GOBIERNO DE LA
REPÚBLICA DOMINICANA

HACIENDA

DIRECCIÓN GENERAL DE CONTRATACIONES PÚBLICAS

Santo Domingo, D.N.
27 de junio de 2023

CIRCULAR CONJUNTA

A los : Ministros de Estado, directores generales y nacionales, administradores generales, ayuntamientos, instituciones del Gobierno Central, instituciones descentralizadas y autónomas del Estado, empresas públicas no financieras y financieras, y demás instituciones sujetas a la aplicación de la Ley núm. 340-06 y sus modificaciones.

Asunto : Recomendaciones generales sobre ciberseguridad en el Sistema Nacional de Compras y Contrataciones Públicas.

Distinguidos señores:

El Centro Nacional de Ciberseguridad (CNCS), en el ejercicio de las atribuciones que le confiere el Decreto núm. 230-18, el cual tiene dentro de sus facultades el desarrollo y seguimiento de la implementación de la Estrategia Nacional de Ciberseguridad, así como la Dirección General de Contrataciones Públicas (DGCP), en su calidad de Órgano Rector del Sistema Nacional de Compras y Contrataciones Públicas (SNCCP), en el ejercicio de las atribuciones que le otorga la Ley núm. 340-06 y sus modificaciones, sobre compras y contrataciones de bienes, servicios y obras, tienen a bien informar lo siguiente:

En fecha 15 del mes de febrero del año 2023, fue suscrito por ambas instituciones un acuerdo de cooperación interinstitucional, en aras de contribuir al logro de los objetivos y metas de la Estrategia Nacional de Ciberseguridad 2030, prevista en el Decreto núm. 313-22, a través de la promoción desde sus respectivos ámbitos de competencia de una cultura nacional de ciberseguridad que se fundamente en la protección efectiva del Estado Dominicano, del desarrollo y seguridad nacional; que derive en un ciberespacio más seguro en el que puedan desarrollarse de manera confiable y permanente las actividades productivas de toda la población.

En ese sentido, se recomienda a las instituciones sujetas al ámbito de aplicación de la Ley núm. 340-06, considerar la implementación y desarrollo de medidas de ciberseguridad para fortalecer su postura institucional, para lo cual ponemos a su disposición las siguientes sugerencias generales a ser tomadas en cuenta en el marco de sus procedimientos de contratación pública destinados a la adquisición de recursos tecnológicos, a saber:

- **Evaluación y gestión de riesgo:** Se recomienda que la institución realice una actualización de su evaluación de riesgo integral contemplando los bienes y servicios tecnológicos que están en proceso de adquisición, para los fines de mitigar las posibles amenazas de ciberseguridad.

- **Recomendaciones requisitos técnicos:** Considerar dentro de sus especificaciones técnicas de ciberseguridad las restricciones del ciclo final de soporte y la obsolescencia para los bienes y

Pedro A. Lluberes esq. Manuel Rodríguez Objío, Gascue Santo Domingo República Dominicana
TELÉFONO: 809 682 7407 • 829 681 7407 DGCP.GOB.DO

Dirección General
Contrataciones Públicas

servicios tecnológicos que se adquieran. Contemplar la adhesión y/o certificación a normas y/o buenas prácticas adoptadas por el proveedor, a fin de garantizar la integridad y disponibilidad de la información institucional alojadas en las premisas del proveedor, resultado de la contratación de servicios. Asimismo, requerir la adhesión a buenas prácticas de desarrollo seguro para las adquisiciones de servicios y/o productos que demanden esfuerzos en este orden.

- **Evaluación del proveedor**: Realizar una debida diligencia ampliada sobre los proveedores potenciales para asegurar que cuenten con los controles y prácticas de ciberseguridad para proteger la información y los sistemas gubernamentales.

- **Consideraciones contractuales y legales:** Incluir cláusulas de acuerdos de confidencialidad en sus contratos de adquisición, para asegurar que los proveedores sean responsables de las informaciones sensibles compartidas sobre las infraestructuras tecnológicas de la institución.

- **Monitoreo continuo:** Implementar programas continuos de monitoreo y aseguramiento para garantizar que se cumplen las obligaciones de ciberseguridad durante la vida del contrato de adquisición.

Por otra parte, se informa que en el marco del referido acuerdo se tiene dentro de sus objetivos garantizar el continuo funcionamiento y seguridad del Sistema Electrónico de Compras y Contrataciones Públicas (SECCP)-Portal Transaccional, administrado por la Dirección General de Contrataciones Públicas, con la finalidad de fortalecer dicha plataforma contra las amenazas y/o ataques informáticos que pudieran presentarse. Esto implicará una serie de medidas y acciones que serán informadas oportunamente a los usuarios del sistema. En ese sentido, recordando la obligación que tienen las entidades del estado de la notificación de incidentes e intercambio de inteligencia de amenazas, según las disposiciones del Decreto núm. 685-22.

Atentamente,

MINISTERIO DE HACIENDA
DIRECCIÓN GENERAL DE CONTRATACIONES PÚBLICAS
Dirección General Contrataciones Públicas
Santo Domingo, R.D.

Lic. Carlos Pimentel Florenzán
Director General de Contrataciones Públicas (DGCP)

PRESIDENCIA DE LA
MINISTERIO DE LA PRESIDENCIA
Dirección Ejecutiva, Centro Nacional de Ciberseguridad
DOMINICANA

Cnel. Juan Gabriel Gautreaux Martínez
Director Ejecutivo del Centro Nacional de Ciberseguridad (CNCS)

Pedro A. Lluberes esq. Manuel Rodríguez Objio, Gascue Santo Domingo República Dominicana
TELÉFONO: 809 682 7407 • 829 681 7407 DGCP.GOB.DO

Dirección General Contrataciones Públicas