y estrategias de actualización, riesgos y evaluación de vulnerabilidades y requerimientos de seguridad".

"DS3.4 Disponibilidad de Recursos de TI.- Brindar la capacidad y desempeño requeridos tomando en cuenta aspectos como cargas de trabajo normales, contingencias, requerimientos de almacenamiento y ciclos de vida de los recursos de TI. Deben tomarse medidas cuando el desempeño y la capacidad no están en el nivel requerido, tales como dar prioridad a las tareas, mecanismos de tolerancia de fallas y prácticas de asignación de recursos. La gerencia debe garantizar que los planes de contingencia consideran de forma apropiada la disponibilidad, capacidad y desempeño de los recursos individuales de TI".

Recomendaciones:

Al director general le corresponde,

1. Garantizar a través de la Dirección de Tecnología de la Información y Comunicación mantener los equipos del portal transaccional actualizados y configurados para cumplir con el propósito de los mismos.

2. Garantizar la disponibilidad de los servicios ofrecidos desde el portal manteniendo la calidad de los mismos.

3. Instruir a la Dirección de Tecnología de la Información y Comunicación crear e implementar los controles que garanticen una administración transparente y trazable de los usuarios con privilegios del portal transaccional.

4. Garantizar que el código fuente del portal transaccional se encuentre custodiado dentro y fuera de la entidad para los fines de actualizaciones o modificaciones al mismo.

Reacción de la ex administración de la entidad:

Mediante comunicación de réplica de fecha 16 de septiembre de 2022, Yokasta Altagracia Guzmán, cédula de identidad y electoral, n.° 001-0081375-7, exdirectora general de la Dirección General de Contrataciones Públicas, expresa:

"En la migración del Sistema Operativo y Base de Datos que se llevó a cabo en el período comprendido entre septiembre - diciembre de 2019, se levantaron las vulnerabilidades detectadas las cuales fueron informadas al fabricante de la solución del Portal Transaccional (Vortal.Biz e INDRA Sistemas), indicando que con la configuración que tenían los equipos es cómo funciona y aprobando esta empresa la arquitectura que actualmente está montada en la plataforma tecnológica. Posteriormente, el fabricante recomendó migrar toda la solución a la versión NEXT VISION que es la evolución para el mercado de la plataforma de su propiedad, lo que fue analizado pero no decidido, primero por la declaratoria de emergencia que provocó la pandemia y segundo, porque con posterioridad a las elecciones se consideró que era una decisión que correspondía a las autoridades entrantes. Todo lo anterior fue documentado en los informes resultantes de ese proyecto que reposan en los archivos de la institución.

ES

En la migración del Sistema Operativo y Base de Datos que se llevó a cabo en el período comprendido entre septiembre - diciembre de 2019, se levantaron las vulnerabilidades detectadas las cuales fueron informadas al fabricante de la solución del Portal Transaccional (Vortal.Biz e INDRA Sistemas), indicando que la configuración que tenían los equipos es cómo funciona y aprobando esta empresa la arquitectura que actualmente está montada en la plataforma tecnológica. Posteriormente, el fabricante recomendó En la migración del Sistema Operativo y Base de Datos que se llevó a cabo en el período comprendido entre septiembre - diciembre de 2019, se levantaron las vulnerabilidades detectadas las cuales fueron informadas al fabricante de la solución del Portal Transaccional (Vortal.Biz e INDRA Sistemas), indicando que la configuración que tenían los equipos es cómo funciona y aprobando esta empresa la arquitectura que actualmente está montada en la plataforma tecnológica.

Posteriormente, el fabricante recomendó la gestión de auditoría, control, validación y monitoreo de los accesos, usuarios y permisos a los sistemas se encuentra documentada por el área de Seguridad TIC (Ing. Eddy Acevedo). Referirse a la documentación que respalda esta respuesta y que se encuentra en los archivos de la institución.

Los mencionados documentos reposan en el archivo institucional.

En el año 2020, la institución tenía planificado certificarse en la Norma Nortic A7 e ISO 27001, con relación a Seguridad Informática, para lo cual se publicó un proceso para contratar un consultor que ajustara los requerimientos de Seguridad alineados a las nuevas tecnologías del momento. Adicionalmente, el objetivo de la referida consultoría se extendía a obtener recomendaciones sobre especificaciones de equipos y herramientas de seguridad para mejorar en ese aspecto la Seguridad Informática de la institución. Dicho proceso fue declarado desierto porque el único proveedor que participó no cumplió con la presentación de la documentación técnica/credenciales requeridas. Se recomendó a la nueva gestión proceder al respecto.

En el caso particular de la persona señalada que poseía usuario habilitado luego de haber dejado la institución, referimos que para agosto del 2020 la mencionada servidora pública aún prestaba servicios a la institución.

Los mencionados documentos reposan en el archivo institucional.

1. *El código fuente se encuentra en los servidores de despliegue de la Plataforma. El procedimiento definido es que con cada versión que sale a producción del Portal Transaccional se guarda versionado con el código fuente original. El código fuente*

original de la versión puesta en producción fue depositado en manos de una Notaría Pública levantando un acta notarial que da fe de esta entrega (Recomendamos ver este tema con la Licda. Mercedes Eusebio, Directora de PN&P).

2. *Se contrató a la firma Argentum para realizar una auditoría de calidad de software al Portal Transaccional (LPN2017-0002), incluyendo sus códigos fuentes en 2018 y 2019, encontrándose el informe en los archivos de la institución.*
3. *Se inició un proceso para implementar las recomendaciones de la auditoría.*
4. *El proveedor entregaba los códigos fuente con cada nueva versión y esta se custodiaba en servidores institucionales.*

    a. *La versión de los códigos fuente se compilaba y desplegaba para prueba y luego en producción; como un mecanismo para asegurar que la institución siempre tuviera la última versión de los códigos fuente que correspondiera a los programas en operación. Los mencionados documentos reposan en el archivo institucional.*

Mejora levantada como requerimiento para que el fabricante de la solución desarrolle la funcionalidad. Todos los requerimientos adicionales a la solución base (esa funcionalidad no la tenía definida para la versión contratada) se debe elevar para aprobación y posterior desarrollo en fases subsiguientes del proyecto.

Los mencionados documentos reposan en el archivo institucional".

Comentarios y conclusiones de los auditores de la CCRD

Luego de una revisión exhaustiva y en vista a la carencia de información necesaria en la que se pudiera ver la subsanación se mantiene la observación en el informe.

2.13 Falta de controles en asignación de roles en el servidor de bases de datos

En el análisis realizado a los resultados de los SCRIPTS ejecutados en fecha 29 de septiembre de 2021 en el Servidor de SQL donde se desarrollan y gestionan las bases de datos, con apoyo del personal del área de administración de base de datos del departamento de TIC, se verificaron al momento de la auditoria las siguientes situaciones:

ES

a. Existen siete (7) empleados con rol fijo "sysadmin". Incluyendo colaboradores que ejercen las funciones de administradores de base de datos. Los miembros del rol citado pueden realizar cualquier actividad en el Servidor.
b. Proveedor del Portal Transaccional con usuarios habilitados (Ejemplo: po-indra1)
c. Existen ocho (8) cuentas de servicio con rol fijo "sysadmin" (Ejemplos: nextdbapp, pacc, entre otras).

La Norma sobre el Desarrollo y Gestión del Software en el Estado Dominicano NORTIC A6 de 2016, en su sub-sección 4.02.2 Monitoreo y afinamiento de una base de datos, establece:

"(a) El organismo debe contar con herramientas que aseguren la operación y el funcionamiento de la base de datos y esta debe contar con las siguientes características como mínimo:

- *Indicadores de rendimiento: La Unidad de Procesamiento Central (CPU, por sus siglas en inglés), memoria física y disco duro.*
- *Capacidad de identificar segmentos de código con problemas.*
- *Disponer de informes de gestión.*
- *Almacenamiento de informes de rendimiento.*

(b) La herramienta de monitoreo usada o adquirida por el organismo debe informar acerca de los siguientes estados:

- *La carga del trabajo: Para verificar la demanda a la que es sometido el DBMS.*
- *Volumen de trabajo: Para definir la capacidad del servidor para procesar datos, en términos de recursos de hardware.*
- *Los recursos: Para administrar el hardware y las herramientas de software como:*

  - *El Kernel de la base de datos.*
  - *Los controladores de caché.*
  - *Los discos duros.*

- *La contención: Para cuando la carga a la que es sometido el DBMS es muy alta y se encuentran comprometidos todos los recursos del servidor*

ES

(c) Para el afinamiento de la base de datos deben aplicarse las siguientes practicas:

(i) Identificar que las tablas tengan los índices adecuados para responder de la manera correcta a las consultas de los usuarios.
(ii) Configurar adecuadamente la memoria y los cachés de datos y procedimientos.
(iii)Alinear la implementación de las bases de datos con la infraestructura de TIC existente.
(iv) Monitorear constantemente las bases de datos y las aplicaciones.
(v) Implementar procedimientos de reorganización de las bases de datos.
(vi) Implementar procedimientos de actualización de las estadísticas de las bases de datos".

El Estándar para la Seguridad de la Información de la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional ISO/IEC 27001 en el Dominio 9. Acceso, y Objetivo de Control 9.2 Gestión de acceso de usuario, establece:

"9.2.3 Gestión de los derechos de acceso con privilegios especiales: La asignación y uso de derechos de acceso con privilegios especiales debería ser restringido y controlado,

9.2.6 Retirada o adaptación de los derechos de acceso: Se deberían retirar los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información a la finalización del empleo, contrato o acuerdo, o ser revisados en caso de cambio".

Los procedimientos realizados con el personal que administra y gestiona las bases de datos evidenciaron debilidades críticas en los servicios y procedimientos internos que se realizan en la DGCP. Usuarios con privilegios Administrador que representan un riesgo tecnológico alto.

Recomendaciones:

Al director general le corresponde,

1. Gestionar a través de las áreas técnicas del departamento de Tecnología de la Información y Comunicación a fortalecer los controles implementados en el diseño y aplicación de las diferentes bases de datos en producción de la entidad. Al igual que el saneamiento de los usuarios en las bases de datos en el uso de las buenas prácticas acogidas por la Dirección de Tecnología de la Información y Comunicación.

ES

2. Garantizar que los controles diseñados e implementados para las bases de datos de la entidad estén siendo ejecutado desde la Dirección de Tecnología de la Información y Comunicación.

Reacción de la ex administración de la entidad:

Mediante comunicación de réplica de fecha 16 de septiembre de 2022, Yokasta Altagracia Guzmán, cédula de identidad y electoral, n.° 001-0081375-7, exdirectora general de la Dirección General de Contrataciones Públicas, expresa:

1. *"No se especifica de que base de datos SQL se hace referencia.*

2. *En el caso de la Plataforma del Portal Transaccional, en la migración que se llevó a cabo entre septiembre y diciembre de 2019, se acordó entre el fabricante de la solución, el área de Seguridad TIC y de Administración de Base de Datos, los usuarios, permisología y funciones de cada usuario. Teniendo bajo sobre los usuarios auditados en el caso de su apertura y uso. Estas funciones se encuentran bien definidas bajo la responsabilidad del área de Seguridad TIC (líder Ing. Eddy Acevedo).*

Los mencionados documentos reposan en el archivo institucional".

Comentarios y conclusiones de los auditores de la CCRD

Luego de una revisión exhaustiva y en vista a la carencia de información necesaria en la que se pudiera ver la subsanación se mantiene la observación en el informe.

III. CONCLUSIONES GENERALES

La estructura de control interno del Departamento de Tecnología de la Información y Comunicación de la **Dirección General de Contrataciones Públicas (DGCP),** presenta debilidades importantes según se especifica en el contenido de este informe de evaluación al Departamento de Tecnología de la Información y Comunicación y recursos tecnológicos, su permanencia vulnera la calidad, confiabilidad, integridad, confidencialidad y disponibilidad de las informaciones. Esta afirmación está fundada en las debilidades de TI detectadas que incluyen:

- Debilidades y vulnerabilidades de gestión del departamento TIC
- Revisión y/o actualización de las políticas y procedimientos de TIC
- El departamento de TIC no cuenta con una herramienta o matriz de riesgo
- Vulnerabilidades del centro de datos (Data Center)
- Ausencia de controles en el Servidor de dominio
- Estructura organizativa del departamento de TIC no alineada a órganos rectores
- Falta de control y monitoreo en los accesos a los sistemas de información
- Carencia de un aplicativo para monitoreo de los controles de TIC
- Falta de segregación de funciones
- Debilidades de la gestión de respaldos de información (backups)
- Debilidades de control en el área de desarrollo e implementación de sistemas
- Debilidades y vulnerabilidades criticas generales del portal transaccional
- Falta de controles en asignación de roles en el servidor de bases de datos

IV. RECOMENDACIÓN GENERAL

Para contribuir al mejoramiento del Departamento de Tecnología de la Información y Comunicación y los controles de TI que permitan garantizar la integridad, confidencialidad y disponibilidad de la información financiera de la **Dirección General de Contrataciones Públicas (DGCP)**, la Cámara de Cuentas de la República Dominicana (CCRD), en ejercicio de sus facultades que le otorga la Constitución de la República, en su artículo 248 sobre control externo y la Ley n.°10-04 de la Cámara de Cuentas, del 20 de enero de 2004, en su artículo 39, Recomendaciones; luego de concluida la auditoría financiera, recomienda:

- Garantizar vía la Dirección de Tecnología de la Información y Comunicación el cumplimiento de la Norma General Sobre el Uso e Implementación de las Tecnologías de la Información y Comunicación en el Estado Dominicano. NORTIC A1 de 2014, Norma para la Seguridad de las Tecnologías de la Información y Comunicación en el Estado dominicano NORTIC A7 de 2016, Norma para la Implementación y Gestión de la Conectividad en el Estado Dominicano NORTIC B1 de 2016, marco de evaluación de Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT 2019).

4 de mayo de 2023
Santo Domingo, D. N.,
República Dominicana

CÁMARA DE CUENTAS DE LA REPÚBLICA DOMINICANA
Santo Domingo, R. D.

ENLLY C. SANTOS UREÑA, CPA
SUPERVISORA DE GRUPOS DE AUDITORÍA

EVELYN A. PEGUERO AURICH, CPA
DIRECTORA INTERINA DE AUDITORÍA

CÁMARA DE CUENTAS
DE LA REPÚBLICA DOMINICANA

RESOLUCIÓN N.° AUD-2023-005
EMANADA DE LA SESIÓN ORDINARIA CELEBRADA
POR EL PLENO EN FECHA 4 DE MAYO DE 2023

INFORME LEGAL

INFORME DE EVALUACIÓN PRACTICADO POR LA CÁMARA DE CUENTAS DE LA REPÚBLICA DOMINICANA AL DEPARTAMENTO DE TECNOLOGÍA DE LA INFORMACIÓN, COMUNICACIÓN Y RECURSOS TECNOLÓGICOS DE LA DIRECCIÓN GENERAL DE CONTRATACIONES PÚBLICAS (DGCP)

POR EL PERÍODO COMPRENDIDO ENTRE EL 1. ° DE ENERO DE 2017 Y EL 31 DE DICIEMBRE DE 2020

CCRD
CÁMARA DE CUENTAS
DE LA REPÚBLICA DOMINICANA

CÁMARA DE CUENTAS
DE LA REPÚBLICA DOMINICANA

RESOLUCION

CCRD
CÁMARA DE CUENTAS
DE LA REPÚBLICA DOMINICANA

REPÚBLICA DOMINICANA
CÁMARA DE CUENTAS DE LA REPÚBLICA

En nombre de la República, la Cámara de Cuentas, regularmente constituida por el Pleno de sus miembros: **Lic. Janel Andrés Ramírez Sánchez,** presidente; **Lcda. Elsa María Catano Ramírez,** vicepresidenta; **Lcda. Tomasina Tolentino de Mckenzie,** miembro secretaria del Bufete Directivo; **Lic. Mario Arturo Fernández Burgos,** miembro, y **Lcda. Elsa Peña Peña,** miembro; asistidos por la secretaria general auxiliar, Lcda. Iguemota Lubienka Alcántara Báez de Peña, en la sala donde acostumbra a celebrar sus sesiones, sita en el 9.° piso del Edificio Gubernamental Manuel Fernández Mármol, ubicado en la avenida 27 de Febrero, esquina calle Abreu, de la ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, hoy día cuatro (4) del mes mayo del año 2023, años 180 de la Independencia y 159 de la Restauración, dicta en sus atribuciones de Órgano Superior de Control y Fiscalización del Estado, Rector del Sistema Nacional de Control y Auditoría, la siguiente resolución:

RESOLUCIÓN N.° AUD-2023-005
EMANADA DE LA SESIÓN ORDINARIA CELEBRADA POR EL PLENO
EN FECHA 4 DE MAYO DEL AÑO 2023

ATENDIDO, a que la Cámara de Cuentas de la República es un órgano instituido por la Constitución de la República Dominicana con carácter principalmente técnico, y en tal virtud le corresponde el examen de las cuentas generales y particulares del Estado, mediante la realización de auditorías, estudios e investigaciones especiales, tendentes a evidenciar la transparencia, eficacia, eficiencia y economía en el manejo y utilización de los recursos públicos por sus administradores o detentadores.

ATENDIDO, a que la Cámara de Cuentas de la República realizó una evaluación al Departamento de Tecnología de la Información Comunicación y Recursos Tecnológicos de la Dirección General de Contrataciones Públicas (DGCP), por el período comprendido entre el 1.° de enero de 2017 y el 31 de diciembre de 2020.

ATENDIDO, a que el informe de evaluación practicada por la Cámara de Cuentas de la República al Departamento de Tecnología de la Información Comunicación y Recursos Tecnológicos de la Dirección General de Contrataciones Públicas (DGCP), por el período comprendido entre el 1.° de enero de 2017 y el 31 de diciembre de 2020, evidencia las observaciones siguientes:

II. Resultados de la evaluación

2.1 Debilidades y vulnerabilidades de gestión del departamento TIC.
2.2 Revisión y/o actualización de las políticas y procedimientos de TIC.
2.3 El departamento de TIC no cuenta con una herramienta o matriz de riesgo.

2.4 Vulnerabilidades del centro de datos (Data Center).
2.5 Ausencia de controles en el Servidor de dominio.
2.6 Estructura organizativa del departamento de TIC no alineada a Órganos rectores.
2.7 Falta de control y monitoreo en los accesos a los sistemas de información.
2.8 Falta de un aplicativo para monitoreo de los controles de TIC.
2.9 Falta de segregación de funciones.
2.10 Debilidades de la gestión de respaldos de información ("backups").
2.11 Debilidades de control en el área de desarrollo e implementación de sistemas.
2.12 Debilidades y vulnerabilidades críticas generales del portal transaccional.
2.13 Falta de controles en asignación de roles en el servidor de bases de datos.

ATENDIDO, a que en el caso de la especie, la Cámara de Cuentas de la República dio estricto cumplimiento a las disposiciones constitucionales y legales que instituyen el derecho de defensa y regulan el debido proceso que debe ser observado; en tal sentido, procedió a notificar mediante comunicaciones n.^{os} 012001/2022 y 012002/2022, de fecha 1.° de septiembre del año 2022, al director general y a la exdirectora general de Compras y Contrataciones Públicas, el informe provisional de evaluación al Departamento de Tecnología de la Información y Comunicación y Recursos Tecnológicos de la Dirección General de Contrataciones Públicas (DGCP), por el período comprendido entre el 1.° de enero de 2017 y el 31 de diciembre de 2020; a los fines de que procedan de conformidad con las disposiciones de la Ley n.° 10-04, de fecha 20 de enero del año 2004, y su Reglamento de Aplicación n.° 06-04, de fecha 20 de septiembre del año 2004, comunicaciones que fueron debidamente recibidas, motivo por el cual, luego del análisis y ponderación de los escritos de réplica correspondientes, procede la emisión del informe final de la presente evaluación, de conformidad con las disposiciones contenidas en la legislación que regula la materia.

ATENDIDO, a la inobservancia de la etapa de reparos por los funcionarios que resultaron auditados, que fueron debidamente comunicados del informe provisional, procede la emisión del informe final de la presente auditoría, de conformidad con las disposiciones contenidas en la legislación que regula la materia.

ATENDIDO, a que la Dirección General de Contrataciones Públicas (DGCP) se encuentra dentro del ámbito de aplicación de la Ley n.° 10-04, de fecha 20 de enero del año 2004, y su Reglamento de Aplicación n.° 06-04, de fecha 20 de septiembre del año 2004.

ATENDIDO, a que en el ejercicio de sus funciones, la Cámara de Cuentas de la República Dominicana debe observar y dar estricto cumplimiento a las disposiciones legales que regulan la obtención de las informaciones; de modo tal, que no se vulneren los derechos legítimamente protegidos de los auditados.

ATENDIDO, a que de conformidad con las prescripciones del artículo 20, numeral 9, de la Ley n.° 10-04, de fecha 20 de enero del año 2004, son atribuciones del presidente las siguientes:

"Artículo 20.- Atribuciones del presidente. El presidente de la Cámara de Cuentas es el representante legal de la institución y su máxima autoridad ejecutiva en todos los asuntos administrativos y técnicos. En tal virtud le corresponde:

9) Firmar la correspondencia y la documentación general de la Cámara de Cuentas en su interrelación con otras instituciones públicas o privadas."

ATENDIDO, a que la Ley General de Libre Acceso a la Información Pública n.° 200-04, de fecha 28 de julio del año 2004, consigna de manera taxativa la obligación de todas las instituciones y personas que desempeñen funciones públicas, de informar a la ciudadanía sobre los pormenores de sus actividades.

VISTO, el informe de evaluación al departamento de Tecnología de la Información y Comunicación y Recursos Tecnológicos de la Dirección General de Contrataciones Públicas (DGCP), por el período comprendido entre el 1.° de enero de 2017 y el 31 de diciembre de 2020.

VISTA, la Constitución de la República Dominicana.

VISTA, la Ley n.° 10-04, de fecha 20 de enero del año 2004, de la Cámara de Cuentas de la República Dominicana, y su Reglamento de Aplicación n.° 06-04, de fecha 20 de septiembre del año 2004.

VISTA, la Ley n.° 494-06, de fecha 21 de diciembre del año 2006, de Organización de la Secretaria de Estado de Hacienda (actual Ministerio de Hacienda).

VISTA, la Ley n.° 340-06, de fecha 18 de agosto del año 2006, modificada por la Ley n.° 449-06, de fecha 6 de diciembre del año 2006, sobre Compras y Contrataciones de Bienes, Servicios, Obras y Concesiones, y sus reglamentos de Aplicación n.os 490-07 y 543-12, de fechas 30 de agosto del año 2007 y 6 de septiembre del año 2012, respectivamente.

VISTA, la Ley n.° 10-07, de fecha 8 de enero del año 2007, que instituye el Sistema Nacional de Control Interno y de la Contraloría General de la República.

VISTA, la Ley n.° 200-04, de fecha 28 de julio del año 2004, General de Libre Acceso a la Información Pública.

VISTOS, los marcos de control y estándares de buenas prácticas reconocidos a nivel nacional e internacional, tales como:

- COBIT (Objetivos de Control para Información y Tecnologías Relacionadas, en inglés: Control Objectives for Information and related Technology).
- ITIL (Biblioteca de Infraestructura de Tecnología de Información, en inglés: Information Technology Infrastructure Library).
- ISO (Organización Internacional de Normalización, en inglés: International Standarization Organization).

- ANSI/TIA-942-A (Asociación de la Industria de Telecomunicaciones, Norma de Infraestructura de Telecomunicaciones para Centros de Datos, en inglés: (The Telecommunications Industry Association (TIA) Telecommunications Infrastructure Standard for Data Centers is an American National Standard (ANS).
- NORTIC (Normas de Tecnologías de la Información y Comunicación, creadas en el año 2013 por el Departamento de Estandarización, Normativa y Auditoría Técnica (ENAT).

Por tales motivos, la Cámara de Cuentas de la República Dominicana, después de haber deliberado,

R E S U E L V E:

ARTÍCULO PRIMERO: APROBAR, como al efecto **APRUEBA,** el Informe Final de evaluación al Departamento de Tecnología de la Información Comunicación y Recursos Tecnológicos de la Dirección General de Contrataciones Públicas (DGCP), por el período comprendido entre el 1.° de enero de 2017 y el 31 de diciembre de 2020, y el Informe Jurídico correspondiente, los cuales forman parte integral de la presente resolución.

ARTÍCULO SEGUNDO: DECLARAR, como al efecto **DECLARA**, que después de haber expuesto los detalles en las conclusiones generales, que la estructura de control interno del Departamento de Tecnología de la Información y Comunicación de la **Dirección General de Contrataciones Públicas (DGCP)** presenta debilidades importantes, según se especifica en el contenido de este informe de evaluación al Departamento de Tecnología de la Información y Comunicación y recursos tecnológicos, su permanencia vulnera la calidad, confiabilidad, integridad, confidencialidad y disponibilidad de las informaciones. Esta afirmación está fundada en las debilidades de TIC detectadas, que incluyen:

- Debilidades y vulnerabilidades de gestión del departamento de TIC.
- Revisión y/o actualización de las políticas y procedimientos de TIC.
- El departamento de TIC no cuenta con una herramienta o matriz de riesgo.
- Vulnerabilidades del centro de datos (Data Center).
- Ausencia de controles en el Servidor de dominio.
- Estructura organizativa del departamento de TIC no alineada a órganos rectores.
- Falta de control y monitoreo en los accesos a los sistemas de información.
- Falta de un aplicativo para monitoreo de los controles de TIC.
- Falta de segregación de funciones.
- Debilidades de la gestión de respaldos de información ("backups").
- Debilidades de control en el área de desarrollo e implementación de sistemas.
- Debilidades y vulnerabilidades criticas generales del portal transaccional.
- Falta de controles en asignación de roles en el servidor de bases de datos.

ARTÍCULO TERCERO: REMITIR, como al efecto **REMITE**, la presente resolución al ente auditado, al director general y a la exdirectora general de Compras y Contrataciones Públicas, a la Contraloría General de la República, así como a cualquier organismo contemplado en la ley, a efectos de que observen las disposiciones de los artículos 47 y 54 de la Ley n.° 10-04, de fecha 20 de enero del año 2004, y procedan con las medidas pertinentes, en ocasión de las conclusiones generales de los auditores, en donde expresan que la estructura de control interno del Departamento de Tecnología de la Información Comunicación y Recursos Tecnológicos de la Dirección General de Contrataciones Públicas (DGCP), presenta debilidades importantes; y del Informe Jurídico, el cual expresa que los hallazgos advertidos constituyen inobservancias a las obligaciones que impone el marco normativo de control interno y las normas específicas al área de tecnología NORTIC.

ARTÍCULO CUARTO: INFORMAR, como al efecto se **INFORMA**, que esta resolución cabe interponer recurso de reconsideración y/o recurrir ante la vía contencioso-administrativa, de conformidad a los términos y plazos, contados a partir de la notificación de la presente, establecidos en la Ley n.° 107-13, sobre derecho de las personas en sus relaciones con la Administración Pública y de Procedimiento Administrativo, la Ley n.° 13-07, que crea Tribunal Contencioso Tributario y Administrativo, así como de la Ley n.° 10-04, de la Cámara de Cuentas.

Dada en la ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, a los cuatro (4) días del mes de mayo del año dos mil veintitrés (2023), años 180 de la Independencia y 159 de la Restauración.

Firmado:

Lcda. Elsa María Catano Ramírez
Vicepresidenta

Lcda. Tomasina Tolentino de Mckenzie
Miembro Secretaria del Bufete Directivo

Lcda. Elsa Peña Peña
Miembro

Aprobada con el voto de tres (3) de los cinco (5) miembros del Pleno. Votos disidentes de los licenciados Janel Andrés Ramírez Sánchez, presidente, y Mario Arturo Fernández Burgos, miembro.
**********ÚLTIMA LÍNEA**********

CÁMARA DE CUENTAS
DE LA REPÚBLICA DOMINICANA

INFORME LEGAL

CCRD
CÁMARA DE CUENTAS
DE LA REPÚBLICA DOMINICANA

Disposiciones jurídicas que sustentan el informe de evaluación practicado por la Cámara de Cuentas de la República al departamento de Tecnología de la Información y Comunicación y Recursos Tecnológicos de la Dirección General de Contrataciones Públicas (DGCP) por el período comprendido entre el 1ro. de enero de 2017 y el 31 de diciembre del año 2020

Atendido, a que corresponde ampliar el análisis jurídico, normas y reglamentaciones que deben ser observadas por los entes auditados y/o investigados, de conformidad con las disposiciones de la Ley n.° 10-04 de fecha 20 de enero del año 2004 y, su Reglamento de Aplicación n.° 06-04 de fecha 20 de septiembre del año 2004.

Atendido, a que, en la actualidad, el uso de las TIC en el quehacer estatal está directamente vinculado a la observancia de principios rectores de la administración pública, tales como transparencia, eficacia y publicidad. En este sentido, las áreas que gerencian el componente de tecnología de cada entidad resultan sustanciales pues se encargan del manejo de los sistemas de almacenamiento y empleo de la información, así como de coadyuvar a la transparencia en la función pública y de garantizar la efectividad en los canales de comunicación y contacto entre la ciudadanía y el Estado.

Atendido, a que, en consecuencia, los departamentos de TIC de cada entidad de la administración pública, en los asuntos de su competencia, están llamados a velar por que el recurso tecnológico permita la implementación de *"reformas efectivas de transparencia y de gestión de la información"*; así como el fortalecimiento de la *"gestión interna de la información, monitoreo horizontal, monitoreo vertical, retroalimentación de los usuarios y voz ciudadana"*.

Atendido, a que todo ello cobra mayor relevancia al tratarse de un organismo de especial asignación en la operatividad del Estado, tal lo es la Dirección General de Contrataciones Públicas (DGCP), en razón de que, al tener a su cargo la gestión del sistema de compras y contrataciones públicas, requiere que, en materia de tecnología y sus sistemas electrónicos, preponderen las mejores prácticas, así como de controles suficientes que garanticen el manejo de la información.

Atendido, a que la evaluación practicada al departamento de Tecnología de la Información y Comunicación y Recursos Tecnológicos de la Dirección General de Contrataciones Públicas (DGCP), en el período abarcado, reveló considerables debilidades en el manejo y gestión de esta área evidenciándose ausencia de mecanismos de evaluación y de implementación de sistemas, así como ausencia de planes estratégicos en orden a buenas prácticas, desactualización de políticas y procedimientos, falta de matriz de riesgo, debilidades en los sistemas operativos (accesos a usuarios, contraseñas, falta de aplicativo de monitoreo), debilidad en el respaldo de la información, falta de segregación de funciones organizativas, entre otros aspectos que conllevan la vulnerabilidad general del sistema tecnológico y de la información de la entidad auditada.

Atendido, a que, de manera transversal a los hallazgos acreditados en el informe de evaluación de referencia, resalta faltas en materia de control interno aplicado al área de

tecnología, responsabilidad que atañe a los servidores públicos; por lo cual, de manera general, procede observar las disposiciones siguientes:

Ley n.° 41-08, de Función Pública, de fecha 16 de enero del año 2008

> **Artículo 79.-** Son deberes de los servidores públicos, los siguientes:
>
> **1.** Cumplir y hacer cumplir la Constitución de la República, las leyes, los reglamentos, manuales, instructivos, y otras disposiciones emanadas de autoridades competentes".

Ley n.° 10-07, de fecha 8 de enero del año 2007

> **Artículo 24.- Componentes del Proceso.** El proceso de control interno está integrado por los siguientes componentes:
>
> **1.** Ambiente de Control.
> **2.** Valoración y Administración de Riesgos.
> **3.** Actividades de Control.
> **4.** Información y Comunicación.
> **5.** Monitoreo y Evaluación.

Reglamento de Aplicación de la Ley n.° 10-07, que instituye el Sistema Nacional de Control Interno y de la Contraloría General de la República, de fecha 30 de agosto del año 2007, aprobado mediante decreto n.° 491-07

> **Artículo 47.-Componentes del Proceso de Control Interno.** Con fines de la implantación del proceso de control interno institucional en las entidades y los organismos del ámbito de la Ley 10-07, los cinco componentes previstos en el artículo 24, de la Ley, se definen como sigue:
>
> **1. Ambiente de Control:** La administración activa, principalmente el titular de cada entidad y organismo público del ámbito de la Ley debe fomentar un ambiente propicio para la operación del control interno, mediante la generación de una cultura de administración y control que promueva, entre el personal de la institución, el reconocimiento del control como parte integrante de los sistemas institucionales. En su calidad de responsable por el proceso de control interno debe mostrar constantemente una actitud de apoyo a las medidas de control implantadas en la institución, mediante la divulgación de éstas y un ejemplo continuo de apego a ellas en el desarrollo de las labores cotidianas. Los elementos principales en que descansa el componente son:
>
> **a)** Integridad y ética pública
> **b)** Compromiso del personal con el control interno
> **c)** Ambiente de confianza
> **d)** Competencia del talento humano
> **e)** La filosofía y estilo de administración
> **f)** Estructura organizacional
> **g)** Acciones coordinadas y coherentes
> **h)** Asignación de responsabilidad
> **i)** Delegación de autoridad
> **j)** Adhesión a las políticas institucionales y específicas aplicables
> **k)** Documentación de los sistemas y procesos
> **l)** Políticas y prácticas de gestión de recursos humanos
>
> **2. Valoración y Administración de Riesgos.** Las entidades y los organismos públicos deberán identificar y evaluar los riesgos relevantes derivados de los factores ambientales que afecten el logro de los objetivos institucionales; así como emprender las medidas pertinentes para afrontar

exitosamente tales riesgos. La gestión de riesgos institucionales es un proceso del cual el control interno es parte integral, que ayuda a la dirección superior de las entidades a administrar eficazmente la incertidumbre y sus riesgos y oportunidades asociadas, para mejorar la capacidad de generar o agregar valor a todos sus grupos de interés, alcanzar los objetivos institucionales y prevenir la pérdida de los recursos, en especial en períodos de cambio. Los elementos principales que se considerarán en este componente son:

a) Determinación de los objetivos institucionales
b) Desarrollo de los objetivos
c) Operaciones y actividades
d) Estándares o indicadores mensurables de resultado, desempeño e impacto de la gestión
e) Identificación de riesgos
f) Determinación de las acciones para administrar los riesgos
g) Revisión periódica de objetivos

3. Actividades de Control. La administración de las entidades y los organismos bajo el ámbito de la Ley 10-07 deberán diseñar y adoptar las medidas y las prácticas de control interno, que mejor se adapten a los procesos organizacionales, a los recursos disponibles, a las estrategias definidas para el enfrentamiento de los riesgos relevantes y a las características, en general, de la institución y sus funcionarios, y que coadyuven, de mejor manera, al logro de los objetivos y la misión institucionales. Los elementos de este componente hacen relación a:

a) Controles integrados e inmersos
b) Análisis costo/beneficio de los controles
c) Actividades de control de los objetivos de las operaciones
d) Actividades de control del sistema de información
e) Actividades de control del cumplimiento y acatamiento legal
f) Actividades de control del cuidado y protección del ambiente

Las actividades de control incorporan, aplican o combinan la gama tradicional de técnicas de control (responsabilidad delimitada, aprobación, autorización, verificación, inspección, confrontación, conciliación, revisión, segregación de funciones, instrucciones escritas, documentación de procesos y transacciones, supervisión, acceso delimitado a activos y registros, arqueos independientes, dispositivos de control y seguridad de los equipos, etc.) y la tipología o clases de control (manuales o electrónicos, físicos o documentales, cuantitativos o cualitativos, absolutos o indicativos, previos o posteriores, etc.)

4. Información y Comunicación. Las entidades y los organismos bajo el ámbito de la Ley 10-07, deben establecer los mecanismos y los sistemas más adecuados para obtener, procesar, generar y comunicar de manera eficaz, eficiente y económica, la información financiera, administrativa, de gestión y de otro tipo requerida en el desarrollo de sus procesos, transacciones y actividades, así como en la operación de sus sistemas de control con miras al logro de los objetivos institucionales. Los principales elementos que se consideran en este componente son:

a) Calidad y suficiencia de la información
b) Sistema integrado de información (financiera y/o de gestión)
c) Controles de acceso, aplicación y otros de los sistemas integrados
d) Canales de comunicación interna y externa
e) Archivo institucional

5. Monitoreo y Evaluación. Se deberá observar y evaluar de manera continuada el funcionamiento de los diversos controles, con el fin de determinar la vigencia, efectividad y calidad del control interno en el marco del Sistema Nacional de Control Interno; para identificar sus debilidades, identificar y emprender las acciones correctivas o de mejora y, darles seguimiento; para mantener o incrementar su efectividad con relación al logro de los objetivos del control interno y formular recomendaciones para agregar valor al control de los procesos de

los sistemas que componen y se relacionan con el Sistema Integrado de Administración Financiera del Estado, en función del logro de los objetivos institucionales. Los elementos principales de este componente son:

a) Supervisión permanente de la efectividad de los controles
b) Auto evaluación de control interno
c) Evaluación de la efectividad del proceso de control interno y de la gestión institucional
d) Evaluación del cumplimiento de los controles previos de las órdenes de pago
e) Evaluación de la calidad y efectividad de la supervisión sobre la ejecución de los contratos de bienes y servicios
f) Evaluación de la calidad de la tecnología informática
g) Evaluaciones de confiabilidad de la información financiera y administrativa de la entidad u organismo
h) Informes de las evaluaciones y formulación de recomendaciones
i) Seguimiento de las recomendaciones.

Atendido, a que con relación al control interno aplicado al área de tecnología en los órganos y entidades de la administración pública resulta necesario observar el conjunto de normativas aplicables, el cual, además de las disposiciones señaladas en el apartado anterior, comprende las siguientes:

- Las normas de tecnologías de la información y comunicación (NORTIC), emitidas por el departamento de estandarización, normativas y auditoría técnica (ENAT) de la oficina presidencial de tecnologías de la información y comunicación (OPTIC), a los fines de normalizar, estandarizar y tener una herramienta de auditoría para el efectivo uso e implementación de las TIC en la administración pública, con el fin de lograr homogeneidad y mejora en los procesos entre los organismos gubernamentales. Estas normas son de aplicación general y mandataria a las entidades adscritas al Poder Ejecutivo de la República Dominicana y de observación a manera de buenas prácticas de los demás órganos del Estado.

- Las directrices contenidas en los objetivos de control para información y tecnologías relacionadas (COBIT); la biblioteca de infraestructura de tecnología de información (ITIL); las normativas ISO, así como el estándar ANSI/TIA-942-A del Instituto Nacional Estadounidense de Estándares y la Asociación de Industria de Telecomunicaciones; todo lo cual opera como marco de referencia a observar en el desarrollo y manejo de lo dispuesto en las NORTIC.

- Respecto de las normativas, estándares y buenas prácticas internacionales que resultan aplicables a la gestión de los departamentos de tecnología del Estado dominicano, especialmente del marco de referencia COBIT, es preciso observar los procesos de gestión de los objetivos a los que se orienta; estos están plasmados en los procesos APO, PO, DSS, y otras, a los cuales hace referencia los hallazgos del informe de la evaluación de que se trató.

Atendido, a que, de manera detallada, el informe de evaluación practicado por la Cámara de Cuentas de la República al departamento de Tecnología de la Información y Comunicación y Recursos Tecnológicos de la Dirección General de Contrataciones Públicas (DGCP) por el

período comprendido entre el 1ro. de enero de 2017 y el 31 de diciembre del año 2020, evidencia los resultados siguientes:

II Resultados de la evaluación

2.1 Debilidades y vulnerabilidades de gestión del departamento TIC [1]

Disposiciones jurídicas

Considerando, que en las debilidades evidenciadas se comprobó la ausencia de mecanismos para evaluar la situación actual tecnológica de la DGCP y la falta de un área que evalué la calidad de los proyectos tecnológicos desarrollados por la entidad; así también no se cuenta con los recursos para el desarrollo e implementación de proyectos basados en buenas prácticas ni con planes de contingencia, de continuidad de negocio y recuperación de desastres.

Considerando, que esto evidencia inobservancia de la entidad respecto de uno de los componentes del proceso de control interno, esto es lo relativo al monitoreo y evaluación de conformidad a las disposiciones del artículo 47 del reglamento de aplicación de la ley 10-07, aprobado mediante decreto número 491-07.

Considerando, que en materia de control interno el cumplimiento del componente de evaluación y monitoreo resulta sustancial pues es la herramienta que permite valorar la eficacia de lo implementado, así como determinar si cualquier cambio surgido en el ambiente amerita realizar ajustes al sistema a fin de dar respuesta a riesgos y/o reenfocar en orden a los objetivos institucionales.

Considerando, que, al reflejarse la ausencia de mecanismos relativos al componente de evaluación en los aspectos señalados, conjuntamente a la inexistencia de recursos para el desarrollo de proyectos acordes a las buenas prácticas y la falta de planes de contingencia, de continuidad de negocio y recuperación de desastres, evidencia desinterés en materia de planificación y monitoreo de los asuntos que competen al departamento de tecnología de la DGCP en el período auditado.

Considerando, que el monitoreo y evaluación incide directamente en la planificación efectiva, así como estratégica, de la gestión institucional, de ahí que la inobservancia de este

[1] Al momento de la fiscalización y mediante la aplicación del cuestionario de Evaluación de Gestión TI, de fecha 5 de octubre de 2021, en el Departamento de TIC se comprobó que existen debilidades y vulnerabilidades de gestión, citadas a continuación:
a. Ausencia de un mecanismo para evaluar la situación actual tecnológica de la DGCP.
b. No se cuenta con los planes de contingencia, continuidad de negocio y recuperación de desastres acorde con la situación actual de la DGCP.
c. El departamento de TIC no cuenta con los recursos necesario para el desarrollo e implementación de proyecto (s) acorde con una metodología basadas en buenas prácticas.
d. El departamento de TIC no cuenta con un área para evaluar la calidad (QA) de los proyectos tecnológicos llevados a cabo en la DGCP.
e. El departamento de TIC no ha creado e implementado los mecanismos que le permitan desplegar una gestión de cambio en las contraseñas de las cuentas de servicios que afectan las áreas sensitivas y críticas de la DGCP.
f. El departamento de TIC no ha creado e implementados los mecanismos para garantizar una efectiva segregación de las funciones entre las áreas que conforman el departamento TIC.

componente de control interno impide concretizar la aspiración de prácticas coherentes a la buena administración en perjuicio del quehacer estatal.

Considerando, que el seguimiento y evaluación de planes, programas y proyectos permite responder a un modelo de gestión pública orientado a resultados, y el establecimiento de un sistema de indicadores de desempeño que permita la concretización de la vocación constitucional de la administración pública.

Considerando, que, por otro lado, dentro de las debilidades identificadas no se cuenta con mecanismos que permitan desplegar la gestión de cambio en las contraseñas de las cuentas de servicios que afectan las áreas sensitivas y críticas de la DGCP; esto supone poner en situación de riesgo y vulnerabilidad el sistema de información de la entidad en razón de que los mecanismos de cambios de contraseñas operan como herramientas de ciberseguridad que previenen afectación a la data y sistema operativo de cualquier organización, riesgo que con mayor justificación debe evitarse en los órganos estatales.

Considerando, que el departamento TIC de la DGCP no ha creado ni implementado los mecanismos para garantizar una efectiva segregación de las funciones entre las áreas que conforman el departamento, lo cual constituye un obstáculo en la gestión del área de que se trata, así como que contradice los lineamientos generales de diseño organizativo y funcional que deben observar las entidades y organismos estatales en materia de función pública.

Considerando, que con relación a las debilidades señaladas procede observar el incumplimiento de los procesos de gestión indicados en los subtítulos APO01.03 Mantener los elementos catalizadores del sistema de gestión, APO01.05 Optimizar la ubicación de la función TI, APO01.07 Gestionar la mejora continua de los procesos y APO01.08 Mantener el cumplimiento con las políticas y procedimientos, título APO01. Gestionar el Marco de Gestión de la TI, dominio APO Alinear, Planificar y Organizar, del marco de evaluación de Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT 2019), que expresan:

> **APO01. Gestionar el Marco de Gestión de la TI.** Aclarar y mantener el gobierno de la misión y la visión corporativa de TI. Implementar y mantener mecanismos y autoridades para la gestión de la información y el uso de TI en la empresa para apoyar los objetivos de gobierno en consonancia con las políticas y los principios rectores.
>
> **APO01.03 Mantener los elementos catalizadores del sistema de gestión.** Mantener los elementos catalizadores del sistema de gestión y del entorno de control de la TI de la empresa y garantizar que están integrados y alineados con la filosofía y el estilo operativo de gobierno y de gestión de la empresa. Estos elementos catalizadores incluyen una comunicación clara de expectativas/requisitos. El sistema de gestión debería fomentar la cooperación interdepartamental y el trabajo en equipo, promover el cumplimiento y la mejora continua y tratar las desviaciones en el proceso (incluidos los fallos).
>
> **1.** Adquirir comprensión de la visión, la dirección y la estrategia corporativas.
> **3.** Inferir e integrar los principios de TI con los principios de negocio.
> **4.** Alinear el entorno de control de TI con el entorno de políticas de TI, con los marcos de trabajo generales de gobierno de TI y procesos de TI y los marcos de trabajo existentes a nivel corporativo en cuanto a riesgo y control. Evaluar las buenas prácticas o los requisitos específicos del sector (p. ej., normativa específica del sector) e integrarlos donde corresponda).

6. Crear un conjunto de políticas para conducir las expectativas de control de TI en temas clave relevantes, como calidad, seguridad, confidencialidad, controles internos, uso de activos de TI, ética y derechos de propiedad intelectual.
7. Evaluar y actualizar las políticas, como mínimo una vez al año, para ajustarlas a los cambiantes entornos operativo o de negocio.
8. Implantar y aplicar las políticas de TI a todo el personal relevante, de forma que estén incorporadas y sean parte integral de las operaciones empresariales.
9. Asegurarse de que los procedimientos estén en funcionamiento para realizar un seguimiento del cumplimiento con las políticas y definir las consecuencias de la no conformidad.

APO01.05 Optimizar la ubicación de la función TI. Posicionar la capacidad de TI en la estructura organizativa global para reflejar en el modelo de empresa la importancia de TI en la organización, especialmente su criticidad para la estrategia empresarial y el nivel de dependencia de TI. La línea de reporte de CIO debe ser proporcional a la importancia de las TI en la empresa.

1. Entender el contexto de la función de TI, incluyendo una evaluación de la estrategia empresarial y el modelo operativo (centralizado, federado, descentralizado, hibrido), importancia de TI, la situación y opciones para la provisión.
2. Identificar, evaluar y priorizar las opciones para la ubicación en la organización, los modelos operativos y de aprovisionamiento.
3. Definir la ubicación de la función de TI y obtener aprobación.

APO01.07 Gestionar la mejora continua de los procesos. Evaluar, planificar y ejecutar la mejora continua de procesos y su madurez para asegurar que son capaces de entregarse conforme a los objetivos de la empresa, de gobierno, de gestión y de control. Considerar las directrices de la implementación de procesos de COBIT, estándares emergentes, requerimientos de cumplimiento, oportunidades de automatización y la realimentación de los usuarios de los procesos, el equipo del proceso y otras partes interesadas. Actualizar los procesos y considerar el impacto en los catalizadores del proceso.

1. Identificar los procesos críticos de negocio basándose en el rendimiento, cumplimiento y los riesgos relacionados. Evaluar la capacidad del proceso e identificar objetivos de mejora. Analizar las diferencias en la capacidad y control del proceso. Identificar las opciones de mejora y rediseño de procesos. Priorizar iniciativas para la mejora de procesos basadas en el potencial coste-beneficio.
2. Implementar las mejores acordadas, funcionando como una práctica normal del negocio y establecer objetivos y métricas de rendimiento que permitan el seguimiento de las mejoras del proceso.
3. Considerar las maneras de mejorar la eficiencia y eficacia (p. eje., mediante formación, documentación, estandarización y automatización de procesos).
4. Aplicar prácticas de gestión de calidad para la actualización de procesos.
5. Retirar procesos, componentes o catalizadores desactualizados.

APO01.08 Mantener el cumplimiento con las políticas y procedimientos. Poner en marcha procedimientos para mantener el cumplimiento y medición del funcionamiento de las políticas y otros catalizadores del marco de referencia; hacer cumplir las consecuencias del no cumplimiento o del desempeño inadecuado. Seguir las tendencias y el rendimiento y considerarlos en el diseño futuro y la mejora del marco control.

1. Hacer un seguimiento del cumplimiento con políticas y procedimientos.
2. Analizar los incumplimientos y adoptar las acciones apropiadas (puede incluir cambio de requerimientos).
3. Integrar rendimiento y cumplimiento dentro de los objetivos individuales del personal.
4. Evaluar periódicamente el desempeño de los catalizadores del marco de referencia y adoptar las acciones necesarias.

5. Analizar las tendencias en el funcionamiento y cumplimiento y adoptar las acciones apropiadas.

Considerando, que las debilidades y vulnerabilidades evidenciadas reflejan inobservancia de las normativas aplicables tanto de control interno como específicas de gestión de las áreas de tecnología de las entidades públicas, precedentemente expuestas. Esto constituye falta administrativa imputable a los servidores públicos incumbentes, de conformidad a las disposiciones de la ley 10-07 y 41-08 de función pública al no obtemperar al cumplimiento de lo establecido en las referidas normas y en los lineamientos de las NORTIC que resultan mandatorios. De igual forma, refiere a la necesidad de fortalecer los controles internos de la entidad.

2.2 Revisión y/o actualización de las políticas y procedimientos de TIC

Considerando, que, durante los procedimientos realizados en la DGCP al departamento de TIC, comprobamos una cantidad considerable de políticas y procedimientos generales de TIC que a la fecha se encuentran desactualizadas, realizándose la última revisión y/o creación en el año 2015[2].

Considerando, que dada la naturaleza dinámica de las tecnologías de la información, las políticas y procedimientos del área encargada se impone su actualización periódica y constante; esto no solo a los fines de garantizar la adecuación de la gestión institucional a las mejores prácticas, lo cual incide en la concretización de la buena administración; sino también observando otros aspectos, tal lo es el incremento de riesgo de afectación en materia de ciberseguridad a los sistemas de información, esto cobra mayor relevancia tratándose de un organismo del Estado con las atribuciones de la DGCP.

Considerando, que las políticas en su mayoría no cuentan con un procedimiento que indique como deben de ser ejecutadas; así como tampoco cuenta con un plan de revisión periódico que permita estar acordes a las necesidades actuales de la DGCP. Esto deja en evidente vulnerabilidad a la entidad siendo sus sistemas electrónicos y de información parte sustancial de la labor que realiza.

Disposiciones jurídicas

Considerando, que procede observar las disposiciones de los subtítulos PO6.1 Ambiente de Políticas y de Control, PO6.3 Administración de Políticas para TI, PO6.4 Implantación de

[2] DGCP.POL-DTI-GT01-Política General de Gestión de Tecnología V33 - JT-AOR (14/08/2015).
DGCP.POL-DTI-IF02-Política de Uso Aceptable Infraestructura para Usuarios V33 - JT-AOB (14/08/2015).
DGCP POL-DTI-CE03-Política de Uso Aceptable para Correo Electrónico V26 – JT (03/06/2015).
DGCP.POL-DTI-AI04-Política de Uso Aceptable para Internet V32 – JT (14/08/2015).
DGCP.POL-DTI-RI08-Política sobre las copias resguardo de la Información V22-AOR (03/07/2015).
DGCP.POL-DTI-MA07-Política de la Mesa de Servicios V32-AOR (14/08/2015).
DGCP.POL-DTI-UA06-Política de Uso de Antivirus V31 (14/08/2015).
DGCP-POL-DTI-091-Políticas de Contraseñas v21 (03/07/2015).
DGCP.POL-DTI-RT05-Política de Propiedad de los Recursos Tecnológicos V32-AOR (14/08/2015).
DGCP.POL-DTI-CS10-Política de Control de Acceso al Cuarto de Servidores V22-AOR (03/07/2015).
DGCP-POL-DTI-061-Política sobre dispositivos móviles y teletrabajo V31 (14/08/2015).
DGCP-POL-DTI-111-Política de Eliminación y Destrucción V21 (03/07/2015).
DGCP-POL-DTI-171-Política de la Continuidad del Negocio V21 (03/07/2015).
DGCP.POL-DTI-SA09-Política Desarrollo e Implementación de Sistemas y Aplicativo V31 (22/09/2015).
DGCP-POL-DTI-151-Política de Seguridad para Proveedores V21 (03/07/2015).

Políticas de TI y PO6.5 Comunicación de los Objetivos y la Dirección de TI, epígrafe objetivos de control, título PO Planear y Organizar, PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia, del marco de evaluación de Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT 4.1), que expresan:

> **PO6.1 Ambiente de Políticas y de Control**
>
> Definir los elementos de un ambiente de control para TI, alineados con la filosofía administrativa y el estilo operativo de la empresa. Estos elementos incluyen las expectativas/requerimientos respecto a la entrega de valor proveniente de las inversiones en TI, el apetito de riesgo, la integridad, los valores éticos, la competencia del personal, la rendición de cuentas y la responsabilidad. El ambiente de control se basa en una cultura que apoya la entrega de valor, mientras administra riesgos significativos, fomenta la colaboración entre divisiones y el trabajo en equipo, promueve el cumplimiento y la mejora continua de procesos, y maneja las desviaciones (incluyendo las fallas) de forma adecuada.
>
> **PO6.3 Administración de Políticas para TI**
>
> Elaborar y dar mantenimiento a un conjunto de políticas que apoyen la estrategia de TI. Estas políticas deben incluir su intención, roles y responsabilidades, procesos de excepción, enfoque de cumplimiento y referencias a procedimientos, estándares y directrices. Su relevancia se debe confirmar y aprobar en forma regular.
>
> **PO6.4 Implantación de Políticas de TI**
>
> Asegurarse de que las políticas de TI se implantan y se comunican a todo el personal relevante, y se refuerzan, de tal forma que estén incluidas y sean parte integral de las operaciones empresariales.
>
> **PO6.5 Comunicación de los Objetivos y la Dirección de TI**
>
> Asegurarse de que la conciencia y el entendimiento de los objetivos y la dirección del negocio y de TI se comunican a los interesados apropiados y a los usuarios de toda la organización.

Considerando, que la actualización de políticas y procedimientos resulta ser un elemento insoslayable de conformidad a las disposiciones contenidas en las NORTIC, su inobservancia entraña falta administrativa a quien no obtempere en su cumplimiento.

2.3 El departamento de TIC no cuenta con una herramienta o matriz de riesgo

En la realización de procedimientos aplicados en el mes de octubre de 2021 al Departamento TIC de la DGCP, se verificó que no cuentan con una herramienta o matriz que le permita identificar cuáles son los riesgos a los que están expuestos y el grado en que afectarían las operaciones del departamento TIC y la DGCP a nivel general. De igual manera no tienen identificadas cuales son las áreas más sensitivas e incidencias más comunes que se presenta en la entidad.

Disposiciones jurídicas

Considerando, que el informe de evaluación evidencia, que el departamento de TIC de la entidad no cuenta con una herramienta o matriz que le permita identificar los riesgos a los

que están expuestos y el grado en que afectarían las operaciones a dicho departamento; tampoco tienen identificadas las áreas más sensitivas y las incidencias más comunes que se presentan en la entidad.

Considerando, que procede observar las disposiciones del subliteral iv, literal j, sección 4.02. Plan de continuidad; los literales a, b, c, subliteral (i), de la subsección 4.02.3 Pruebas y simulacros, de la Norma para la Seguridad de las Tecnologías de la Información y Comunicación en el Estado Dominicano NORTIC A7, de fecha abril del año 2016, que expresan:

Sección 4.02. Plan de continuidad

La implementación de los procesos de la gestión de la continuidad es un aspecto de gran importancia dentro del departamento de TIC; esta implementación busca que tanto los servicios del organismo, como los procesos que sustentan las operaciones permanezcan en funcionamiento ante cualquier eventualidad, ya sea externa o interna.

(j) Debe tomarse en cuenta lo siguiente para la prueba, mantenimiento y re-evaluación del plan de continuidad del organismo:

(iv) Deben verificarse las siguientes informaciones del plan al momento de su revisión:

- Personal responsable de plan y personal alternativo.
- Direcciones y números de contacto.
- Alineación del plan con la estrategia organizacional.
- Locales y/o sucursales.
- Proveedores de servicios y clientes.
- Procesos, tanto nuevos como actualizados o eliminados.
- Evaluación de riesgo.

Sub-sección 4.02.3 Pruebas y simulacros

(a) El CONTI solo debe ser considerado como completado cuando se ha realizado una prueba funcional del mismo, se han validado los resultados y realizados los ajustes necesarios a fin de que cumpla con los objetivos identificados durante su fase de diseño.

(b) La forma de medir que el plan ha sido completado es mediante el informe del comité del CONTI informando a la máxima autoridad, la cual, luego de revisarla hará las observaciones de lugar y dará por completado el proceso de implantación inicial mediante firma de que los objetivos han sido logrados.

(c) Los organismos gubernamentales deben generar periódicamente informes sobre la ejecución y estado de su plan de continuidad.

(i) Los organismos gubernamentales deben tomar en cuenta lo siguiente para sus evaluaciones periódicas del plan de continuidad:

- Análisis sobre nuevos riesgos y los impactos de los mismos.
- Revisión del impacto económico asociado al plan de continuidad.
- Evaluación sobre los simulacros del plan de continuidad.
- Capacitación del personal del departamento de TIC para llevar a cabo el plan de continuidad.

Considerando, que procede observar las disposiciones de los numerales 1, 2, 3 y 4, subtítulo APO12.06 Responder al riesgo, título APO12 Gestionar el Riesgo, dominio APO Alinear, Planificar y Organizar; los numerales 1, 2, 3, 4, 5 y 6, subtítulo DSS04.04 Ejercitar, probar y revisar el BCP, título DSS04 Gestionar la Continuidad, dominio DSS Entrega, Servicio y Soporte, del marco de evaluación de Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT 2019), que expresan:

> **APO12 Gestionar el Riesgo**. Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de los niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.
>
> **APO12.06 Responder al riesgo.** Responder de una forma oportuna con medidas efectivas que limiten la magnitud de pérdida por eventos relacionados con TI.
>
> **1.** Preparar, mantener y probar planes que documenten los pasos específicos a tomar cuando un evento de riesgo pueda causar un incidente significativo operativo o evolucionar en un incidente con un impacto de negocio grave. Asegurar que los planes incluyan vías de escalado a través de la empresa.
>
> **2.** Categorizar los incidentes y comparar las exposiciones reales con los umbrales de tolerancia al riesgo. Comunicar los impactos en el negocio a los responsables de toma de decisiones como parte de la notificación y actualizar el perfil de riesgo.
>
> **3.** Aplicar el plan de respuesta apropiado para minimizar el impacto cuando ocurren incidentes de riesgo.
>
> **4.** Examinar eventos, adversos/pérdidas del pasado y oportunidades perdidas y determinar sus causas raíz. Comunicar la causa raíz, requerimientos de respuesta adicionales para el riesgo y mejoras de proceso a los responsables de toma de decisiones apropiados y asegurarse de que la causa, los requerimientos de respuesta y la mejora del proceso se incluyan en los procesos de gobierno del riesgo.
>
> **DSS04 Gestionar la Continuidad.** Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa.
>
> **DSS04.04 Ejercitar, probar y revisar el BCP.** Probar los acuerdos de continuidad regularmente para ejercitar los planes de recuperación respecto a unos resultados predeterminados, para permitir el desarrollo de soluciones innovadoras y para ayudar a verificar que el plan funcionará, en el tiempo, como se espera.
>
> **1.** Definir los objetivos para ejercitar y probar los sistemas del plan (de negocio, técnicos, logísticos, administrativos, procedimentales y operacionales) para verificar la completitud del plan de continuidad de negocio (BCP) para enfrentarse a los riesgos de negocio.
> **2.** Definir y acordar ejercicios que sean razonables con las partes interesadas, validar los procedimientos de continuidad, e incluir roles y responsabilidades y acuerdos de retención de datos que ocasionen la mínima disrupción en los procesos de negocio.
> **3.** Asignar roles y responsabilidades para realizar ejercicios y pruebas del plan de continuidad.
> **4.** Planificar ejercicios y actividades de prueba tal como esté definido en el plan de continuidad.
> **5.** Realizar un análisis y revisión postejercicio para considerar el logro.
> **6.** Desarrollar recomendaciones para mejorar el plan de continuidad actual en base a los resultados de revisión.

Considerando, que procede observar las disposiciones de los numerales 17.1 Continuidad de la seguridad de la información y 17.1.1 Planificación de la continuidad de la seguridad de la información, anexo 17 Seguridad de la Información en la Gestión de la Continuidad del Negocio, del Estándar para la Seguridad de la Información de la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional ISO/IEC 27002 que expresan:

> **ANEXO 17. Seguridad de la Información en la Gestión de la Continuidad del Negocio.** Se deberían analizar las consecuencias de los desastres, fallas de seguridad, pérdidas de servicio y la disponibilidad del servicio y desarrollar e implantar planes de contingencia para asegurar que los procesos del negocio se pueden restaurar en los plazos requeridos las operaciones esenciales, manteniendo las consideraciones en seguridad de la información utilizada en los planes de continuidad y función de los resultados del análisis de riesgos.
>
> **17.1 Continuidad de la seguridad de la información:** El objetivo es que la seguridad de la información sea integrada en los sistemas de gestión de la continuidad del negocio de la organización.
>
> **17.1.1 Planificación de la continuidad de la seguridad de la información:** La organización debería determinar los requisitos para la seguridad de la información y su gestión durante situaciones adversas como situaciones de crisis o de desastre.

2.4 Vulnerabilidades del centro de datos (Data Center)

Considerando, que el informe de evaluación evidencia debilidades en los subsistemas mecánico, arquitectura y eléctrico, así como en la gestión de control.[3]

---

[3] 1) Durante el procedimiento de inspección física realizado al centro de datos (Data Center) de la Dirección General de Contrataciones Públicas se encontraron las siguientes debilidades en los subsistemas mecánico, arquitectura y eléctrico:
a. Sistemas de refrigeración, en la actualidad la DGCP cuenta con dos aires tipo central de cinco (5) toneladas que trabajan configurado uno como respaldo del otro.
b. Sistema de respaldo UPS, se comprobó que la unidad de UPS EATON POWERWARE 9355 funciona como respaldo general en las instalaciones de la DGCP.
c. El sistema de supresión de incendio automático no cuenta con los detectores de humos que en caso de un incendio fuera del perímetro en el mismo centro de datos active la alarma de la existencia de un siniestro o humo.
d. Extintor manual dentro del centro de datos (Data Center) y señalización suelta.
e. No se cuenta con un estudio o plano que determine que la ubicación actual del centro de datos (Data Center) sea la más idónea y favorable a la DGCP estando este en un perímetro de acceso general para los colaboradores y personal de visita con un acceso más allá de la recepción.
f. Las puertas de acceso al centro de datos (Data Center) no cumplen con las buenas prácticas por las siguientes condiciones detalladas:
i. Puertas de vidrios solo con el marco en aluminio.
ii. Puertas sin sensores de rupturas de Vidrios.
iii. Puertas con llavines y cerraduras mecánicas.
iv. Ausencia de sensores que notifique la apertura de las puertas.
v. Puertas en la cara frontal y lateral del centro de datos (Data Center).
g. No se cuenta con un falso piso.
h. El falso techo de material inflamable.
i. El cableado de data y el cableado eléctrico pasando por el mismo conducto para llegar a los RACKs.
j. Una sola cámara de circuito cerrado (CCTV) la cual no cubre todos los ángulos del centro de datos (Data Center) permitiendo puntos ciegos.
k. Sistema eléctrico de la DGCP no aísla el sistema eléctrico del centro de datos (Data Center) para proteger los equipos de este frente a caída, picos o incidentes eléctricos.
2) Durante los procedimientos de inspección realizados al centro de datos (Data Center) se encontraron las siguientes debilidades gestión de control:
a. No se cuenta con una bitácora de visitas.
b. No existen políticas y procedimientos actualizados relativos a los controles y mecanismo del sistema eléctrico y respaldo.
c. No se cuenta con políticas y procedimientos para asegurar el adecuado diseño del centro de datos (Data Center).
d. No se cuenta con políticas y procedimientos actualizados para los accesos temporales de personal al centro de datos (Data Center).

Disposiciones jurídicas

Considerando, que el informe de evaluación evidencia debilidades en los subsistemas mecánico, arquitectura y eléctrico, así como en la gestión de control, los cuales han sido citados precedentemente; en ese sentido, procede observar las disposiciones de los literales DS12.1 Selección y Diseño del Centro de Datos, DS12.2 Medidas de Seguridad Física, DS12.3 Acceso Físico, DS12.4 Protección Contra Factores Ambientales, DS12.5 Administración de Instalaciones Físicas, subtítulo Objetivos de Control, Título DS12 Entregar y Dar Soporte, Administración del Ambiente Físico, del marco de evaluación de Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT 4.1), que expresan:

> **DS12.1 Selección y Diseño del Centro de Datos**
> Definir y seleccionar los centros de datos físicos para el equipo de TI para soportar la estrategia de tecnología ligada a la estrategia del negocio. Esta selección y diseño del esquema de un centro de datos debe tomar en cuenta el riesgo asociado con desastres naturales y causados por el hombre. También debe considerar las leyes y regulaciones correspondientes, tales como regulaciones de seguridad y de salud en el trabajo.
>
> **DS12.2 Medidas de Seguridad Física**
> Definir e implementar medidas de seguridad físicas alineadas con los requerimientos del negocio. Las medidas deben incluir, pero no limitarse al esquema del perímetro de seguridad, de las zonas de seguridad, la ubicación del equipo crítico y de las áreas de envío y recepción. En particular, mantenga un perfil bajo respecto a la presencia de operaciones críticas de TI. Deben establecerse las responsabilidades sobre el monitoreo y los procedimientos de reporte y de resolución de incidentes de seguridad física.
>
> **DS12.3 Acceso Físico**
> Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a locales y áreas de acuerdo con las necesidades del negocio, incluyendo las emergencias. El acceso a locales, edificios y áreas debe justificarse, autorizarse, registrarse y monitorearse. Esto aplica para todas las personas que accedan a las instalaciones, incluyendo personal, clientes, proveedores, visitantes o cualquier tercera persona.
>
> **DS12.4 Protección Contra Factores Ambientales**
> Diseñar e implementar medidas de protección contra factores ambientales. Deben instalarse dispositivos y equipo especializado para monitorear y controlar el ambiente.
>
> **DS12.5 Administración de Instalaciones Físicas**
> Administrar las instalaciones, incluyendo el equipo de comunicaciones y de suministro de energía, de acuerdo con las leyes y los reglamentos, los requerimientos técnicos y del negocio, las especificaciones del proveedor y los lineamientos de seguridad y salud.

Considerando, que procede observar las disposiciones del literal a, subliterales i, literal a, ii, literal a, iii, iv, v y vi, de la sección 3.01 Control de Acceso de Usuario, de la Norma para la Seguridad de las Tecnologías de la Información y Comunicación en el Estado Dominicano NORTIC A7, de fecha abril del año 2016, que expresan:

> **(a)** Los organismos gubernamentales deben tener procedimientos establecidos para la gestión de accesos de sus empleados, estos procedimientos deben contemplar:
> **(i)** Accesos de entrada y salida al organismo gubernamental.
> **a)** El sistema de acceso al organismo gubernamental debe cumplirlas directrices establecidas en la sección 3.02 Controles de acceso a la infraestructura.

(ii) Controles de accesos a la información del organismo gubernamental.
a) Estos controles deben contemplar las directrices establecidas en la sección 2.02 Políticas para la administración de la información.
(iii) Controles de accesos a estaciones de trabajo.
(iv) Controles de accesos a áreas restringidas.
(v) Controles de accesos a áreas de servidores.
(vi) Controles de accesos a software del organismo gubernamental.

Considerando, que procede observar las disposiciones del literal a, subliterales i, ii, iii, iv y v, y literal b, subliterales i, ii y iii, literal a, iv, v, vi, vii, viii, ix, subliteral a, x y xi, de la sección, 5.02. Gestión del centro de datos y Servidores, de la Norma para la Implementación y Gestión de la Conectividad en el Estado Dominicano, NORTIC B1, de fecha 29 de julio del año 2016, que expresan:

SECCIÓN 5.02. Gestión del centro de datos y Servidores

(a) Para la correcta administración de los centros de datos, deben seguirse las directrices a continuación:

(i) El personal de la unidad de TIC debe tener contratos de confidencialidad sobre los datos o información que estos manipulen.

(ii) En caso de que el organismo opte por la contratación de terceros para el almacenamiento de la información, el proveedor debe entregar un SLA, el cual debe especificar su compromiso con salvaguardar la información.

(iii) La unidad de TIC debe asegurar la redundancia de su infraestructura para eventualidades o catástrofes. Ver NORTIC A7:2016, Capítulo IV. Plan de disponibilidad y continuidad.

(iv) Deben existir políticas de privilegios dentro del departamento de TIC, específicamente el área de operaciones TIC, para que solo el personal autorizado pueda acceder a la infraestructura del organismo. Ver NORTIC A7:2016, sección 3.02 controles de acceso a la infraestructura.

(b) Para la correcta administración de los servidores dentro del centro de datos, deben seguirse las directrices a continuación:

(i) Debe darse soporte y mantenimiento al sistema operativo y el software utilitario instalado.

(ii) Deben crearse políticas de respaldo y restauración.

(iii) Deben gestionarse todas licencias para los sistemas instalados en los servidores, especialmente sistemas operativos, utilidades y cualquier software de aplicación.

a) Para los temas sobre el licenciamiento el organismo debe cumplir con las directrices especificadas en la NORTIC A1, subsección 1.05.2 Licenciamiento.

(iv) Deben aplicarse medidas de seguridad, incluyendo la identificación y aplicación de parches de seguridad, gestión de acceso y la detección de intrusiones.

(v) Debe realizarse un mantenimiento continuo, el cual incluya la sustitución de servidores antes de estos ser obsoletos para apoyar la evolución de los servicios.

(vi) Los servidores deben tener el cifrado de unidad activado desde el Sistema Básico de Entrada/Salida (BIOS, por sus siglas en inglés) para la encriptación de sus datos.

(vii) Los servidores de dominio deben tener habilitado el protocolo LDAPS.

(viii) Todas las estaciones de trabajo deben estar protegidas por políticas para ser accedidas solo por el personal autorizado.

(ix) Los servidores de la infraestructura, deben tener las últimas actualizaciones y parches de seguridad.

a) Antes de la implementación en ambientes de producción, esto debe pasar por un ambiente de pruebas.

(x) Todos los servidores deben tener una solución de antivirus actualizada que aseguren la protección de la red, así como las estaciones de trabajo.

(xi) Los controles de acceso biométricos o de tarjetas de código que estén conectados a la infraestructura de la red, deben estar conectados mediante una VLAN separada del tráfico de usuarios.

Considerando, que procede observar las disposiciones del numeral 3.1 General, literales a, b, c, d, e y f, título 3 Resumen de diseño de centro de datos, de la norma ANSI/TIA-942 de la Asociación de la Industria de Telecomunicaciones, Estándar de Infraestructura de Telecomunicaciones para Centros de Datos, en inglés: (The Telecommunications Industry Association (TIA) Telecommunications Infrastructure Standard for Data Centers is an American National Standard (ANS), aprobado el 12 de abril de 2005, que expresan:

3 Resumen de diseño de centro de datos

3.1 General

La intención de este apartado es proporcionar información general sobre los factores que deben tenerse en cuenta al planificar el diseño de un centro de datos. La información y las recomendaciones están destinadas a permitir una aplicación efectiva de un diseño del centro de datos mediante la identificación de las acciones apropiadas que se deben tomar en cada paso del proceso de planificación y diseño. Los detalles de diseño específicos se proporcionan en las cláusulas y anexos posteriores.

Los pasos en el proceso de diseño que se describen a continuación se aplican al diseño de un nuevo centro de datos o ampliación de un centro de datos existente. Es esencial para cualquiera de los casos que el diseño de los sistemas de telecomunicaciones, plan de equipamiento de piso, planos eléctricos, proyecto arquitectónico de cableado, sistemas de climatización, se coordinara de seguridad y sistemas de iluminación. Idealmente, el proceso debe ser:

a) Estimación de equipos de telecomunicaciones, espacio, energía y demanda de refrigeración del centro de datos a plena capacidad. Anticipar futuras telecomunicaciones, el poder y las tendencias de enfriamiento durante la vida útil del centro de datos.

b) Proporcionar espacio, energía, refrigeración, seguridad, carga sobre el suelo, tierra, protección eléctrica y otros requisitos de las instalaciones a los arquitectos e ingenieros. Proporcionar los requisitos para el centro de operaciones, muelle de carga, sala de almacenamiento, áreas de almacenamiento y otras áreas de apoyo.

c) Coordinar los planes de centro de datos espaciales preliminares de arquitectos e ingenieros. Sugerir cambios necesarios según sea necesario.

d) Crear un plan de equipamiento para el salón incluyendo la colocación de las principales salas y espacios para salas de ingreso, principales áreas de distribución, áreas de distribución horizontal, zonas de distribución de zonas y áreas de distribución de equipos. Proporcionar energía esperada, la refrigeración, y el piso cargando requisitos para el equipo de ingenieros. Proporcionar los requisitos para las vías de telecomunicaciones.

e) Obtener un plan actualizado de los ingenieros de telecomunicaciones con las vías, equipos eléctricos, equipos mecánicos y añadido a la planta del centro de datos a plena capacidad.

f) Sistema de cableado de telecomunicaciones Diseño basado en las necesidades del equipo que se encuentran en el centro de datos.

2.5 Ausencia de controles en el Servidor de dominio

Considerando, que el informe de evaluación evidencia que durante los procedimientos de extracción de Logs y revisión del servidor de active directory, practicado en el mes de julio de 2021, se detectaron que existen vulnerabilidades y falta de control con relación a los sistemas operativos.[4]

Disposiciones jurídicas

Considerando, que, en ese sentido, procede observar las disposiciones del literal h, subliterales i, ii, iii, iv, v, vi vii y viii, de la sección 3.03. Control de Acceso al Sistema Operativo, de la Norma para la Seguridad de las Tecnologías de la Información y Comunicación en el Estado Dominicano NORTIC A7, de fecha abril del año 2016, que expresan:

SECCIÓN 3.03.

Control de acceso al sistema operativo

(h) Todas las estaciones de trabajo de los organismos gubernamentales deben estar protegidas por contraseña que cumplan las siguientes características:
(i) Las contraseñas deben tener un mínimo de ocho (8) caracteres.
(ii) Las contraseñas deben tener al menos una letra mayúscula.
(iii) Las contraseñas deben tener letras minúsculas.

---

[4] 1-Logs o pistas de auditorías deshabilitadas como se detallan a continuación:
i. Reinicio y apagado: Sin auditoría (Restart and Shutdown: No auditing).
ii. Inicio y cierre de sesión: Sin auditoría (Logon and Logoff: No auditing).
iii. Archivo / Acceso a objetos: Sin auditoría (File/Object Access: No auditing).
iv. Uso del derecho de usuario: Sin auditoría (Use of User Right: No auditing).
v. Proceso de seguimiento: Sin auditoría (Process Tracking: No auditing).
vi. Cambios en la política de seguridad: Sin auditoría (Security Policy Changes: No auditing).
vii. Gestión de Usuarios / Grupos: Sin auditoría (User / Group Management: No auditing).
viii. Acceso al servicio de directorio: Sin auditoría (Directory Service Access: No auditing).
ix. Inicio de sesión de cuenta privilegiada: Sin auditoría (Privileged Account Logon: No auditing).
x. Cuentas de usuarios activas en el active directory con acceso mediante VPN que las contraseñas no expiran o caducan.
xi. Cuentas de servicios activas, en el active directory, con dos años o más tiempo sin cambio de contraseñas.
xii. Cuentas de usuarios del active directory con privilegios y pertenecen al grupo de Administradores en la que no expira o caduca la contraseña.
xiii. Cuentas de usuarios en el active directory con privilegios de administración de esquemas (Schema Admin).
xiv. Cuentas de usuarios de active directory con privilegios de administradores de empresas (Enterprise Admin).
xv. Cuentas de usuarios para pruebas activas en el active directory sin uso.

(iv) Las contraseñas deben tener al menos un número.
(v) Las contraseñas deben ser renovadas cada cuarenta y cinco (45) días.
(vi) Las contraseñas personales no deben ser compartidas para no comprometer información sensible que resida en las estaciones de trabajo.
(vii) Las contraseñas definidas por el empleado no deben ser comunes.
(viii) Las contraseñas no se pueden reutilizar en diferentes sistemas a menos que se esté utilizando un sistema de autenticación centralizado o de Autentificación Sencilla.

Considerando, que procede observar las disposiciones del literal DS5.4 Administración de Cuentas del Usuario, subtítulo Objetivos de Control, título DS5 Entregar y Dar Soporte, Garantizar la seguridad de los Sistemas y DS10.2 Rastreo y Resolución de Problemas, subtítulo Objetivos de Control, y DS10 Entregar y Dar Soporte, Administración de Problemas, del marco de evaluación de Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT 4.1), que expresan:

DS5.4 Administración de Cuentas del Usuario

Garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, sean tomados en cuenta por un conjunto de procedimientos de la gerencia de cuentas de usuario. Debe incluirse un procedimiento de aprobación que describa al responsable de los datos o del sistema otorgando los privilegios de acceso. Estos procedimientos deben aplicarse a todos los usuarios, incluyendo administradores (usuarios privilegiados), usuarios externos e internos, para casos normales y de emergencia. Los derechos y obligaciones relativos al acceso a los sistemas e información de la empresa deben acordarse contractualmente para todos los tipos de usuarios. Realizar revisiones regulares de la gestión de todas las cuentas y los privilegios asociados.

DS10.2 Rastreo y Resolución de Problemas

El sistema de administración de problemas debe mantener pistas de auditoría adecuadas que permitan rastrear, analizar y determinar la causa raíz de todos los problemas reportados considerando:

- Todos los elementos de configuración asociados
- Problemas e incidentes sobresalientes
- Errores conocidos y sospechados
- Seguimiento de las tendencias de los problemas.

Identificar e iniciar soluciones sostenibles indicando la causa raíz, incrementando las solicitudes de cambio por medio del proceso de administración de cambios establecido. En todo el proceso de resolución, la administración de problemas debe obtener reportes regulares de la administración de cambios sobre el progreso en la resolución de problemas o errores. La administración de problemas debe monitorear el continuo impacto de los problemas y errores conocidos en los servicios a los usuarios. En caso de que el impacto se vuelva severo, la administración de problemas debe escalar el problema, tal vez refiriéndolo a un comité determinado para incrementar la prioridad de la solicitud del cambio (RFC) o para implementar un cambio urgente, lo que resulte más pertinente. El avance de la resolución de un problema debe ser monitoreado contra los SLAs.

Considerando, que procede observar las disposiciones de los subliterales 9.2.2 Gestión de los derechos de acceso asignados a usuarios, 9.2.3 Gestión de los derechos de acceso con privilegios especiales, 9.2.5 Revisión de los derechos de acceso de los usuarios, 9.2.6 Retirada o adaptación de los derechos de acceso, literal 9.2 Gestión de acceso de usuario; y el subliteral 9.4.2 Procedimientos seguros de inicio de sesión, literal 9.4 Control de acceso a

sistemas y aplicaciones, ANEXO 9. Control de Accesos, del Estándar para la Seguridad de la Información de la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional ISO/IEC 27002, que expresan:

> **ANEXO 9. Control de Accesos.** El objetivo del presente dominio es controlar el acceso por medio de un sistema de restricciones y excepciones a la información como base de todo sistema de seguridad informática (redes y sistemas/plataformas de información).
>
> **9.2 Gestión de acceso de usuario**
> El objetivo es el de garantizar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información y servicios.
>
> **9.2.2 Gestión de los derechos de acceso asignados a usuarios:** Se debería de implantar un proceso formal de aprovisionamiento de accesos a los usuarios para asignar o revocar derechos de acceso a todos los tipos de usuarios y para todos los sistemas y servicios.
>
> **9.2.3 Gestión de los derechos de acceso con privilegios especiales:** La asignación y uso de derechos de acceso con privilegios especiales debería ser restringido y controlado.
>
> **9.2.5 Revisión de los derechos de acceso de los usuarios:** Los propietarios de los activos deberían revisar con regularidad los derechos de acceso de los usuarios.
>
> **9.2.6 Retirada o adaptación de los derechos de acceso:** Se deberían retirar los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información a la finalización del empleo, contrato o acuerdo, o ser revisados en caso de cambio.
>
> **9.4 Control de acceso a sistemas y aplicaciones**
> El objetivo es impedir el acceso no autorizado a la información mantenida por los sistemas y aplicaciones.
>
> **9.4.2 Procedimientos seguros de inicio de sesión:** Cuando sea requerido por la política de control de accesos se debería controlar el acceso a los sistemas y aplicaciones mediante un procedimiento seguro de log-on.

2.6 Estructura organizativa del departamento de TIC no alineada a Órganos rectores.

Considerando, que el informe de evaluación evidencia que el departamento de TIC no cuenta con una infraestructura organizacional alineada, conforme a las recomendaciones del MAP a través de la resolución 51-2013 y de la OPTIC a través de la NORTIC A1 del año 2014.

Disposiciones jurídicas

Considerando, que procede observar las disposiciones de los literales f y h, numeral 1, artículo 47, del Decreto n.° 491-07, que establece el Reglamento de Aplicación de la Ley n.° 10-07, que instituye el Sistema Nacional de Control Interno y de la Contraloría General de la República, de fecha 30 de agosto del año 2007, que expresan:

> **Artículo 47.-Componentes del Proceso de Control Interno.** Con fines de la implantación del proceso de control interno institucional en las entidades y los organismos del ámbito de la Ley 10-07, los cinco componentes previstos en el artículo 24, de la Ley, se definen como sigue:

1. Ambiente de Control: La administración activa, principalmente el titular de cada entidad y organismo público del ámbito de la Ley, debe fomentar un ambiente propicio para la operación del control interno, mediante la generación de una cultura de administración y control que promueva, entre el personal de la institución, el reconocimiento del control como parte integrante de los sistemas institucionales. En su calidad de responsable por el proceso de control interno debe mostrar constantemente una actitud de apoyo a las medidas de control implantadas en la institución, mediante la divulgación de éstas y un ejemplo continuo de apego a ellas en el desarrollo de las labores cotidianas. Los elementos principales en que descansa el componente son:

f) Estructura organizacional
h) Asignación de responsabilidad.

Considerando, que procede observar las disposiciones del artículo 5, del Decreto n.º 527-09, que establece el Reglamento de las Estructuras Organizativas, Cargos y Política Salarial del sector público dominicano, de fecha 21 de julio del año 2009, que expresan:

Artículo 5. Contenido. La estructura organizativa es un instrumento fundamental para desarrollar una estrategia efectiva de gestión, por tanto, para su presentación y aprobación debe contener y reflejar todos los cargos clasificados, valorados y presupuestados requeridos para el cumplimiento de los objetivos y proyección estratégica de cada institución, así como su realidad.

Considerando, que procede observar las disposiciones del literal a, literal b, subliterales i, ii, iii, iv, v y vi de la subsección 2.01.1. Estructura Organizacional, sección 2.01. Estructura del departamento de TIC; literales a, subliterales i, ii, iii, iv, v, vi, vii, viii, ix, x, xi, xii, xiii, xiv y xv y b, subliterales i, ii, sección 2.02. Políticas generales del departamento de TIC; literales a, b y c, subliterales i, ii, iii, iv, v, vi y vii, sección 2.03. Servicios de TIC; literal a, subliterales i, ii subliterales a, b, c, sección 2.04. Inventario general de TIC; y la sección 2.05. Recomendaciones para las políticas del departamento de TIC, de la Norma General sobre el Uso e Implementación de las Tecnologías de la Información y Comunicación en el Estado Dominicano, NORTIC A1, de fecha 15 de mayo del año 2014, que expresan:

CAPÍTULO II
GESTIÓN DEL DEPARTAMENTO DE TIC

En este capítulo se establecen las directrices para la gestión del departamento de TIC, especificando cómo este debe estar estructurado organizacionalmente, las políticas departamentales para una gestión efectiva, cómo deben gestionar los servicios de TIC y cómo llevar el control de los activos que están bajo la responsabilidad del departamento.

SECCIÓN 2.01. Estructura del departamento de TIC

Se ha dispuesto una estructura organizacional que consta de 5 áreas básicas, las cuales deben cumplir con los roles establecidos para cada una de estas áreas, así como 3 modelos de estructura organizacional y dos formas para la selección de uno de estos modelos basado en una serie de criterios y tablas de ponderaciones.

Sub-sección 2.01.1. Estructura organizacional

(a) Todo organismo gubernamental debe organizar la estructura departamental de TIC, de acuerdo con todas las directrices especificadas en la resolución 51-2013 elaborada entre la OPTIC y el MAP.

(b) La gestión del departamento de TIC debe agruparse en 6 grandes áreas básicas y cumplir con los roles asignados a cada una:

(i) Unidad TIC: Tiene bajo su cargo las responsabilidades indicadas en la sección 2.02. Políticas generales del departamento TIC.

(ii) Desarrollo e implementación de sistemas: Debe responsabilizarse de todas las actividades relacionadas con el diseño, desarrollo, implementación y soporte de los programas y sistemas que apoyan los procesos esenciales de los organismos.

(iii) Operaciones de TIC: Debe responsabilizarse de todas las actividades relacionadas con la operación y administración de la infraestructura tecnológica (servidores, bases de datos, redes, entre otros), así como el aseguramiento de la continuidad de las operaciones.

(iv) Administración del servicio de TIC: Debe responsabilizarse de todas las actividades de soporte técnico a la infraestructura tecnológica, incluyendo el soporte funcional y mesa de ayuda a los usuarios de los servicios de TIC.

(v) Seguridad y monitoreo: Debe responsabilizarse de todas las actividades relacionadas con la definición e implementación de políticas de seguridad de la información, control y monitoreo de los accesos a los sistemas de información.

(vi) Administración de proyectos de TIC: Debe responsabilizarse de todas las actividades relacionadas con la administración y coordinación de la implementación de proyectos de TIC.

SECCIÓN 2.02. Políticas generales del departamento de TIC

Una buena gestión del departamento de TIC incrementa la efectividad y productividad del departamento, y permite lograr los objetivos establecidos previamente, haciendo un mejor uso de la tecnología y la estructura organizacional. Para lograrlo, todo organismo gubernamental debe cumplir con las siguientes directrices:
(a) La máxima autoridad del departamento de TIC debe cumplir con las siguientes responsabilidades, apoyándose en todos los miembros pertenecientes al departamento:

(i) Evaluar y monitorear el cumplimiento de normas, políticas y leyes por parte de todos los miembros del departamento.

(ii) Dirigir la preparación y la implementación de planes y políticas.

(iii) Gestionar y administrar eficientemente las fuentes y activos de información del organismo, disponiendo de controles la calidad y seguridad de los sistemas.

(iv) Gestionar y administrar las licencias de software y realizar su distribución entre las unidades administrativas que las requieran.

(v) Administrar y coordinar todas las actividades relacionadas con la implementación de proyectos de TIC de impacto interno o externo del organismo.

(vi) Administrar y gestionar los servicios del centro de datos, garantizando la tecnología que soporte las actividades de TIC del organismo, así como el aseguramiento de la redundancia y balanceo de los servicios, monitorear el óptimo estado de los sistemas y plataformas alojadas.

(vii) Desarrollar y administrar aplicaciones de TIC que contribuyan al logro de las metas del organismo, asegurando la calidad de la plataforma y el cumplimiento de los estándares especificados en las NORTIC.

(viii) Disponer de los servicios informáticos y de telecomunicaciones que soliciten las diferentes unidades administrativas del organismo.

(ix) Fomentar la integración a diferentes redes de informaciones nacionales e internacionales mediante Internet, para permitir el acceso a distintas bases de datos en línea.

(x) Implantar y mantener actualizado un sistema de información integral que automatice las operaciones y procesos del organismo fomentando la comunicación interna, mediante el uso intensivo de las TIC.

(xi) Implementar y mantener la infraestructura de TIC que permita al organismo alcanzar sus metas estratégicas y promover el Gobierno Electrónico, mediante el intercambio, acceso y uso de la información por los usuarios internos y externos.

(xii) Participar en la elaboración, ejecución y seguimiento, de acuerdos y protocolos de intercambios de información por medios electrónicos que realice el organismo con otras instituciones públicas y privadas.

(xiii) Proveer soporte técnico a los usuarios de las aplicaciones, así como a la información y la infraestructura del organismo.

(xiv) Realizar la planificación estratégica y presupuestaria de las soluciones de TIC del organismo.

(xv) Revisar periódicamente el funcionamiento de la red, el desempeño de los sistemas en operación y el de las bases de datos del organismo para identificar desviaciones respecto a los objetivos y formular recomendaciones que optimicen los recursos y procesos operativos, propiciando el incremento de la productividad y la eficiencia.

(b) De acuerdo con la naturaleza de cada organismo gubernamental, debe crearse políticas de documentación para cada procedimiento, resolución de incidentes, software desarrollado internamente, y cualquier otra información relevante que manipule el departamento.

(i) La documentación debe realizarse de manera minuciosa, explicando todos los detalles de la información a documentar.

(ii) En caso de prescindir de un recurso, debe utilizarse la documentación realizada previamente, de manera que se pueda continuar brindando los servicios que se ofrecen.

SECCIÓN 2.03. Servicios de TIC

En esta sección se establece el procedimiento a seguir en la prestación de servicios y la gestión de incidentes. Así como las especificaciones para la estructuración del catálogo de servicio y la elaboración de los Acuerdos de Nivel de Servicio (SLA, por sus siglas en inglés).

(a) La disponibilidad de los servicios debe contemplarse en el plan de disponibilidad y continuidad de cada organismo. Ver sección 6.05. Plan de disponibilidad y continuidad.

(b) Cualquier tarea que implique una degradación o interrupción del servicio debe realizarse en las horas de inactividad o de menor demanda de este, siempre que sea posible.

(c) Si el servicio debe estar disponible las 24 horas del día y la interrupción es necesaria:

(i) Debe consultarse con el cliente acerca de las horas en la que la interrupción del servicio afectará menos a sus actividades.

(ii) Debe informarse con antelación suficiente a todos los involucrados.

(iii) Debe incorporarse dicha información a los SLA.

(iv) Debe monitorizarse la disponibilidad del servicio y elaborarse informes con los resultados.

(v) Debe especificarse el tiempo de detección.

(vi) Debe especificarse el tiempo de respuesta.

(vii) Debe especificarse el tiempo de reparación/recuperación.

SECCIÓN 2.04. Inventario general de TIC

Se establece el procedimiento para el levantamiento, actualización y control de inventario que todos los organismos deben seguir para la gestión de los activos físicos y de información que se encuentren bajo la responsabilidad del departamento de TIC.

(a) Todo organismo debe realizar un inventario ordenado, completo y actualizado de todos los activos que estén bajo la responsabilidad del departamento de TIC.

(i) El inventario general de TIC debe estar organizado en dos secciones principales:

• **Activos físicos:** Donde se registrarán todos los equipos de la infraestructura TI, estaciones de trabajo, portátiles y demás.

• **Activos de información:** Donde se registrará todo el software utilizado, sistemas operativos y demás.

(ii) La unidad de operaciones de TIC debe tener un personal que asuma la función de llevar a cabo todo el proceso de inventario. Este tendrá a la responsabilidad de coordinar las tareas que deben desarrollarse:

a) Levantamiento de inventario: Registrar todos los bienes que forman el equipamiento tecnológico bajo el control del departamento de TIC. Esta fase se realizará en caso de que el organismo no haya realizado un inventario anteriormente.

b) Actualizaciones de inventario: Agregar al inventario nuevos bienes adquiridos por el departamento de TIC, igualmente eliminar los bienes que han salido de la responsabilidad del organismo.

c) Control de inventario: Revisar físicamente los bienes que se encuentran en el inventario.

SECCIÓN 2.05. Recomendaciones para las políticas del departamento de TIC

• Establecer responsabilidades claramente entendidas y aceptadas por todos los miembros del departamento de TIC.

• Para cumplir con los objetivos departamentales, antes de elaborar las estrategias de trabajo, es necesario tomar en cuenta las capacidades y recursos técnicos que posee el departamento de TIC.

• Que la estructura del departamento de TIC esté distribuida, tanto en recursos tecnológicos como en recursos humanos, de manera que pueda darse soporte al organismo y brindar los servicios con la calidad exigida.

Considerando, que procede observar las disposiciones de los párrafos I, II, III y IV, artículo 7, de la resolución n.° 51-2013, que aprueba los Modelos de Estructura Organizativa de la Unidades de Tecnologías de la Información y Comunicación (TIC), de fecha 3 de diciembre del año 2013, emitida por la Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC) conjuntamente con el Ministerio de Administración Pública (MAP), que expresan:

> **Artículo 7.-** Se establecen tres (3) Modelos para la organización de las Unidades Institucionales de Tecnologías de la Información y Comunicación: A, B, y C, los cuales serán adoptados por las instituciones de acuerdo a los siete criterios básicos que se establecen más adelante.
>
> **Párrafo I:** Modelo A: Este modelo de estructura es el más complejo y está definido para Instituciones Gubernamentales con alta complejidad en términos de usuarios a los que se les brinda servicio, desarrollo de sistemas e infraestructura tecnológica.
>
> **Párrafo II:** Modelo B: Este modelo de estructura es de complejidad media y está definido para Instituciones Gubernamentales que no cumplan con las definiciones de alta complejidad establecidas en los criterios descritos en este documento, sin embargo, su infraestructura requiere de la ejecución de la mayoría de labores genéricas de TIC.
>
> **Párrafo III:** Modelo C: Es el modelo de estructura más simple y se ajusta a Instituciones Gubernamentales con baja complejidad en términos de infraestructura y servicios TIC brindados.
>
> **Párrafo IV:** La selección del Modelo a ser adoptado por las instituciones se realizará en coordinación con el Ministerio de Administración Pública, y refrendado por este. La Oficina Presidencial de Tecnologías de la Información y Comunicación (OPTIC) apoyará al Ministerio de Administración Pública en la verificación del cumplimiento de los criterios establecidos.

2.7 Falta de control y monitoreo en los accesos a los sistemas de información

Considerando, que el informe de evaluación evidencia que el área de seguridad y monitoreo del departamento de TIC no ha sido responsable del control y monitoreo de algunos de los accesos a los sistemas de información de la entidad, además, se han delegado funciones propias de dicha área a otras divisiones y departamentos.

Disposiciones jurídicas

Considerando, que, en ese sentido, procede observar las disposiciones de los subtítulos PO4.11 Segregación de Funciones, PO4.13 Personal Clave de TI y PO7.5 Dependencia Sobre los Individuos, epígrafe Objetivos de Control, títulos PO Planear y Organizar, PO4 Definir los Procesos, Organización y Relaciones de TI. y PO7. Administrar los Recursos Humanos de TI, del marco de evaluación de Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT 4.1), que expresan:

> **PO4.11 Segregación de Funciones**

Implementar una división de roles y responsabilidades que reduzca la posibilidad de que un solo individuo afecte negativamente un proceso crítico. La gerencia también se asegura de que el personal realice sólo las tareas autorizadas, relevantes a sus puestos y posiciones respectivas.

PO4.13 Personal Clave de TI
Definir e identificar al personal clave de TI y minimizar la dependencia en un solo individuo desempeñando una función de trabajo critica.

PO7.5 Dependencia Sobre los Individuos
Minimizar la exposición a dependencias críticas sobre individuos clave por medio de la captura del conocimiento (documentación), compartir el conocimiento, planeación de la sucesión y respaldos de personal.

2.8 Falta de un aplicativo para monitoreo de los controles de TIC

Considerando, que el informe de evaluación evidencia que el departamento de TIC no posee un software que permita alertar e identificar de forma oportuna y efectiva cambios en los sistemas de información, es decir, no cuentan con una herramienta apropiada de monitoreo.

Disposiciones jurídicas

Considerando, que, en ese sentido, procede observar las disposiciones de los literales a, b, c, d y e, de la sección, 5.04. Herramientas y Sistemas de Monitoreo, de la Norma para la Implementación y Gestión de la Conectividad en el Estado Dominicano, NORTIC B1, de fecha 29 de julio del año 2016, que expresan:

SECCIÓN 5.04. Herramientas y Sistemas de Monitoreo

(a) Todos los componentes de la infraestructura de TIC deben ser monitoreados continuamente en conjunción con la gestión de eventos, de modo que los posibles problemas o las tendencias puedan ser identificadas antes de que se produzcan un fallo o cualquier evento de degradación de rendimiento.

(b) La vigilancia debe ser automatizada y la misma debe tener alertas periódicas con las acciones correctivas que permitan evitar que ocurra un impacto adverso en la infraestructura.

(c) El departamento de TIC debe tener un Software de Gestión de la Infraestructura del Centro de Datos (DCIM, por sus siglas en inglés) para su monitoreo y gestión.

(d) El departamento de TIC debe disponer de un Centro de Control de la Red (NOC, por sus siglas en inglés), y que el mismo brinde servicios las 24 horas, 7 días de la semana, los 365 días del año.

(e) Los componentes y elementos identificados por el organismo que deben ser objeto de seguimiento y monitoreo, como mínimo debe evaluarse lo siguiente:

- La utilización de la Unidad Central de Procesamiento (CPU, por sus siglas en inglés).
- La utilización del almacén de archivos, tales como:

° Discos duros.
° Particiones.
° Segmentos.
- El uso de las aplicaciones.

- La utilización de bases de datos.
- Tasas de transacción, tasas de error y reintentos.
- Los números de sistema/aplicación inicios de sesión y usuarios concurrentes.
- Los números de nodos de red en uso, y los niveles de utilización.

2.9 Falta de segregación de funciones

Durante los procedimientos de levantamiento de informaciones, aplicación de cuestionarios e indagaciones realizados a las divisiones y áreas que conforman el departamento de TIC, en los meses de septiembre y octubre de 2021, se comprobó que, al momento de los procedimientos, existen debilidades en la segregación de funciones.[5]

Disposiciones Jurídicas

Considerando, que en ese sentido, procede observar las disposiciones de los subtítulos PO4.11 Segregación de Funciones, PO4.13 Personal Clave de TI y PO7.5 Dependencia Sobre los Individuos, epígrafe Objetivos de Control, títulos PO Planear y Organizar, PO4 Definir los Procesos, Organización y Relaciones de TI. y PO7. Administrar los Recursos Humanos de TI, del marco de evaluación de Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT 4.1), que expresan:

> **PO4.11 Segregación de Funciones**
>
> Implementar una división de roles y responsabilidades que reduzca la posibilidad de que un solo individuo afecte negativamente un proceso crítico. La gerencia también se asegura de que el personal realice sólo las tareas autorizadas, relevantes a sus puestos y posiciones respectivas.
>
> **PO4.13 Personal Clave de TI**
>
> Definir e identificar al personal clave de TI y minimizar la dependencia en un solo individuo desempeñando una función de trabajo critica.
>
> **PO7.5 Dependencia Sobre los Individuos**
>
> Minimizar la exposición a dependencias críticas sobre individuos clave por medio de la captura del conocimiento (documentación), compartir el conocimiento, planeación de la sucesión y respaldos de personal.

2.10 Debilidades de la gestión de respaldos de información (backups)

[5] 1-División de operaciones TIC (Infraestructura) actualmente ejerce las siguientes funciones no propias del área:
i) Implementación desde el área de infraestructura TIC de la DGCP de los controles y mecanismos de seguridad desarrollados que debieron ser implementados por el área de seguridad y monitoreo TIC.
ii) Gestión de los usuarios de las cuentas de usuarios destinados a los servicios, la cual le corresponde al área de seguridad y monitoreo TIC gestionar.
La división de desarrollo e implementación de sistemas realiza el proceso completo para el desarrollo de un sistema o aplicativo incluyendo el desarrollo de la base de datos, el cual se debería de realizar desde el área de infraestructura TIC.
Los analistas funcionales en la gestión de usuario del portal transaccional con la asignación de permisos a los usuarios administrativos roles, que solo debería de tener el área de seguridad y monitoreo TIC.
El administrador de base de datos no desarrolla en la actualidad las bases de datos utilizadas en los aplicativos desarrollados en la DGCP.

Considerando, que el informe de evaluación evidencia que en cuestionario aplicado en fecha 19 de septiembre de 2021 al Departamento de TIC de la entidad, se verificaron que existen debilidades relacionadas con la gestión de respaldos de la información (backups).[6]

Disposiciones jurídicas

Considerando, que en ese sentido, procede observar las disposiciones de los literales a, subliterales i, subliteral a, ii, subliteral a, iii, subliteral a, iv, v y b, c; los literales a, subliterales i y ii, b, c y d, del apartado 2.03.3.1 Almacenamiento fuera de sitio; los literales a, subliterales i, ii y iii, b, c y d, del apartado 2.03.3.3 Confidencialidad de la información almacenada; y los literales a, b, c y d del Apartado 2.03.4.2 Prueba de la recuperación, de la subsección 2.03.3. Respaldo de la información, de la Norma para la Seguridad de las Tecnologías de la Información y Comunicación en el Estado Dominicano NORTIC A7, de fecha abril del año 2016, que expresan:

> **Sub-sección 2.03.3. Respaldo de la información**
>
> Por la naturaleza y alcance de la información generada por los organismos, los procesos de respaldo y restauración de la información son, quizás, los activos más importantes luego de la vida humana. De no disponer de los medios administrativos, procedimientos y recursos técnicos adecuados podría ser imposible llevar a cabo un proceso de continuidad exitoso.
>
> **(a)** Los organismos gubernamentales deben tener políticas, procedimientos y recursos tecnológicos para los sistemas de respaldo de la información.
>
> **(i)** Los organismos gubernamentales deben definir cuáles informaciones serán incluidas en el respaldo.
>
> **a)** Las informaciones vitales para el correcto funcionamiento de los organismos deben ser incluidas dentro del programa de respaldo.
>
> **(ii)** Los organismos gubernamentales deben disponer de un espacio físico y seguro para el almacenamiento de los respaldos.
>
> **a)** Solo el personal autorizado podrá acceder y manipular los respaldos.
>
> **(iii)** Los organismos gubernamentales deben asegurar que los datos respaldados están íntegros y libres de errores para su posterior uso.
>
> **a)** Debe probarse periódicamente y aleatoriamente los respaldos realizados para garantizar su integridad.

6

a. Ausencia de almacenamiento externos de los respaldos de información realizados a la infraestructura interna (archivos, bases de datos de aplicaciones, correo electrónico, active directory, entre otros).
b. Los planes de respaldos y restauración, tanto de la infraestructura interna como del Portal Transaccional no aprobados por la dirección ejecutiva de la DGCP durante el procedimiento realizado.
c. Las pruebas de los respaldos de la información, no se documentan.
d. La herramienta utilizada para la automatización de los respaldos de información de su infraestructura interna (Veritas Backup Exec) sin licenciamiento durante el procedimiento realizado.
e. Usuarios no pertenecientes a la división de operaciones TIC (infraestructura), con accesos a la carpeta donde se encuentran los backups de las bases de datos.

(iv) Los organismos gubernamentales deben definir la vigencia que tendrá cada respaldo realizado.

(v) Debe realizarse una frecuencia de respaldos semanal, mensual y anual de todos los datos identificados como críticos para el organismo.

(b) Los organismos deben presentar información verificable del cumplimiento y nivel de éxito de este proceso.

(c) Los organismos deben hacer el aprovisionamiento necesario de medios de almacenamiento para poder cumplir con las demás directivas antes expuestas.

Apartado 2.03.3.1 Almacenamiento fuera de sitio

(a) Debe mantener una copia fiel de la información respaldada en una localidad física diferente, fuera de las facilidades inmediatas donde se realiza el respaldo.

(i) Esta localidad alternativa debe tener los controles de protección necesarios para que la información guardada no sea dañada tanto por factores ambientales, operacional o mal uso.

(ii) Los medios de respaldo móviles, tales como cintas, y otras unidades externas, deben ser almacenadas bajo llave o con un acceso controlado.

(b) Estos lugares de almacenamiento de los medios deben incluir no solo el control de acceso sino también la protección contra fuego, humedad, electricidad estática e influencia electromagnético, iluminación, entre otros controles de seguridad.

(c) La información respaldada fuera de sitio debe también estar fuera de línea, es decir, que utilice dispositivos discretos que no requieran ni estén conectados a otros sistemas para proteger la información.

(d) Los medios de almacenamiento utilizados deben estar capacitados para proteger la información que contienen, aun después de períodos prolongados, de hasta varios años, sin recibir electricidad.

Apartado 2.03.3.3 Confidencialidad de la información almacenada

(a) Para fines de mantener la confidencialidad de la información respaldada los organismos deben:

(i) Cifrar la información que se encuentra en los medios de respaldo móviles, para lo cual deben hacer las previsiones necesarias para la gestión de las llaves, contraseñas o cualquier otro esquema de autorización.

(ii) No indicar cual información contienen estos medios, para lo cual deben elaborar un esquema de etiquetado que sea útil desde el punto administrativo pero que no revele la información que está respaldada.

(iii) En caso de transporte físico, fuera de las facilidades del organismo, estos medios deben ser transportados por un personal autorizado.

(b) Los medios a transportar no deben ser incluidos en rutas de trabajo del personal que labora externamente evitando que el dispositivo esté lo menos posible en posesión de este personal y sean dejados en vehículos o en situaciones de riesgo en que puedan ser perdidos o sustraídos.

(c) El organismo debe disponer de mecanismos administrativos que permitan la rápida y correcta organización y acceso a los medios de almacenamiento externos.

(d) La pérdida de un dispositivo personal con información clasificada del organismo debe ser notificada y ser manejada como un incidente de seguridad de Información para ser categorizado y planificar la respuesta correspondiente al nivel del impacto del mismo.

Apartado 2.03.4.2 Prueba de la recuperación

(a) Los organismos deben de disponer de los procesos administrativos y recursos tecnológicos para la verificación de las facilidades de restauración, así como la integridad de la información respaldada.

(b) Los organismos deben disponer de los indicadores necesarios para poder confirmar cuando la prueba ha sido exitosa.

(c) En caso de que las pruebas no arrojen un resultado exitoso, debe abrirse un caso para la identificación y solución de la causa raíz del problema, realizando de nuevo el proceso de respaldo y restauración hasta que los resultados obtenidos sean satisfactorios.

(d) En caso de no poder disponer de los medios, recursos o cualquier otro factor crítico para las pruebas debe notificarse a la alta dirección con el más alto nivel de prioridad para la toma de acción correspondiente.

2.11 Debilidades de control en el área de desarrollo e implementación de sistemas

Considerando, que el informe de evaluación evidencia debilidades de control en el área de desarrollo e implementación de sistemas [7]

Disposiciones jurídicas

Considerando, que el informe de evaluación evidencia las debilidades de control en el área de desarrollo e implementación de sistemas, especificadas precedentemente; en ese sentido, procede observar las disposiciones de la sección 2.02 Desarrollo del software gubernamental, de la Norma sobre el Desarrollo y Gestión del Software en el Estado Dominicano NORTIC A6, de fecha abril del año 2016, que expresan:

Sección 2.02 Desarrollo del software gubernamental

En el Estado Dominicano son necesarias directrices y políticas para el correcto establecimiento de estándares sobre el software desarrollado en los organismos, para lo cual, en esta sección, se establecen las pautas necesarias para lograr un desarrollo óptimo bajo las mejores metodologías y prácticas. Ver sección 2.05. Marco de desarrollo recomendado.

[7] a. No se rige por una metodología para el desarrollo de los sistemas.
b. No tienen los controles de las aplicaciones, considerados para el desarrollo de esta, consistentes con los estándares de seguridad de la organización.
c. No se realizan análisis funcional de las soluciones propuesta.
d. No cuenta con un control que les permita a los usuarios finales evaluar todas las etapas de los sistemas desarrollados.
e. No ha desarrollado un mecanismo para medir el grado de satisfacción de los usuarios finales.

Considerando, que procede observar las disposiciones del literal PO8.3 Estándares de Desarrollo y de Adquisición, subtítulo Objetivos de Control, título PO8 Planear y Organizar, Administrar la Calidad, del marco de evaluación de Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT 4.1), que expresan:

> **PO8.3 Estándares de Desarrollo y de Adquisición**
>
> Adoptar y mantener estándares para todo desarrollo y adquisición que siga el ciclo de vida, hasta el último entregable e incluir la aprobación en puntos clave con base en criterios de aceptación acordados. Los temas a considerar incluyen estándares de codificación de software, normas de nomenclatura; formatos de archivos, estándares de diseño para esquemas y diccionario de datos; estándares para la interfaz de usuario; interoperabilidad; eficiencia de desempeño de sistemas; escalabilidad; estándares para desarrollo y pruebas; validación contra requerimientos; planes de pruebas; y pruebas unitarias, de regresión y de integración.

2.12 Debilidades y vulnerabilidades críticas generales del portal transaccional

Considerando, que el informe de evaluación evidencia vulnerabilidades críticas en el área de monitoreo TIC.[8]

Disposiciones jurídicas

Considerando, que, en ese sentido, procede observar las disposiciones de los literales a y d de la sub-sección 2.01.3 adquisición del software de la sección 2.01. Administración del software, de la Norma sobre el Desarrollo y Gestión del Software en el Estado Dominicano NORTIC A6, de fecha abril del año 2016, que expresan:

> **SECCIÓN 2.01. Administración del software**
>
> Los organismos gubernamentales requieren políticas y controles para una correcta administración del software, los cuales permitan un control sobre los mismos para asegurar el correcto funcionamiento y desempeño.
>
> **Sub-sección 2.01.3. Adquisición del Software**
> **(a)** Los organismos gubernamentales que contraten servicios de desarrollo de aplicaciones, deben exigir a los desarrolladores la propiedad exclusiva de la aplicación y el código fuente desarrollado.
>
> **(d)** El software de Gestión de Servidores Web (http server y servicios relacionados) debe ser abierta.

---

[8]a Los equipos FORTINET – FortiGate 500D y FortiGate 600C no se le realizaron actualizaciones al software de los equipos manteniendo la versión 5.2.6 y en la actualidad el proveedor va por la versión 5.2.10.
b. Equipo de balanceo de datos FORTINET – FortiADC 2000D con la configuración de seguridad que el equipo tiene por defecto.
c. Usuario ADMIN utilizado tanto por el área de seguridad y monitoreo TI como por el área de análisis funcional.
d. Usuario ADMIN, quien es utilizado por diferentes servidores públicos sin trazabilidad de eventos realizados (pistas de auditoría).
e. Usuarios no pertenecientes al área de seguridad y monitoreo TIC con acceso a los equipos (FortiGate 500D, frontend) y (FortiGate 600C, backend).
f. Excolaboradores con usuarios activos en el Portal Transaccional (Ejemplo: Aleida Batista - abatista@dgcp.gob.do).
g. El departamento de TIC no cuenta con los accesos al código fuente del Portal Transaccional.
h. Las contraseñas de los usuarios internos y externos del Portal Transaccional no caducan o expiran.

Considerando, que procede observar las disposiciones de los literales b, c, d y e, de la sección 3.01 Control de Acceso de Usuario; literal a y subliterales iv y v de la subsección 2.02.1 Responsabilidad del empleado, sección 2.02. Políticas para la administración de la información, de la Norma para la Seguridad de las Tecnologías de la Información y Comunicación en el Estado Dominicano NORTIC A7, de fecha abril del año 2016, que expresan:

> **Subsección 2.02.1. Responsabilidad del empleado**
>
> **a)** Los empleados de los organismos gubernamentales deben cumplir con las siguientes responsabilidades:
>
> **(iv)** El empleado público no debe divulgar las credenciales que utiliza dentro del organismo gubernamental.
>
> **(v)** El empleado público no debe divulgar información confidencial a otro personal no autorizado para circular con dicha información.
>
> **SECCIÓN 3.01. Control de acceso de usuario**
>
> **(b)** Los organismos gubernamentales deben hacer una revisión de los accesos de los usuarios anualmente. Esta revisión debe estar documentada.
>
> **(c)** Los organismos gubernamentales deben hacer una revisión, modificación o eliminación de los accesos de los usuarios al momento en que estos:
>
> • Sean cancelados.
> • Sean promovidos.
> • Sean transferidos a diferentes localidades.
> • En caso de fallecimiento.
> • Cambien de funciones dentro del mismo organismo.
>
> **(d)** La unidad de Seguridad y Monitoreo debe tener un personal asignado del área de Administración de accesos para la gestión de accesos de los empleados.
>
> **(e)** Las aplicaciones deben disponer de un esquema de control de acceso que efectivamente controle la separación de roles de los usuarios, administradores y diferentes grupos de usuarios según los perfiles de uso.

Considerando, que procede observar las disposiciones de los subliterales v, viii y ix, literal b, sección 5.02 Gestión de Centro de datos y servidores, de la Norma para la Implementación y Gestión de la Conectividad en el Estado Dominicano, NORTIC B1, de fecha 29 de julio del año 2016, que expresan:

> **SECCIÓN 5.02. Gestión del centro de datos y Servidores**
>
> **(b)** Para la correcta administración de los servidores dentro del centro de datos, deben seguirse las directrices a continuación:
>
> **(v)** Debe realizarse un mantenimiento continuo, el cual incluya la sustitución de servidores antes de estos ser obsoletos para apoyar la evolución de los servicios.

(viii) Todas las estaciones de trabajo deben estar protegidas por políticas para ser accedidas solo por el personal autorizado.

(ix) Los servidores de la infraestructura, deben tener las últimas actualizaciones y parches de seguridad.

Considerando, que procede a observar las disposiciones del literal 6.1.2 Segregación de tareas, del anexo 6 Aspectos Organizativos; literales 9.1.1 Política de control de accesos y 9.1.2 Control de acceso a las redes y servicios asociados del Anexo 9. Control de Accesos; literales 9.2.1 Gestión de altas/bajas en el registro de usuarios, 9.2.2 Gestión de los derechos de acceso asignados a usuarios, 9.2.3 Gestión de los derechos de acceso con privilegios especiales, 9.2.4 Gestión de información confidencial de autenticación de usuarios, 9.2.5 Revisión de los derechos de acceso de los usuarios, 9.2.6 Retirada o adaptación de los derechos de acceso y 9.4.3 Gestión de contraseñas de usuario de los subliterales 9.2 Gestión de acceso de usuario y 9.4 Control de acceso a sistemas y aplicaciones del Anexo 9. Control de Accesos; literal 12.4.3 Registros de actividad del administrador y operador del sistema del Anexo 12. Seguridad en la Operativa del Estándar para la Seguridad de la Información de la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional ISO/IEC 27002, que expresan:

Anexo 6. Aspectos Organizativos. El objetivo del presente dominio es establecer la administración de la seguridad de la información, como parte fundamental de los objetivos y actividades de la organización.

6.1.2 Segregación de tareas: Se deberían segregar tareas y las áreas de responsabilidad ante posibles conflictos de interés con el fin de reducir las oportunidades de una modificación no autorizada o no intencionada, o el de un mal uso de los activos de la organización.

Anexo 9. Control de Accesos. El objetivo del presente dominio es controlar el acceso por medio de un sistema de restricciones y excepciones a la información como base de todo sistema de seguridad informática (redes y sistemas/plataformas de información).

9.1.1 Política de control de accesos: Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización.

9.1.2 Control de acceso a las redes y servicios asociados: Se debería proveer a los usuarios de los accesos a redes y los servicios de red para los que han sido expresamente autorizados a utilizar.

9.2 Gestión de acceso de usuario
El objetivo es el de garantizar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información y servicios.

9.2.1 Gestión de altas/bajas en el registro de usuarios: Debería existir un procedimiento formal de alta y baja de usuarios con objeto de habilitar la asignación de derechos de acceso.

9.2.2 Gestión de los derechos de acceso asignados a usuarios: Se debería de implantar un proceso formal de aprovisionamiento de accesos a los usuarios para asignar o revocar derechos de acceso a todos los tipos de usuarios y para todos los sistemas y servicios.

9.2.3 Gestión de los derechos de acceso con privilegios especiales: La asignación y uso de derechos de acceso con privilegios especiales debería ser restringido y controlado.

9.2.4 Gestión de información confidencial de autenticación de usuarios: La asignación de información confidencial para la autenticación debería ser controlada mediante un proceso de gestión controlado.

9.2.5 Revisión de los derechos de acceso de los usuarios: Los propietarios de los activos deberían revisar con regularidad los derechos de acceso de los usuarios.

9.2.6 Retirada o adaptación de los derechos de acceso: Se deberían retirar los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información a la finalización del empleo, contrato o acuerdo, o ser revisados en caso de cambio.

9.4 Control de acceso a sistemas y aplicaciones
El objetivo es impedir el acceso no autorizado a la información mantenida por los sistemas y aplicaciones.

9.4.3 Gestión de contraseñas de usuario: Los sistemas de gestión de contraseñas deberían ser interactivos y asegurar contraseñas de calidad.

Anexo 12. Seguridad en la Operativa. El objetivo es controlar la existencia de los procedimientos de operaciones y el desarrollo y mantenimiento de documentación actualizada relacionada.

12.4.3 Registros de actividad del administrador y operador del sistema: Se deberían registrar las actividades del administrador y del operador del sistema y los registros asociados se deberían proteger y revisar de manera regular.

12.6 Gestión de la vulnerabilidad técnica. El objetivo es evitar la explotación de vulnerabilidades técnicas.

12.6.1 Gestión de las vulnerabilidades técnicas: Se debería obtener información sobre las vulnerabilidades técnicas de los sistemas de información de manera oportuna para evaluar el grado de exposición de la organización y tomar las medidas necesarias para abordar los riesgos asociados.

Considerando, que procede observar las disposiciones de los literales AI2.3 Control y Posibilidad de Auditar las Aplicaciones y AI2.4 Seguridad y Disponibilidad de las Aplicaciones, subtítulo Objetivos de Control, título AI2 Adquirir e implementar, Adquirir y Mantener Software Aplicativo; literales AI3.2 Protección y Disponibilidad del Recurso de Infraestructura y AI3.3 Mantenimiento de la Infraestructura, subtitulo Objetivos de Control, título AI3 Adquirir e Implementar, Adquirir y Mantener Infraestructura Tecnológica; literal DS3.4 Disponibilidad de Recursos de TI, subtitulo Objetivos de Control, título DS3 Entregar y Dar Soporte, Administrar el Desempeño y la Capacidad, del marco de evaluación de Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT 4.1), que expresan:

AI2.3 Control y Posibilidad de Auditar las Aplicaciones
Implementar controles de negocio, cuando aplique, en controles de aplicación automatizados tal que el procesamiento sea exacto, completo, oportuno, autorizado y auditable.

AI2.4 Seguridad y Disponibilidad de las Aplicaciones

Abordar la seguridad de las aplicaciones y los requerimientos de disponibilidad en respuesta a los riesgos identificados y en línea con la clasificación de datos, la arquitectura de la

información, la arquitectura de seguridad de la seguridad de la información y la tolerancia a riesgos de la organización.

AI3.2 Protección y Disponibilidad del Recurso de Infraestructura

Implementar medidas de control interno, seguridad y auditabilidad durante la configuración, integración y mantenimiento del hardware y del software de la infraestructura para proteger los recursos y garantizar su disponibilidad e integridad. Se deben definir y comprender claramente las responsabilidades al utilizar componentes de infraestructura sensitivos por todos aquellos que desarrollan e integran los componentes de infraestructura. Se debe monitorear y evaluar su uso.

AI3.3 Mantenimiento de la Infraestructura

Desarrollar una estrategia y un plan de mantenimiento de la infraestructura y garantizar que se controlan los cambios, de acuerdo con el procedimiento de administración de cambios de la organización. Incluir una revisión periódica contra las necesidades del negocio, administración de parches y estrategias de actualización, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad.

DS3.4 Disponibilidad de Recursos de TI

Brindar la capacidad y desempeño requeridos tomando en cuenta aspectos como cargas de trabajo normales, contingencias, requerimientos de almacenamiento y ciclos de vida de los recursos de TI. Deben tomarse medidas cuando el desempeño y la capacidad no están en el nivel requerido, tales como dar prioridad a las tareas, mecanismos de tolerancia de fallas y prácticas de asignación de recursos. La gerencia debe garantizar que los planes de contingencia consideran de forma apropiada la disponibilidad, capacidad y desempeño de los recursos individuales de TI.

2.13 Falta de controles en asignación de roles en el servidor de bases de datos

Considerando, que el informe de evaluación evidencia debilidades relacionadas con la asignación de roles en el servidor de bases de datos.[9]

Disposiciones jurídicas

Considerando, que, en ese sentido, procede observar las disposiciones de los subliterales 9.2.3 Gestión de los derechos de acceso con privilegios especiales y 9.2.6 Retirada o adaptación de los derechos de acceso, literal 9.2 Gestión de acceso de usuario, Anexo 9. Control de Accesos, del Estándar para la Seguridad de la Información de la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional ISO/IEC 27002, que expresan:

> **Anexo 9. Control de Accesos.** El objetivo del presente dominio es controlar el acceso por medio de un sistema de restricciones y excepciones a la información como base de todo sistema de seguridad informática (redes y sistemas/plataformas de información).

[9]a. Existen siete (7) empleados con rol fijo "sysadmin". Incluyendo colaboradores que ejercen las funciones de administradores de base de datos. Los miembros del rol citado pueden realizar cualquier actividad en el Servidor.
b. Proveedor del Portal Transaccional con usuarios habilitados (Ejemplo: po-indra1)
c. Existen ocho (8) cuentas de servicio con rol fijo "sysadmin" (Ejemplos: nextdbapp, pacc, entre otras).

9.2 Gestión de acceso de usuario
El objetivo es el de garantizar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información y servicios.

9.2.3 Gestión de los derechos de acceso con privilegios especiales: La asignación y uso de derechos de acceso con privilegios especiales debería ser restringido y controlado.

9.2.6 Retirada o adaptación de los derechos de acceso: Se deberían retirar los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información a la finalización del empleo, contrato o acuerdo, o ser revisados en caso de cambio.

Considerando, que procede observar las disposiciones de los literales a, b y c y sub-literales i, ii, iii, iv, v y vi, de la sub-sección 4.02.2 monitoreo y afinamiento de una base de datos, de la Norma sobre el Desarrollo y Gestión del Software en el Estado Dominicano NORTIC A6, de fecha abril del año 2016, que expresan:

Sub-sección 4.02.2 monitoreo y afinamiento de una base de datos

(a) El organismo debe contar con herramientas que aseguren la operación y el funcionamiento de la base de datos y esta debe contar con las siguientes características como mínimo:

- Indicadores de rendimiento: La Unidad de Procesamiento Central (CPU, por sus siglas en inglés), memoria física y disco duro.
- Capacidad de identificar segmentos de código con problemas.
- Disponer de informes de gestión.
- Almacenamiento de informes de rendimiento.

(b) La herramienta de monitoreo usada o adquirida por el organismo debe informar acerca de los siguientes estados:

- La carga del trabajo: Para verificar la demanda a la que es sometido el DBMS.
- Volumen de trabajo: Para definir la capacidad del servidor para procesar datos, en términos de recursos de hardware.
- Los recursos: Para administrar el hardware y las herramientas de software como:

- El Kernel de la base de datos.
- Los controladores de caché.
- Los discos duros.

- La contención: Para cuando la carga a la que es sometido el DBMS es muy alta y se encuentran comprometidos todos los recursos del servidor.

(c) Para el afinamiento de la base de datos deben aplicarse las siguientes practicas:
(i) Identificar que las tablas tengan los índices adecuados para responder de la manera correcta a las consultas de los usuarios.
(ii) Configurar adecuadamente la memoria y los cachés de datos y procedimientos.
(iii) Alinear la implementación de las bases de datos con la infraestructura de TIC existente.
(iv) Monitorear constantemente las bases de datos y aplicaciones.
(v) Implementar procedimientos de reorganización de las bases de datos.
(vi) Implementar procedimientos de actualización de las estadísticas de las bases de datos.

Conclusiones jurídicas

En el informe de evaluación practicado por la Cámara de Cuentas de la República al Departamento de Tecnología de la Información y Comunicación y Recursos Tecnológicos de la Dirección General de Contrataciones Públicas (DGCP), por el período comprendido entre el 1ro. de enero de 2017 y el 31 de diciembre del año 2020, reveló considerables debilidades en el manejo y gestión de esta área evidenciándose ausencia de mecanismos de evaluación y de implementación de sistemas, así como ausencia de planes estratégicos en orden a buenas prácticas, desactualización de políticas y procedimientos, falta de matriz de riesgo, debilidades en los sistemas operativos (accesos a usuarios, contraseñas, falta de aplicativo de monitoreo), debilidad en el respaldo de la información, falta de segregación de funciones organizativas, entre otros aspectos que conllevan la vulnerabilidad general del sistema tecnológico y de la información de la entidad auditada.

Estos hallazgos constituyen un incumplimiento a los deberes a cargo de los funcionarios incumbentes de la entidad evaluada, quiénes son los responsables de la creación, implementación, desarrollo y monitoreo de los componentes de control interno aplicados al área de tecnología de la entidad. En ese sentido, en su gestión inobservaron el estricto cumplimiento de la Ley n.° 10-07, de fecha 8 de enero del año 2007, así como su Reglamento de Aplicación, aprobado mediante Decreto n.° 491-07 de fecha 30 de agosto del año 2007, la Ley n.° 41-08, de Función Pública, de fecha 16 de enero del año 2008 y las normativas complementarias en materia de tecnología, especialmente las NORTIC y las directrices de marco de referencia que le integran, COBIT, ANSI/TIA-942-A, las cuales permiten y coadyuvan al efectivo uso e implementación de las TIC en la administración pública.

Los mecanismos o procesos referidos en las normativas aplicables al control interno de las áreas de tecnología de la administración pública permiten materializar el uso eficaz de las TIC al servicio de la buena administración; de ahí que resulta esencial asegurar que los procesos se realicen de manera correcta, además, de que las decisiones tomadas sean cónsonas con la planificación y los objetivos de la entidad; dichos mecanismos deben ser verificados y observados con la debida diligencia por los principales funcionarios, en su calidad de administradores de los recursos públicos.

A partir de lo expuesto anteriormente, se concluye en las consideraciones jurídicas siguientes, respecto de los hallazgos evidenciados en el informe de evaluación practicado:

- **Con relación a los hallazgos relativos a la gestión del Departamento, esto es las debilidades y vulnerabilidades en cuanto la ausencia de mecanismos y áreas de evaluación, la falta de recursos para el desarrollo e implementación de proyectos basados en buenas prácticas, la ausencia de planes de contingencia, de continuidad de negocio y recuperación de desastres, la falta de mecanismo para gestión de cambios de contraseñas, la no creación ni implementación de mecanismos de segregación efectiva de funciones (2.1); así como la falta de revisión y/o actualización de las políticas y procedimientos (2.2); la falta de una herramienta o matriz de riesgo (2.3):**

El incumplimiento evidenciado en los hallazgos referidos refleja que los funcionarios de la entidad auditada inobservaron lo relativo al monitoreo y evaluación, el cual resulta ser uno de los componentes fundamentales del proceso de control interno, de conformidad a las disposiciones del artículo 47 del reglamento de aplicación de la ley 10-07, aprobado mediante decreto número 491-07.

Es preciso considerar que el componente de monitoreo y evaluación que contienen las disposiciones de control interno resultan ser instrumentos de gestión que permiten proveer la información necesaria para la toma de decisiones y la planificación de mejoras en las intervenciones y la gestión de las instituciones públicas. La evaluación como proceso constante está estrechamente ligada a los procesos de planificación y presupuestación, pues su enfoque va en orden a medir los resultados de lo implementado.

Debido a lo anterior, es que se correlaciona la falta de evaluación y monitoreo con la ausencia de planificación estratégica en los aspectos puntuales evidenciados en el departamento de TI de DGCP; de tal suerte que la inobservancia del proceso evaluativo impide concretizar la aspiración de prácticas coherentes a la buena administración en perjuicio del quehacer estatal.

Por otro lado, dentro de las vulnerabilidades evidenciadas resalta la falta de mecanismos de cambios de contraseñas, lo cual entraña un riesgo importante con relación a la integridad de la data y sistema operativo de cualquier organización, pues es fácilmente afectable.

De igual manera, la falta de actualización de políticas y procedimientos, así como la ausencia de matriz de riesgo, evidencian debilidades importantes relativas a la gestión del departamento auditado en aspectos que resultan sustanciales al área, dada la naturaleza dinámica de las tecnologías de la información y la necesidad de que se cuente con la valoración de riesgo correspondiente. Esto resulta ser una de las tareas principales de un departamento de tecnología de cualquier entidad estatal pues se requiere la valoración de las situaciones que pudiesen afectar la data y sistemas operativos de la entidad, más aún debido a la calidad de la DGCP.

- **Con relación a los hallazgos relativos a la vulnerabilidad, en cuanto a infraestructura, del centro de datos (Data Center), en los subsistemas mecánico, arquitectura y eléctrico (2.4):**

La inobservancia de las normativas relativas a la adecuación de la infraestructura del centro de datos impide contar con medidas de seguridad física, así como de protección a factores ambientales y otros, lo cual pone en riesgo la administración de las instalaciones que albergan la data institucional.

- **Con relación a los hallazgos relativos a debilidades del control y monitoreo; esto es ausencia de controles en el servidor de dominio (2.5); falta de control y monitoreo en los accesos a los sistemas de información (2.7); falta de un aplicativo para monitoreo de los controles de TIC (2.8); debilidades de la gestión de respaldos de información o *backups* (2.10); debilidades de control en el área de desarrollo e implementación de sistemas (2.11); debilidades y**

vulnerabilidades criticas generales del portal transaccional (2.12); falta de controles en asignación de roles en el servidor de base de datos (2.13):

Las inobservancias detectadas en la auditoría permiten colegir que la entidad auditada falló en el proceso de gestión y control para garantizar en cumplimiento irrestricto a estas disposiciones. Las NORTIC promueven la rendición de cuentas y la transparencia. Ésta ayuda, no solo a ser más eficiente, sino que contribuye a transparentar procesos; creando instituciones eficientes y eficaces que fomenten la confianza pública en cuanto al fortalecimiento de la capacidad de respuesta de la administración pública y garantizar la colaboración en el proceso de desarrollo para modernizar y fortalecer la administración del Estado.

Las inobservancias a las directrices aplicables al sistema NORTIC por parte del Departamento de TIC, constituye un incumplimiento a los deberes formales dispuestos en los marcos de referencia y los estándares internacionales de las buenas prácticas de TIC, esta conducta lesiva situaron a la DGCP en un ambiente de vulnerabilidad en cuanto al manejo de control y monitoreo de acceso a los sistema de información, la falta de control y las debilidades en gestión de respaldos de información o *backups*, generando además una infraestructura crítica al Sistemas TIC al no obtemperar en niveles de protección adecuadas en materia de ciberseguridad.

- **Con relación a los hallazgos relativos a la falta de estructura organizativa y funcional adecuada; esto es que la estructura organizativa del departamento de TIC de DGCP no está alineada a los órganos rectores (2.6); así como la falta de segregación de funciones (2.9):**

La falta de estructura organizativa adecuada según las directrices del órgano rector, esto es el MAP, impide lograr el objetivo del desarrollo de las capacidades institucionales en torno al área de que se trata.

Un aspecto que resalta es la falta de división de roles y responsabilidades en los servidores del departamento de tecnología, lo cual aumenta la posibilidad de que un solo individuo afecte negativamente procesos críticos, así como que tenga incidencia respecto a tareas diferentes a las autorizadas.

De manera general, es preciso referir que el cumplimiento de las normativas aplicables en materia de control interno en el área de tecnología de las instituciones, coadyuvan a lo que ha considerado el Tribunal Constitucional dominicano, sobre la buena administración, sobre esto refiere que *"todo procedimiento administrativo debe lograr su finalidad y evitar dilaciones indebidas. Este mandato normativo da existencia actual a lo que se ha configurado como un derecho fundamental nuevo entre nosotros, denominado "derecho al buen gobierno o a la buena administración"*[10]. De igual forma, refiere en sentencia TC/0203/13[11] que *"la eficacia en la actuación de la administración es uno de los soportes*

[10] Tribunal Constitucional, Sentencia TC/0322/14, de fecha 22 de diciembre 2014, p. 15, párrafo 11.8.
[11] Tribunal Constitucional, Sentencia TC/0203/13, de fecha 13 de noviembre del año 2013. Pág., 21.

que garantizan la realización de las personas que conforman un Estado y la protección efectiva de sus derechos fundamentales (...). Este llamado constitucional contrasta con las actuaciones reflejadas en el informe de evaluación referido, que indican que el ente auditado[12] no actúo en apego irrestricto a los principios de la buena administración.

En ese sentido, se determina que las inobservancias presentadas se llevaron a cabo sin tomar en consideración la norma sobre la prestación y automatización del Estado Dominicano, *la llamada NORTIC*[13], concebida con el fin de contar con una herramienta de auditoría con la cual normalizar, homogeneizar y automatizar los servicios y procesos de la administración pública a través del uso e implementación de las TIC y gobierno electrónico.

En consecuencia, la inobservancia al sistema de control interno, en gestión, organización, directivo, operativo, y estratégico, evidencian una falta de control y supervisión de la Dirección General de Compras y Contrataciones, sin advertir las irregularidades que se estaban cometiendo en el Departamento de Tecnología de la Información y Comunicación y Recursos Tecnológicos de la DGCP. Por ende, dichas faltas constituyen un menoscabo al sistema de gestión y de control interno, y, en consecuencia, tal ejercicio permite concluir que las acciones y omisiones de los funcionarios que comprometen su responsabilidad administrativa, en razón, de la aplicación de los artículos 47 y 54, de la Ley n.° 10-04 de fecha 20 de enero del año 2004.

A la luz de lo expuesto precedentemente, se determina que las deficiencias en los procesos del sistema de control interno del departamento de TIC de la Dirección General de Contrataciones Públicas traen como consecuencia la afectación de la eficacia de la buena administración, lo que constituye una violación de uno de los principios de la administración pública consignados en el artículo 138 de la Constitución dominicana

En ese sentido y en consonancia con todo lo anterior expuesto, se determina que las inobservancias presentadas radican en el incumplimiento de la operatividad del sistema de control interno, lo que significa que los principales funcionarios de la entidad evaluada han incumplido con su obligación ineludible de planeación, organización y evaluación, puesto que, los mismos no sólo serán responsables por sus acciones, sino también por sus omisiones, siendo estos pasibles de sanciones administrativas y por acción u omisión, establecidas en los artículos 47 y 54, de la Ley n.° 10-04 de fecha 20 de enero del año 2004.

En virtud de las facultades que le otorga la Constitución dominicana a la Cámara de Cuentas de la República, en su artículo 248, recomendamos que las autoridades actuales implementen, cumplan y procuren el debido seguimiento a las actividades de control que comprenden el sistema de control interno y las normativas NORTIC, con la finalidad de no incurrir en inobservancias de la Ley n.° 10-07, de fecha 8 de enero del año 2007, del Decreto n.° 491-07, que establece el Reglamento de Aplicación de dicha ley, de fecha 30 de agosto del año 2007 y demás leyes, decretos, resoluciones y normativas relativas a la Tecnología de la Información y Comunicación, contribuyendo de esta manera al mejoramiento del

[12] Departamento de Tecnología de la Información y Comunicación y Recursos Tecnológicos de la Dirección General de Contrataciones Públicas (DGCP)

[13] Norma de Prestación y Automatización de los Servicios Públicos sobre del Estado Dominicano

Departamento de Tecnología de la Información y Comunicación y los controles de TI de la Dirección General de Contrataciones Públicas (DGCP).

Es importante identificar a todos aquellos funcionarios y servidores públicos actuales y salientes, cuya actuación u omisión en el desempeño de sus funciones dieron lugar al incumplimiento de las normativas detalladas precedentemente. Las acciones por tomar por las autoridades actuales, de ningún modo significan que sean limitativas con relación a las responsabilidades atribuidas por la Cámara de Cuentas de la República Dominicana.

En la ciudad de Santo Domingo de Guzmán, Distrito Nacional, República Dominicana, a los cuatro (04) días del mes de mayo del año dos mil veintitrés (2023).

Lcda. Yudelka Polanco
Directora jurídica interina
Cámara de Cuentas República Dominicana