Biblioteca Nacional

Pedro Henríquez Ureña

Informe de Avance en la Implementación del Plan de Mejora Institucional en base al Modelo CAF

(COMMON ASSESSMENT FRAMEWORK).

COMITÉ DE CALIDAD

Santo Domingo, D.N.

Julio 2024

Introducción

La Biblioteca Nacional Pedro Henríquez Ureña, es la Biblioteca Central del Estado Dominicano y uno de los pilares del Sistema Nacional de Cultura, la misma tiene bajo su responsabilidad recopilar, preservar y facilitar la difusión del patrimonio bibliográfico del país y principalmente la obra de autores dominicanos. La BNPHU tiene por objetivo, contribuir con la creación, organización y control de manifestaciones culturales para la consolidación de la identidad y valores de los activos bibliográficos de la nación.

Nuestra organización está comprometida en las mejoras de nuestros servicios y procesos, a través de las evaluaciones continuas en la cual nos sometemos para lograr la excelencia. Elaboramos el Plan de Mejora Institucional 2024, tomando como referencia aquellas áreas de mejoras identificadas en el Autodiagnóstico CAF del año 2023, las mismas fueron efectuadas con el acompañamiento de las Analistas del Ministerio de Administración Pública (MAP) y el Comité de Calidad de la BNPHU.

Basados en lo expuesto anteriormente, presentamos a continuación las evidencias de los avances experimentados en el Plan de Mejora, acciones de mejora, nivel de logro y las evidencias hasta la fecha.

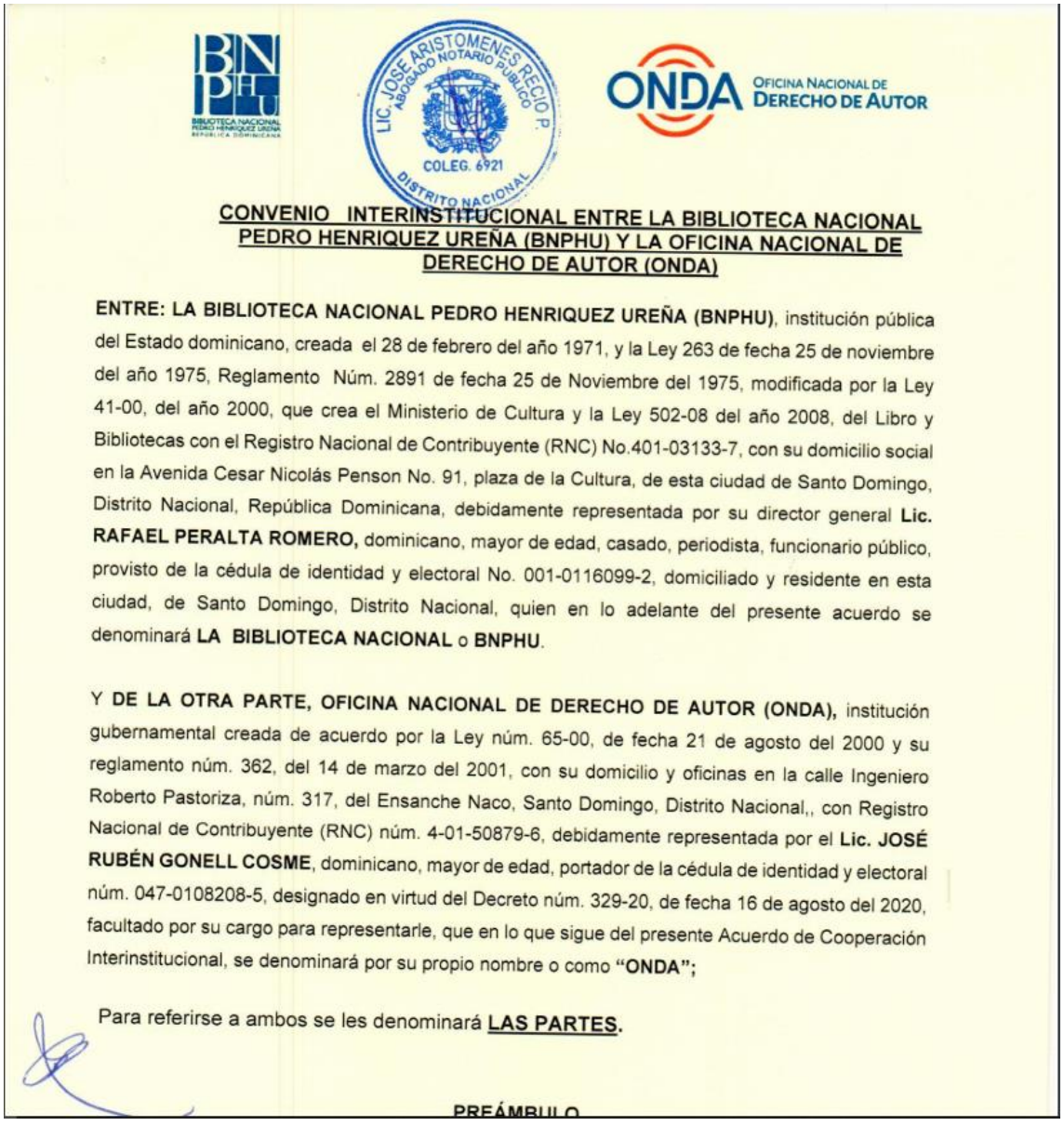
Criterio 1: Liderazgo.

Subcriterio 1.1.5 No se evidencia acuerdo interinstitucional entre la Biblioteca Nacional y la Oficina de Derecho de Autor para la difusión de los servicios afines, intercambio de información y capacitaciones.

- **Acción realizada:** La institución procedió a remitir comunicación al director general de la Oficina Nacional de Derecho de Autor para la difusión de los servicios afines. Con un nivel de cumplimiento al 100%.

- **Evidencias:**

Evidencia 1: Acuerdo firmado y sellado por las autoridades de ambas instituciones.



LIC. JOSE ARISTOMENES RECIO P. ABOGADO NOTARIO PUBLICO COLEG. 6921 DISTRITO NACIONAL

ONDA OFICINA NACIONAL DE DERECHO DE AUTOR

CONVENIO INTERINSTITUCIONAL ENTRE LA BIBLIOTECA NACIONAL PEDRO HENRIQUEZ UREÑA (BNPHU) Y LA OFICINA NACIONAL DE DERECHO DE AUTOR (ONDA)

ENTRE: LA BIBLIOTECA NACIONAL PEDRO HENRIQUEZ UREÑA (BNPHU), institución pública del Estado dominicano, creada el 28 de febrero del año 1971, y la Ley 263 de fecha 25 de noviembre del año 1975, Reglamento Núm. 2891 de fecha 25 de Noviembre del 1975, modificada por la Ley 41-00, del año 2000, que crea el Ministerio de Cultura y la Ley 502-08 del año 2008, del Libro y Bibliotecas con el Registro Nacional de Contribuyente (RNC) No.401-03133-7, con su domicilio social en la Avenida Cesar Nicolás Penson No. 91, plaza de la Cultura, de esta ciudad de Santo Domingo, Distrito Nacional, República Dominicana, debidamente representada por su director general **Lic. RAFAEL PERALTA ROMERO,** dominicano, mayor de edad, casado, periodista, funcionario público, provisto de la cédula de identidad y electoral No. 001-0116099-2, domiciliado y residente en esta ciudad, de Santo Domingo, Distrito Nacional, quien en lo adelante del presente acuerdo se denominará **LA BIBLIOTECA NACIONAL** o **BNPHU**.

Y **DE LA OTRA PARTE, OFICINA NACIONAL DE DERECHO DE AUTOR (ONDA),** institución gubernamental creada de acuerdo por la Ley núm. 65-00, de fecha 21 de agosto del 2000 y su reglamento núm. 362, del 14 de marzo del 2001, con su domicilio y oficinas en la calle Ingeniero Roberto Pastoriza, núm. 317, del Ensanche Naco, Santo Domingo, Distrito Nacional,, con Registro Nacional de Contribuyente (RNC) núm. 4-01-50879-6, debidamente representada por el **Lic. JOSÉ RUBÉN GONELL COSME**, dominicano, mayor de edad, portador de la cédula de identidad y electoral núm. 047-0108208-5, designado en virtud del Decreto núm. 329-20, de fecha 16 de agosto del 2020, facultado por su cargo para representarle, que en lo que sigue del presente Acuerdo de Cooperación Interinstitucional, se denominará por su propio nombre o como **"ONDA";**

Para referirse a ambos se les denominará **LAS PARTES.**

PREÁMBULO

CONSIDERANDO: Que la **Biblioteca Nacional** según lo establecido en la Ley 502-08 está directamente involucrada en los procesos vinculados con la gestión del conocimiento, así como también con la promoción del libro y la lectura.

CONSIDERANDO: Que la **Biblioteca Nacional** ofrece a los autores y editores la asignación del ISBN e ISSN, códigos numéricos que se asignan a libros, folletos y publicaciones seriadas, gratuitamente, con la finalidad de identificarlos como la cédula de identidad de cada documento, que permite su difusión y comercialización.

CONSIDERANDO: Que la **Biblioteca Nacional** se encarga de recibir de toda persona que publique o empresa editora de publicaciones periódicas, radicadas en el país, cualquier publicación, en la forma que se haga, o por cualquier método de reproducción que se emplee, y cualquiera que sea el tipo de publicación, incluyendo libros, folletos, programas, hojas sueltas, postales o similares, está en la obligación de enviar dos (2) ejemplares a la Biblioteca Nacional las Bibliotecas del Congreso Nacional y al Archivo General de la Nación", según lo establece la ley 418 del 11 de marzo del año 1982, que derogo la ley 112-71.

CONSIDERANDO: Que la **ONDA,** conforme a lo establecido por la Ley 65-00, de Derecho de Autor, se encarga de administrar y tutelar, todo lo relacionado con el derecho de autor y derecho conexo en la República Dominicana, así como de hacer cumplir las leyes, reglamentos y disposiciones, contribuyendo al desarrollo de una cultura de respeto y seguridad a la actividad creativa.

CONSIDERANDO: Que la **ONDA,** en los artículos 156 al 161 de la ley 65-00 sobre Derecho de Autor, establece en el artículo 157: Si la obra estuviera publicada en forma impresa, se presentaran tres (3) ejemplares a la Biblioteca Nacional, dentro de un plazo de 60 días después de la publicación.

CONSIDERANDO: Que la **ONDA,** establece textualmente en el artículo 161: *El cumplimiento de la* obligación de depósito legal, de conformidad con las normas de la ley, es requisito previo e indispensable para el registro de las obras y fonogramas que deben ser depositados. También estable el incumplimiento de la obligación del depósito legal, dará lugar al pago de una suma equivalente a diez (10) veces el valor comercial de los ejemplares que no fueren depositados.

POR TANTO Y EN EL ENTENDIDO de que el anterior preámbulo forma parte del presente acuerdo,

AMBAS PARTES HAN CONVENIDO LO SIGUIENTE:

ARTÍCULO PRIMERO: El objetivo: El presente acuerdo tiene por objeto establecer el marco general de colaboración interinstitucional entre la **BIBLIOTECA NACIONAL PEDRO HENRIQUEZ UREÑA (BNPHU) y la OFICINA NACIONAL DE DERECHO DE AUTOR (ONDA)**, a fin de regir las relaciones de cooperación entre ambas instituciones con el propósito de facilitar la realización de las gestiones y procesos relacionados al Depósito Legal, según lo establecido en los artículos 156 al 161 de la Ley 65-00 sobre Derecho de Autor.

ARTÍCULO SEGUNDO: Compromisos entre las partes: Las partes de manera conjunta en cuanto a sus ***COMPROMISOS Y OBLIGACIONES*** establecen lo siguiente:

a) La Biblioteca Nacional se compromete a entregar un documento que formará parte de este acuerdo **"Características sobre el Depósito Legal".**

b) La Biblioteca Nacional brindará asesoría técnica-metodológica para la organización y Catalogación del Centro de Documentación o biblioteca de la ONDA, siempre y cuando sea requerida.

c) La Biblioteca Nacional ofrece capacitación en materia bibliotecológica al personal del Centro de Documentación o biblioteca de la ONDA, mediante el Departamento de Capacitación en Bibliotecología (DECABI), de acuerdo con los requisitos de DECABI.

d) La ONDA se compromete a incluir en su portal de transparencia, los procedimientos de registros: entrega de tres (3) ejemplares a la Biblioteca Nacional de obras, libros, revistas, manuales, periódicos, anuarios, entre otros, en cumplimiento al depósito legal.

e) Ambas instituciones se comprometen a insertar el enlace en su portal digital, para que los ciudadanos tengan mayor facilidad de acceso a las informaciones aportadas y conocer específicamente del registro de Depósito Legal y el código ISBN-ISSN.

f) La Biblioteca Nacional, de acuerdo con la política de la institución, pone a disposición de la ONDA los espacios físicos para el uso y desarrollo de conferencias, seminarios, charlas, talleres sobre Derecho de Autor y Derechos Conexos; cuyo uso se ejecutará de acuerdo con el tarifario vigente establecido por la División de Eventos y Protocolo.

g) La ONDA y la Biblioteca Nacional organizarán, según sus respectivos intereses, conferencias, seminarios, previamente coordinados entre **LAS PARTES**.

ARTÍCULO TERCERO: Coordinación y enlace. La BIBLIOTECA NACIONAL designa a la **ENCARGADA DE LA DIVISIÓN DE DEPÓSITO LEGAL**, quien será responsable de dar el debido seguimiento al cumplimiento de lo establecido en el presente acuerdo, y de conocer y resolver los asuntos derivados de su aplicación. **La ONDA** designa a **ENCARGADA DEL CENTRO DE CAPACITACION Y DESARROLLO**, para los mismos efectos, quedando ambas partes facultadas para sustituir a sus representantes cuando lo consideren conveniente, notificándolo por escrito a la parte que corresponda.

ARTÍCULO CUARTO: Información Confidencial. A requerimiento de cualquiera de LAS PARTES, las mismas convienen no divulgar a terceros la "Información Confidencial" que reciba de la otra. Para efectos del presente CONVENIO, "Información Confidencial" comprende toda la información suministrada o divulgada por cualquiera de las partes ya sea en forma oral, visual, escrita, grabada en medios magnéticos o por cualquier otro medio.

ARTÍCULO QUINTO: Relación Laboral. Las Partes convienen en que el personal que asignen para el cumplimiento de los compromisos derivados de este convenio que a cada una corresponda, estará bajo la dependencia directa de la parte que lo hubiere contratado, y, por tanto, en ningún momento, se considerará a una u otra parte como empleador sustituto del personal contratado por su contraparte. Consiguientemente, las Partes quedan liberadas de cualquier responsabilidad que pudiera presentarse en materia de trabajo y seguridad social, derivadas de las relaciones laborales de su contraparte.

ARTÍCULO SEXTO: Solución de Controversias. En caso de presentarse cualquier divergencia en la interpretación del convenio, o en la solución de cualquier controversia que se derive del mismo, serán resueltos de común acuerdo por las Partes, haciendo constar por escrito las decisiones que se tomen.

ARTÍCULO SEPTIMO: Vigencia, duración, renovación y modificaciones. El presente acuerdo entrará en vigor a la fecha de su firma y tendrá una duración de **tres (03) años**, pudiendo terminarse en el caso de que al menos una de **las partes** comunique a la otra, por notificación oficial razonada con treinta (30) días de anticipación, su deseo de finalizarlo y sin responsabilidad para ninguna de éstas, podrá ser modificado por cualquiera de las partes, a solicitud de cualquiera de ellas, siempre en miras de procurar una mejor y más eficaz implementación del mismo; para estos fines, las partes elaborarán una solicitud por escrito que será sometida a la contraparte para obtener su aprobación

ARTÍCULO OCTAVO: LAS PARTES están exentas de toda responsabilidad por daños y perjuicios que puedan derivarse del incumplimiento total o parcial de este **convenio,** debido a caso fortuito o fuerza mayor, fuera del dominio de la voluntad de las partes y que no pueda preverse o aun en tal caso no pueda evitarse.

ARTÍCULO NOVENO: Elección de domicilio y notificaciones: Para los fines y consecuencias legales del presente acuerdo, las Partes hacen elección de domicilio en las direcciones mencionadas al inicio de éste; las notificaciones y otras comunicaciones que deban ser hechas, según este acuerdo, podrán ser enviadas por correo electrónico con acuse de recibo.

ARTÍCULO CUARTO: Información Confidencial. A requerimiento de cualquiera de LAS PARTES, las mismas convienen no divulgar a terceros la "Información Confidencial" que reciba de la otra. Para efectos del presente CONVENIO, "Información Confidencial" comprende toda la información suministrada o divulgada por cualquiera de las partes ya sea en forma oral, visual, escrita, grabada en medios magnéticos o por cualquier otro medio.

ARTÍCULO QUINTO: Relación Laboral. Las Partes convienen en que el personal que asignen para el cumplimiento de los compromisos derivados de este convenio que a cada una corresponda, estará bajo la dependencia directa de la parte que lo hubiere contratado, y, por tanto, en ningún momento, se considerará a una u otra parte como empleador sustituto del personal contratado por su contraparte. Consiguientemente, las Partes quedan liberadas de cualquier responsabilidad que pudiera presentarse en materia de trabajo y seguridad social, derivadas de las relaciones laborales de su contraparte.

ARTÍCULO SEXTO: Solución de Controversias. En caso de presentarse cualquier divergencia en la interpretación del convenio, o en la solución de cualquier controversia que se derive del mismo, serán resueltos de común acuerdo por las Partes, haciendo constar por escrito las decisiones que se tomen.

ARTÍCULO SEPTIMO: Vigencia, duración, renovación y modificaciones. El presente acuerdo entrará en vigor a la fecha de su firma y tendrá una duración de **tres (03) años**, pudiendo terminarse en el caso de que al menos una de **las partes** comunique a la otra, por notificación oficial razonada con treinta (30) días de anticipación, su deseo de finalizarlo y sin responsabilidad para ninguna de éstas, podrá ser modificado por cualquiera de las partes, a solicitud de cualquiera de ellas, siempre en miras de procurar una mejor y más eficaz implementación del mismo; para estos fines, las partes elaborarán una solicitud por escrito que será sometida a la contraparte para obtener su aprobación

ARTÍCULO OCTAVO: LAS PARTES están exentas de toda responsabilidad por daños y perjuicios que puedan derivarse del incumplimiento total o parcial de este **convenio,** debido a caso fortuito o fuerza mayor, fuera del dominio de la voluntad de las partes y que no pueda preverse o aun en tal caso no pueda evitarse.

ARTÍCULO NOVENO: Elección de domicilio y notificaciones: Para los fines y consecuencias legales del presente acuerdo, las Partes hacen elección de domicilio en las direcciones mencionadas al inicio de éste; las notificaciones y otras comunicaciones que deban ser hechas, según este acuerdo, podrán ser enviadas por correo electrónico con acuse de recibo.

ARTÍCULO DÉCIMO: Para todo lo no previsto en el presente convenio, **LAS PARTES** se remiten al derecho común.

HECHO Y FIRMADO en tres (3) originales, uno para cada una de las partes y uno para el protocolo del notario público actuante; en la ciudad de Santo Domingo, Distrito Nacional, República Dominicana, a los cuatro (04) días del mes de octubre del año dos mil veintitrés (2023)

Por. La BIBLIOTECA NACIONAL

Lic. RAFAEL PERALTA ROMERO
Director general

Por La ONDA

Lic. JOSÉ RUBEN GONELL COSME
Director general

Yo, José Aristómenes Recio P., abogado notario público de los del número para esta jurisdicción, matriculado en el Colegio Dominicano de Notarios con el número 6921, **CERTIFICO Y DOY FE** que las firmas que figuran en el presente documento fueron puestas en mi presencia, libre y voluntariamente, por los señores **LIC. RAFAEL PERALTA ROMERO** *y* **JOSÉ RUBEN GONELL COSME**, manifestándome, al mismo tiempo, dichos señores, que esas son las firmas que ellos acostumbran a usar en todos los actos de su vida pública y privada. En la ciudad de Santo Domingo, Distrito Nacional, a los cuatro (04) días del mes de octubre del año dos mil veintitrés (2023)

NOTARIO PÚBLICO

LIC. JOSE ARISTOMENES RECIO P. ABOGADO NOTARIO PUBLICO COLEG. 6921 DISTRITO NACIONAL

Evidencia 2: Acuerdo firmado y sellado por las autoridades de ambas instituciones.

Biblioteca Nacional firma acuerdo con el Centro Nacional de Ciberseguridad

MONDAY, 13 MAY 2024

Santo Domingo, D.N - La Biblioteca Nacional Pedro Henríquez Ureña (BNPHU) y el Centr...

Criterio 3: Personas.

Subcriterio: 3.3.8 Involucrar y empoderar a las personas y apoyar su bienestar. Presta atención especial a las necesidades de los empleados más desfavorecidos o con discapacidad.

- **Acción realizada:** La BNPHU, procedió a la instalación de los accesorios complementarios de apoyo y barras de seguridad en los baños a personas con discapacidad. Con un nivel de cumplimiento al 100%.

- **Evidencias:**

Evidencia 1: Habladores con el Sistema Braille, basado en seis puntos que se distribuyen de diferentes formas, cayendo dentro de lo que se considera un sistema binario para personas con discapacidad.

Baño de hombres.

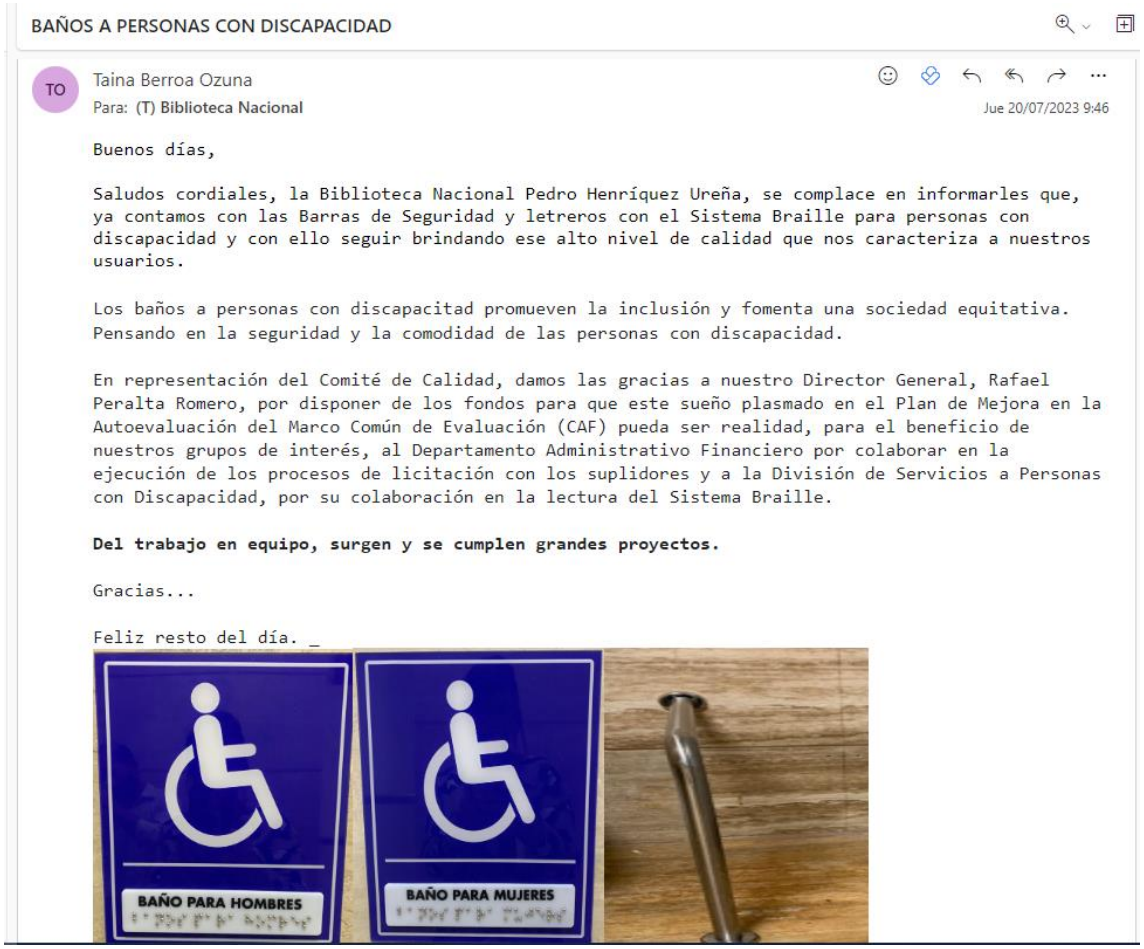
- **Evidencias 2:** Habladores para el baño de mujeres.

- **Evidencias 3:** Barras de Seguridad.

- **Evidencias 4:** Momentos de la instalación, colaborador de la Biblioteca Nacional del área de la División de Servicios a Personas con Discapacidad (DISEPEDI) y la empresa instaladora.

- **Evidencias 5:** Momentos de la instalación.

- **Evidencias 6:** Correo masivo a todo el personal, notificando la habilitación de los baños a personas con discapacidad y colaboren en su orientación.



BAÑOS A PERSONAS CON DISCAPACIDAD

TO

Taina Berroa Ozuna

Para: (T) Biblioteca Nacional

Jue 20/07/2023 9:46

Buenos días,

Saludos cordiales, la Biblioteca Nacional Pedro Henríquez Ureña, se complace en informarles que, ya contamos con las Barras de Seguridad y letreros con el Sistema Braille para personas con discapacidad y con ello seguir brindando ese alto nivel de calidad que nos caracteriza a nuestros usuarios.

Los baños a personas con discapacitad promueven la inclusión y fomenta una sociedad equitativa. Pensando en la seguridad y la comodidad de las personas con discapacidad.

En representación del Comité de Calidad, damos las gracias a nuestro Director General, Rafael Peralta Romero, por disponer de los fondos para que este sueño plasmado en el Plan de Mejora en la Autoevaluación del Marco Común de Evaluación (CAF) pueda ser realidad, para el beneficio de nuestros grupos de interés, al Departamento Administrativo Financiero por colaborar en la ejecución de los procesos de licitación con los suplidores y a la División de Servicios a Personas con Discapacidad, por su colaboración en la lectura del Sistema Braille.

Del trabajo en equipo, surgen y se cumplen grandes proyectos.

Gracias...

Feliz resto del día. _

Criterio No.4 Alianzas y Recursos

Subcriterio 4.5.6 Implementa normas o protocolos y otras medidas para la protección efectiva de la data y otras medidas para la protección efectiva de la data y la seguridad cibernética entre la provisión de datos abiertos y la protección de datos.

- **Acción realizada:** La BNPHU, procedió a impartir una charla sobre Ciberseguridad, también remite por el correo institucional masivo cápsulas sobre ciberseguridad para mantener a todos los colaboradores ante cualquier ataque cibernético, también firmamos un acuerdo con el Consejo Nacional de Ciberseguridad (CNCS). Con un nivel de cumplimiento al 100%.

- **Evidencias:**

Evidencia 1: Arte para ser usado en la convocatoria de todo el personal.

Evidencia 2: Acuerdo de Cooperación Interinstitucional BNPHU y CNCS.

CNCS CENTRO NACIONAL DE CIBERSEGURIDAD

BIBLIOTECA NACIONAL PEDRO HENRÍQUEZ UREÑA

ACUERDO DE COOPERACIÓN INTERINSTITUCIONAL ENTRE EL CENTRO NACIONAL DE CIBERSEGURIDAD (CNCS) Y LA BIBLIOTECA NACIONAL PEDRO HENRIQUEZ UREÑA (BNPHU).

ENTRE: De una parte, el **CENTRO NACIONAL DE CIBERSEGURIDAD (CNCS),** dependencia del Ministerio de la Presidencia, creado por mandato del artículo 10 del Decreto No. 230-18, de fecha 19 de junio del año 2018, que establece y regula la Estrategia Nacional de Ciberseguridad, con su domicilio ubicado en la Ave. México esq. Calle Dr. Delgado, sector Gazcue, Palacio Nacional, de esta ciudad de Santo Domingo de Guzmán, Distrito Nacional, República Dominicana; debidamente representada de conformidad con el artículo 15, literal c), del Decreto No. 230-18, de fecha 19 de junio del año 2018, por el Director Ejecutivo, General P.N. **JUAN GABRIEL GAUTREAUX MARTÍNEZ,** P.N., dominicano, mayor de edad, provisto de la Cédula de Identidad No. 001-0061362-9, de igual domicilio que la entidad, que en lo que sigue del presente Acuerdo de Cooperación Interinstitucional se denominará por su propio nombre o como **"CNCS";** y, de la otra parte **LA BIBLIOTECA NACIONAL PEDRO HENRIQUEZ UREÑA (BNPHU)**, institución pública del Estado dominicano, creada el 28 de febrero del año 1971, mediante la Ley 263 de fecha 25 de noviembre del año 1975, Reglamento Núm. 2891 de fecha 25 de Noviembre del 1975, modificada por la Ley 41-00, del año 2000, que crea el Ministerio de Cultura y la Ley 502-08 del año 2008, del Libro y Bibliotecas con el Registro Nacional de Contribuyente (RNC) No.401-03133-7, con su domicilio social en la Avenida Cesar Nicolás Penson, No. 91, plaza de la Cultura, de esta ciudad de Santo Domingo, Distrito Nacional, República Dominicana, debidamente representada por su director general **Lic. RAFAEL PERALTA ROMERO,** dominicano, mayor de edad, casado, periodista, funcionario público, provisto de la cédula de identidad y electoral No. 001-0116099-2, domiciliado y residente en esta ciudad, de Santo Domingo, Distrito Nacional, quien en lo adelante del presente acuerdo se denominará **LA BIBLIOTECA NACIONAL** o **BNPHU**.

El **CNCS** y **la BNPHU,** en lo que sigue de este Acuerdo de Cooperación Interinstitucional, serán identificados individualmente por sus respectivos nombres o como **"PARTE"** y cuando sean designadas de manera conjunta, se denominarán **"LAS PARTES"**.

PREÁMBULO:

POR CUANTO : De conformidad con lo establecido en los artículos 10 y 11 del Decreto No. 230-

la prevención, detección y gestión de incidentes generados en los sistemas de información relevantes del Estado dominicano e infraestructuras críticas nacionales.

POR CUANTO: Que mediante el Decreto núm. 313-22, de fecha 14 de junio del año 2022, Se aprueba la Estrategia Nacional de Ciberseguridad 2030, con vigencia hasta el 31 de diciembre de 2030, con el objeto de fortalecer el marco nacional de ciberseguridad, fomentando la concientización y creación de entornos digitales seguros, confiables y resilientes, que promuevan una sociedad digital dentro de un esquema de inclusión y de respeto a los derechos fundamentales.

POR CUANTO: De conformidad con el artículo 5 del referido Decreto, la Estrategia Nacional de Ciberseguridad 2030, se encuentra conformada por objetivos estratégicos, objetivos específicos y líneas de acción.

POR CUANTO: Que el **OBJETIVO ESTRATÉGICO 1**, establece: Fortalecimiento de la capacidad institucional. Fortalecer las capacidades de las entidades y organismos especializados de apoyo, para mejorar la prevención, detección, respuesta y recuperación en materia de ciberseguridad. Asimismo, contribuir al fortalecimiento de las instituciones del Estado, en todo el contexto de la ciberseguridad.

Objetivo específico 1.1: Fortalecimiento integral de las entidades y organismos especializados de apoyo en el ámbito de la gestión y seguimiento de ciberseguridad.

Línea de acción 1.1.1: Fortalecer las entidades y organismos especializados de apoyo en la gestión, seguimiento, monitoreo y evaluación de ciberseguridad, a nivel de recursos tecnológicos, financieros, humanos, entre otros.

Línea de acción 1.1.2: Fortalecer la gobernanza de las entidades y organismos especializados de apoyo y de las instituciones de investigación y persecución del ciberdelito.

Línea de acción 1.1.3: Desarrollar planes de formación, capacitación y sensibilización para funcionarios y servidores en materia de ciberseguridad.

Línea de acción 1.1.4: Crear mecanismos seguros y ágiles para reportes y denuncias de forma presencial y digital, así como también simplificar dichos trámites.

Objetivo específico 1.2: Fortalecimiento de las instituciones del Estado en materia de ciberseguridad a nivel de estructuras, formación, estándares y lineamientos para el fortalecimiento de la seguridad de la información.

Línea de acción 1.2.1: Articular la revisión de las estructuras actuales de tecnologías de la información (TI) de las instituciones del Estado para establecer una estructura independiente, enfocada en la ciberseguridad, conforme a las buenas prácticas internacionales, con fines de priorizar los pilares fundamentales de la seguridad de la información en las instituciones del Estado.

Línea de acción 1.2.2: Diseñar un plan de formación, capacitación y sensibilización en ciberseguridad para personal responsable de la seguridad de la información en las instituciones del Estado.

Línea de acción 1.2.3: Elaborar, definir y garantizar cumplimiento de los estándares para la seguridad de las Tecnologías de la Información y Comunicación (TIC) en el Estado.

POR CUANTO: Que el **OBJETIVO ESTRATÉGICO 2,** establece: Protección y resiliencia de infraestructuras. Asegurar el continuo funcionamiento de las infraestructuras críticas nacionales y las infraestructuras de tecnologías de la información (TI) del Estado.

Objetivo específico 2.1: Fortalecer la protección de las infraestructuras críticas nacionales y las de tecnologías de la información (TI) del Estado.

Línea de acción 2.1.1: Elaborar y establecer un plan nacional de respuesta a incidentes de ciberseguridad, y contingencias a riesgos, que procure la adecuada actuación en la gestión de incidentes cibernéticos, riesgos de emergencia y crisis nacional.

Línea de acción 2.1.2: Identificar y apoyar los organismos principales en el área de respuesta a incidentes que puedan proporcionar soporte a las infraestructuras críticas nacionales y a las infraestructuras tecnologías de la información (TI) del Estado y del sector privado en función al Plan Nacional de Respuesta a Incidentes de Ciberseguridad.

Línea de acción 2.1.3: Desarrollar y establecer los protocolos de activación y acción para los organismos de respuesta, y todo el ciclo de gestión de los incidentes.

Línea de acción 2.1.4: Elaborar y establecer un plan nacional de comunicación e intercambio de información ante crisis de incidentes de seguridad cibernética

Línea de acción 2.1.5: Fortalecer los Equipos Sectoriales de Respuestas a Incidentes Cibernéticos (CSIRT) y promover el establecimiento de estos en los sectores críticos nacionales.

Línea de acción 2.1.6: Diseñar, establecer y poner en marcha un plan de ejercicios de simulación de incidentes cibernéticos para las infraestructuras críticas nacionales y las instituciones del Estado.

Objetivo específico 2.2: Fortalecer la gestión de riesgos, identificar las infraestructuras críticas nacionales y las infraestructuras de tecnologías de la información (TI) relevantes del Estado y efectuar un análisis de riesgo.

Línea de acción 2.2.1: Establecer una metodología común para la gestión de los riesgos cibernéticos, y sus lineamientos, así como los mecanismos de gobernabilidad, para la supervisión, evaluación y medición periódica de implementación y cumplimiento de las políticas de tecnologías de información, los planes de riesgos y de continuidad operativa, en conformidad con las mejores prácticas, y alineada a los estándares y metodologías internacionales para las infraestructuras criticas nacionales y de las instituciones del Estado, y promover su adopción en el sector privado.

Línea de acción 2.2.2: Establecer los criterios que determinan el grado de criticidad de una infraestructura, basado en los estándares internacionales en la materia.

Línea de acción 2.2.3: Catalogar las infraestructuras críticas nacionales e infraestructuras tecnologías de la información (TI) relevantes del Estado de acuerdo con los criterios que determinan su grado de criticidad, incluyendo los servicios colaterales que las soportan.

Línea de acción 2.2.4: Efectuar análisis de riesgo sobre las infraestructuras críticas nacionales e infraestructuras tecnologías de la información (TI) relevantes del Estado y determinar su nivel de vulnerabilidad, contemplando la inclusión de los perfiles de riesgos sectoriales más críticos para la sociedad y la economía nacional.

Objetivo específico 2.3: Elaborar los reglamentos, normas, estándares y lineamientos para el fortalecimiento de la coordinación y respuesta a incidentes de ciberseguridad en las infraestructuras críticas nacionales y de tecnologías de la información (TI) del Estado.

Línea de acción 2.3.1: Evaluar las normas y reglamentaciones emitidas por reguladores sectoriales para someter propuestas de actualizaciones a estos órganos, atendiendo a estándares internacionales.

Línea de acción 2.3.2: Apoyar la elaboración y el establecimiento de reglamentos sectoriales y en el diseño del modelo de gobernanza del sector.

Línea de acción 2.3.3: Elaborar y establecer los protocolos de intercambio de información entre los Equipos Sectoriales de Respuestas a Incidentes Cibernéticos (CSIRT), las instituciones del Estado, las infraestructuras críticas y el Equipo Nacional de Respuesta a Incidentes Cibernéticos (CSIRT-RD), para la gestión de los incidentes de ciberseguridad.

POR CUANTO: Que el **OBJETIVO ESTRATÉGICO 3**, establece: Educación y cultura. Promover y fortalecer la educación, sensibilización y cultura nacional de ciberseguridad.

Objetivo específico 3.1: Fomentar la inclusión de la formación y sensibilización en ciberseguridad en todos los niveles del sistema educativo.

Línea de acción 3.1.1: Establecer una política de desarrollo de competencias digitales en la población con énfasis en la ciberseguridad, contemplando programas de educación, formación técnica, sensibilización y concientización para lograr un ciberespacio más seguro.

Línea de acción 3.1.2: Fortalecer los programas de educación en ciberseguridad de las instituciones de educación superior y técnicos, en los diferentes niveles de grado, técnico, licenciatura, maestrías y doctorado, para aumentar la disponibilidad y calidad de las ofertas académicas y profesionales especializados.

Línea de acción 3.1.3: Incorporar contenidos básicos de ciberseguridad, en las asignaturas de tecnología de información de los programas de formación de las diferentes carreras, en las instituciones de educación y técnicos superiores para fortalecer la concienciación y cultura de la ciberseguridad a nivel profesional.

Línea de acción 3.1.4: Incorporar en el programa de educación básica e intermedia, contenidos de ciberseguridad para fortalecer la sensibilización, concienciación y cultura de la ciberseguridad en los estudiantes y profesores de esos niveles.

Línea de acción 3.1.5: Diseñar un programa de cooperación para la implementación de formaciones especializadas en coordinación con las instituciones académicas.

Línea de acción 3.1.6: Implementar sistema de certificación emitida por institución acreditada para formación especializada en ciberseguridad.

Línea de acción 3.1.7: Diseñar e implementar programas de pasantías para fomentar nuevos talentos en materia de ciberseguridad con el apoyo y cooperación de las instituciones de educación intermedia, superior y técnicos profesional.

Línea de acción 3.1.8: Diseñar un programa de desarrollo de cibertalentos para apoyar la demanda de recursos especializados en el sector de la seguridad de la información.

Objetivo específico 3.2: Impulsar una cultura nacional de ciberseguridad en todo el país enfocada a las diferentes poblaciones vulnerables.

Línea de acción 3.2.1: Desarrollar un programa general de concientización para sensibilizar y fortalecer el entendimiento de ciberseguridad, conocer los riesgos, amenazas y forma de abordarlos estos temas, para niños, adolescentes, adultos mayores, MiPymes, el sector público y privado, entre otros.

Línea de acción 3.2.2: Desarrollar campañas de sensibilización, en medios tradicionales y digitales, con el apoyo del sector público, privado, la academia, organizaciones de medios y las organizaciones de la sociedad civil para fortalecer la cultura de ciberseguridad, promover la protección en línea de la información personal, y buenas prácticas en el uso de plataformas en línea y redes sociales.

Línea de acción 3.2.3: Implementar programas de reconocimiento para diversos sectores en apoyo a la cooperación en los esfuerzos de concientización y cultura de ciberseguridad a la población.

POR CUANTO: Que el **OBJETIVO ESTRATÉGICO 4**, establece: Alianzas públicas y privadas, nacionales e internacionales. Establecer alianzas nacionales e internacionales entre los sectores público y privado, sociedad civil y organismos e instituciones internacionales, para facilitar la cooperación técnica, operativa y de capacitación, así como generar los mecanismos que permitan una mejor articulación de las políticas exteriores relacionadas con la ciberseguridad.

Objetivo específico 4.1: Realizar alianzas nacionales e internacionales para fortalecer la cooperación.

Línea de acción 4.1.1: Establecer acuerdos marcos de cooperación técnica, operativa y de capacitación para el fortalecimiento de la ciberseguridad

Línea de acción 4.1.2: Fortalecer las alianzas con el sector privado, organizaciones de la sociedad civil y la academia para reafirmar la confianza ciudadana en la seguridad cibernética.

Línea de acción 4.1.3: Fomentar la relación con organismos e instituciones internacionales para facilitar la cooperación transfronteriza.

Línea de acción 4.1.4: Asegurar la participación de la República Dominicana en los foros internacionales.

Línea de acción 4.1.5: Monitorear y evaluar el nivel de cumplimiento país con los acuerdos y gobernanza del ciberespacio a nivel internacional.

POR CUANTO: Que el **OBJETIVO ESTRATÉGICO 5,** establece: Investigación y desarrollo de la ciberseguridad y su entorno. Promover el análisis, la investigación y el desarrollo de la ciberseguridad y su entorno a nivel nacional e internacional.

Objetivo específico 5.1: Fomentar la investigación, el desarrollo y la innovación de la ciberseguridad y su entorno.

Línea de acción 5.1.1: Promover programas de emprendimientos e innovaciones en la industria de ciberseguridad.
Línea de acción 5.1.2: Incentivar el análisis y las investigaciones para el fortalecimiento y desarrollo de capacidades a nivel país.

Línea de acción 5.1.3: Desarrollar estudios, y promover la generación de estadísticas y creación de indicadores para apoyar en el desarrollo de políticas públicas, basadas en evidencias, vinculado al ecosistema de ciberseguridad.

Línea de acción 5.1.4: Realizar encuestas regionales o nacionales, análisis de datos, y evaluaciones para medir el impacto de la Estrategia Nacional de Ciberseguridad 2030 en diferentes sectores.

POR EL CNCS:

JUAN GABRIEL GAUTREAUX MARTÍNEZ
General P.N.
Director Ejecutivo

POR *LA BNPHU*:

RAFAEL PERALTA ROMERO
Director General

Yo, DR. FREDDY BOLIVAR ALMONTE BRITO, Abogado, Notario Público de los del Número del Distrito Nacional, Miembro del Colegio Dominicano de Notarios, Inc., Matrícula No. 801, **CERTIFICO Y DOY FE**: que las firmas que anteceden en este documento de los señores **JUAN GABRIEL GAUTREAUX MARTÍNEZ** y **RAFAEL PERALTA ROMERO,** de generales y calidades que constan y a quienes doy fe conocer, fueron puestas libre y voluntariamente en mi presencia por dichas personas, quienes me declaran bajo la fe del juramento que son esas las firmas que acostumbran a usar en todos los actos de su vida pública y privada. En la ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, a los nueve (09) días del mes de mayo del año dos mil veinticuatro (2024).

FREDDY BOLIVAR ALMONTE BRITO
ABOGADO NOTARIO PÚBLICO
COLEGIATURA 801
SANTO DOMINGO, R.D.

NOTARIO PÚBLICO

Evidencia 3: Correo de convocatoria a todo el personal de la Biblioteca Nacional.

Evidencia 4: Cápsulas de Seguridad.

Cápsulas de Seguridad Informática.

Cápsulas de Seguridad Informática: Contraseñas

Jesús Carlos Peralta
Para: (T) Biblioteca Nacional
Mié 26/07/2023 8:00

Siempre crea y utilice contraseñas seguras de ocho o más caracteres, que contengan números, letras minúsculas, mayúsculas y símbolos. ¡Y recuerda que nunca debes compartirla!

Cápsulas de Seguridad Informática: ¡No pase por alto los materiales impresos!

JP Jesús Carlos Peralta
Para: (T) Biblioteca Nacional

Mié 19/07/2023 8:23

Protección y destrucción de datos

No pase por alto los materiales impresos

Los documentos impresos y los archivos físicos pueden contener tanta información sensible como los archivos electrónicos.

Sea tan cuidadoso con los materiales impresos como con los dispositivos electrónicos a la hora de compartir, almacenar y eliminar datos.

Jesús Peralta
Soporte Técnico/Responsable de Seguridad Informática
Tel.: (829) 946-2674 Ex.: 2497.
jperalta@bnphu.gob.do
http://www.bnphu.gob.do
Biblioteca Nacional Pedro Henríquez Ureña
C/ César Nicolás Penson #91 Santo Domingo, D.N.

Cápsulas de Seguridad Informática: Phishing

JP **Jesús Carlos Peralta**
Para: (T) Biblioteca Nacional
Mié 02/08/2023 10:04

El **phishing** es una de las técnicas más comunes utilizadas por los cibercriminales, donde intentan robar datos privados y datos bancarios de los usuarios.

Algunos consejos para que evites ser víctima de **Phishing**:

Nunca hagas clic en un enlace que esté en un correo electrónico de una supuesta entidad bancaria o empresa.

Verifica la dirección de correo electrónico del remitente.

Introduce únicamente tus datos confidenciales **en páginas web que sean seguras**.

Si tienes dudas, **contacta directamente** con el Departamento de TIC de la **BNPHU.**

Jesús Peralta
Soporte Técnico/Responsable de Seguridad Informática
Tel.: (829) 946-2674 Ex.: 2497.
jperalta@bnphu.gob.do
http://www.bnphu.gob.do
Biblioteca Nacional Pedro Henríquez Ureña
C/ César Nicolás Penson #91 Santo Domingo, D.N.

Cápsulas de Seguridad Informática: Prevé el Ciberacoso en Niños y Adolescentes.

JP **Jesús Carlos Peralta**
Para: (T) Biblioteca Nacional
Mié 09/08/2023 8:50

Manténgase atento a los cambios en el comportamiento; si su hijo **evita** repentinamente el uso de la computadora, tablet o celular, **puede ser una señal de que esté siendo acosado en línea.**

Si usted o sus hijos **han sido víctimas de un delito en línea**, **repórtelo** al **Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT) de la Policía Nacional.**
Correo electrónico: info@dicat.gob.do

Jesús Peralta
Soporte Técnico/Responsable de Seguridad Informática
Tel.: (829) 946-2674 Ex.: 2497.
jperalta@bnphu.gob.do
http://www.bnphu.gob.do
Biblioteca Nacional Pedro Henríquez Ureña
C/ César Nicolás Penson #91 Santo Domingo, D.N.

Cápsulas de Seguridad Informática: Dispositivos extraíbles

JP **Jesús Carlos Peralta**
Para: (T) Biblioteca Nacional
Mié 20/09/2023 9:41

¡Protegiendo Nuestra Biblioteca, Protegiendo Nuestra Información!

Estimados colegas de la **Biblioteca Nacional Pedro Henríquez Ureña**,

Quiero aprovechar esta oportunidad para abordar un tema crucial que **afecta a la seguridad informática de nuestra institución**: los peligros asociados con el uso de dispositivos de almacenamiento extraíbles, **como memorias USB, discos duros externos y tarjetas SD.**

La seguridad de los datos y la información que manejamos en nuestra biblioteca es de suma importancia, y es responsabilidad de todos nosotros contribuir a mantenerla protegida. **Los dispositivos de almacenamiento extraíbles pueden ser una puerta de entrada para amenazas cibernéticas y pérdida de datos si no se utilizan de manera adecuada.**

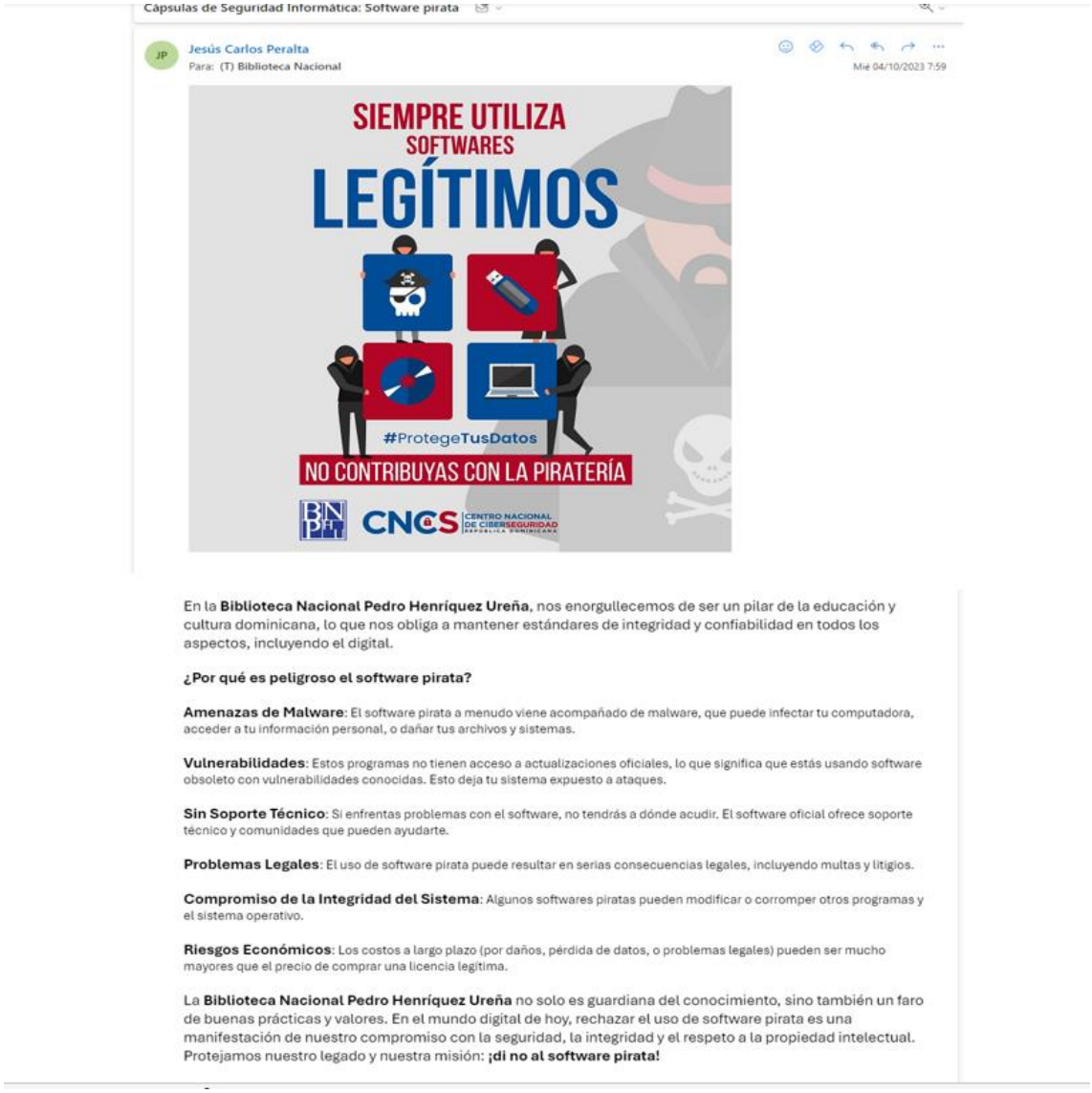
A continuación, quiero destacar algunos de los riesgos más comunes asociados con el uso de estos dispositivos y cómo podemos mitigarlos:

1. **Malware y Virus:** Los dispositivos extraíbles pueden ser portadores de malware y virus. Es importante asegurarse de que cualquier dispositivo que se conecte a nuestras redes o sistemas sea escaneado en busca de amenazas antes de su uso.

2. **Pérdida de Datos:** La pérdida de un dispositivo extraíble puede resultar en la exposición de información confidencial. Evite almacenar información sensible en dispositivos de este tipo y, si es necesario, cifre los datos para protegerlos.

3. **Acceso No Autorizado:** El uso no autorizado de dispositivos extraíbles puede dar lugar a fugas de información.

Jesús Peralta
Soporte Técnico/Responsable de Seguridad Informática
Tel.: (829) 946-2674 Ex.: 2497.
jperalta@bnphu.gob.do
http://www.bnphu.gob.do
Biblioteca Nacional Pedro Henríquez Ureña
C/ César Nicolás Penson #91 Santo Domingo, D.N.



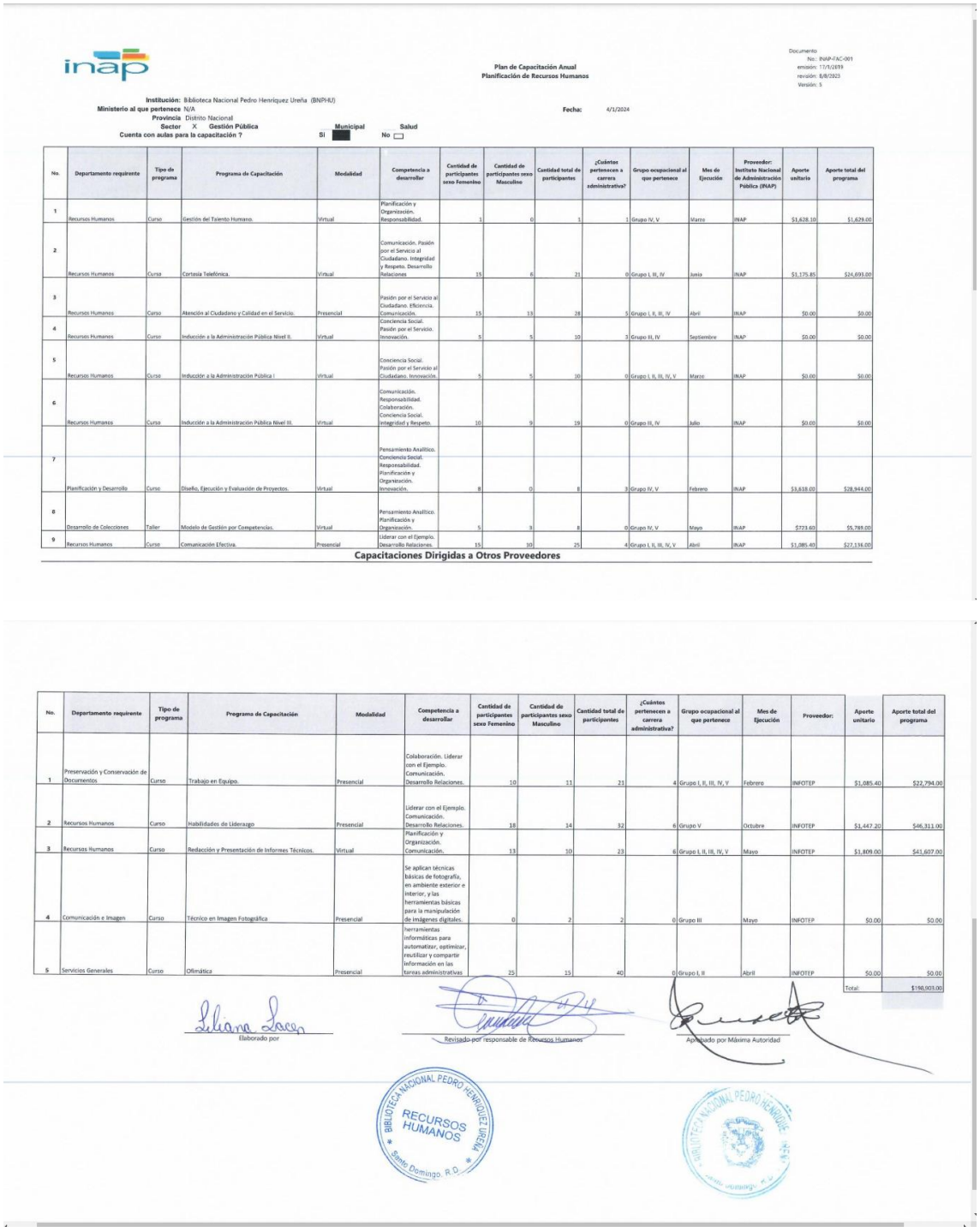
Criterio 3: Personas.

Subcriterio 3.1.6 Aplica una política de género como apoyo a la gestión eficaz de los recursos humanos de la organización, hombres, mujeres, participación en programas de formación y/o actividades institucionales.

- **Acción realizada:** La institución procedió a elaborar un programa de formación para garantizar la participación de los colaboradores. Con un nivel de cumplimiento al 100%.

- **Evidencias:**

Evidencia 1: Programa de Capacitación.



inap

Documento
No.: INAP-FAC-001
emisión: 17/1/2019
revisión: 8/8/2023
Versión: 5

Plan de Capacitación Anual
Planificación de Recursos Humanos

Institución: Biblioteca Nacional Pedro Henríquez Ureña (BNPHU)
Ministerio al que pertenece N/A
Provincia Distrito Nacional
Sector X **Gestión Pública** **Municipal** **Salud**
Cuenta con aulas para la capacitación ? **SI** [redacted] **No**

Fecha: 4/1/2024

No.	Departamento requirente	Tipo de programa	Programa de Capacitación	Modalidad	Competencia a desarrollar	Cantidad de participantes sexo Femenino	Cantidad de participantes sexo Masculino	Cantidad total de participantes	¿Cuántos pertenecen a carrera administrativa?	Grupo ocupacional al que pertenece	Mes de Ejecución	Proveedor: Instituto Nacional de Administración Pública (INAP)	Aporte unitario	Aporte total del programa
1	Recursos Humanos	Curso	Gestión del Talento Humano.	Virtual	Planificación y Organización. Responsabilidad.	1	0	1	1	Grupo IV, V	Marzo	INAP	$1,628.10	$1,629.00
2	Recursos Humanos	Curso	Cortesía Telefónica.	Virtual	Comunicación. Pasión por el Servicio al Ciudadano. Integridad y Respeto. Desarrollo Relaciones	15	6	21	0	Grupo I, III, IV	Junio	INAP	$1,175.85	$24,693.00
3	Recursos Humanos	Curso	Atención al Ciudadano y Calidad en el Servicio.	Presencial	Pasión por el Servicio al Ciudadano. Eficiencia. Comunicación.	15	13	28	5	Grupo I, II, III, IV	Abril	INAP	$0.00	$0.00
4	Recursos Humanos	Curso	Inducción a la Administración Pública Nivel II.	Virtual	Conciencia Social. Pasión por el Servicio. Innovación.	5	5	10	3	Grupo III, IV	Septiembre	INAP	$0.00	$0.00
5	Recursos Humanos	Curso	Inducción a la Administración Pública I	Virtual	Conciencia Social. Pasión por el Servicio al Ciudadano. Innovación.	5	5	10	0	Grupo I, II, III, IV, V	Marzo	INAP	$0.00	$0.00
6	Recursos Humanos	Curso	Inducción a la Administración Pública Nivel III.	Virtual	Comunicación. Responsabilidad. Colaboración. Conciencia Social. Integridad y Respeto.	10	9	19	0	Grupo III, IV	Julio	INAP	$0.00	$0.00
7	Planificación y Desarrollo	Curso	Diseño, Ejecución y Evaluación de Proyectos.	Virtual	Pensamiento Analítico. Conciencia Social. Responsabilidad. Planificación y Organización. Innovación.	8	0	8	3	Grupo IV, V	Febrero	INAP	$3,618.00	$28,944.00
8	Desarrollo de Colecciones	Taller	Modelo de Gestión por Competencias.	Virtual	Pensamiento Analítico. Planificación y Organización.	5	3	8	0	Grupo IV, V	Mayo	INAP	$723.60	$5,789.00
9	Recursos Humanos	Curso	Comunicación Efectiva.	Presencial	Liderar con el Ejemplo. Desarrollo Relaciones.	15	10	25	4	Grupo I, II, III, IV, V	Abril	INAP	$1,085.40	$27,136.00

Capacitaciones Dirigidas a Otros Proveedores

No.	Departamento requirente	Tipo de programa	Programa de Capacitación	Modalidad	Competencia a desarrollar	Cantidad de participantes sexo Femenino	Cantidad de participantes sexo Masculino	Cantidad total de participantes	¿Cuántos pertenecen a carrera administrativa?	Grupo ocupacional al que pertenece	Mes de Ejecución	Proveedor:	Aporte unitario	Aporte total del programa
1	Preservación y Conservación de Documentos	Curso	Trabajo en Equipo.	Presencial	Colaboración. Liderar con el Ejemplo. Comunicación. Desarrollo Relaciones.	10	11	21	4	Grupo I, II, III, IV, V	Febrero	INFOTEP	$1,085.40	$22,794.00
2	Recursos Humanos	Curso	Habilidades de Liderazgo	Presencial	Liderar con el Ejemplo. Comunicación. Desarrollo Relaciones.	18	14	32	6	Grupo V	Octubre	INFOTEP	$1,447.20	$46,311.00
3	Recursos Humanos	Curso	Redacción y Presentación de Informes Técnicos.	Virtual	Planificación y Organización. Comunicación.	13	10	23	6	Grupo I, II, III, IV, V	Mayo	INFOTEP	$1,809.00	$41,607.00
4	Comunicación e Imagen	Curso	Técnico en Imagen Fotográfica	Presencial	Se aplican técnicas básicas de fotografía, en ambiente exterior e interior, y las herramientas básicas para la manipulación de imágenes digitales.	0	2	2	0	Grupo III	Mayo	INFOTEP	$0.00	$0.00
5	Servicios Generales	Curso	Ofimática	Presencial	herramientas informáticas para automatizar, optimizar, reutilizar y compartir información en las tareas administrativas	25	15	40	0	Grupo I, II	Abril	INFOTEP	$0.00	$0.00
													Total:	$190,903.00

Liliana Lares
Elaborado por

Revisado por responsable de Recursos Humanos

Aprobado por Máxima Autoridad

BIBLIOTECA NACIONAL PEDRO HENRÍQUEZ UREÑA
RECURSOS HUMANOS
Santo Domingo, R.D.

BIBLIOTECA NACIONAL PEDRO HENRÍQUEZ UREÑA
Santo Domingo, R.D.

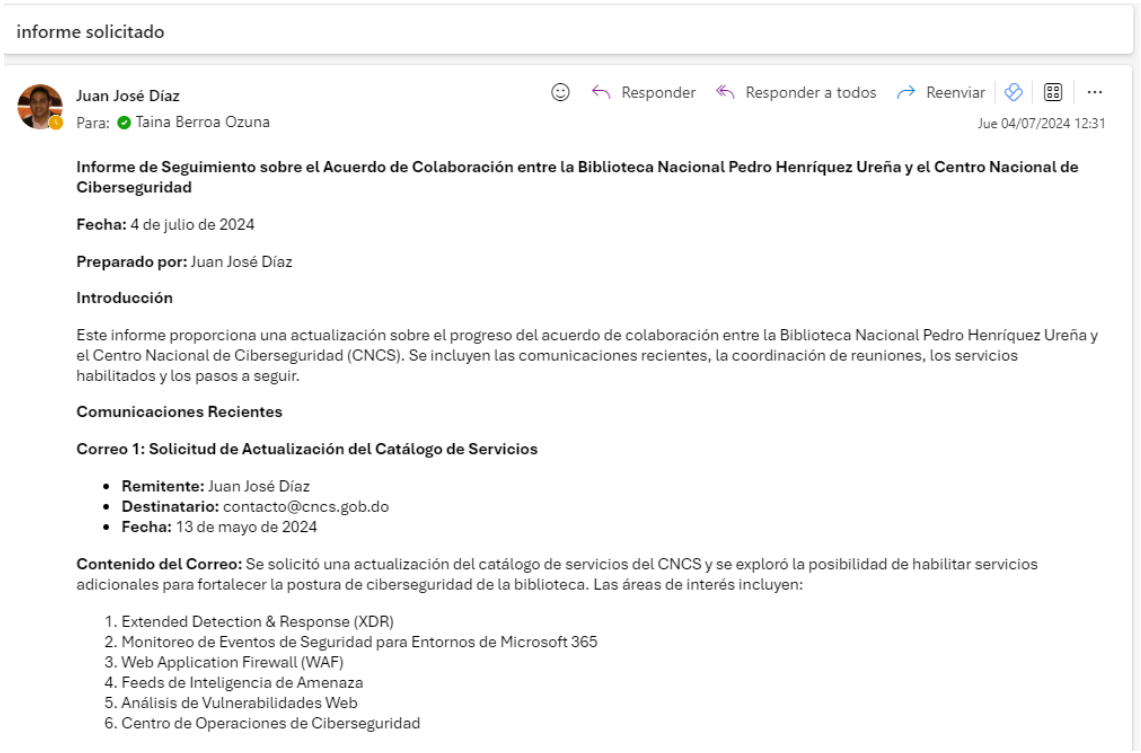
Criterio 3: Personas.

Subcriterio 4.1.2 No se evidencia informes de seguimiento ni asignación de responsables para los acuerdos y/o convenios interinstitucionales

- **Acción realizada:** La institución procedió a llevar el control de los acuerdos y/o convenios a través de los informes. Con un nivel de cumplimiento al 100%.

- **Evidencias:**

Evidencia 1: Informe de seguimiento acuerdos y/o alianzas.



informe solicitado

Juan José Díaz
Para: Taina Berroa Ozuna

Responder | Responder a todos | Reenviar | ···

Jue 04/07/2024 12:31

Informe de Seguimiento sobre el Acuerdo de Colaboración entre la Biblioteca Nacional Pedro Henríquez Ureña y el Centro Nacional de Ciberseguridad

Fecha: 4 de julio de 2024

Preparado por: Juan José Díaz

Introducción

Este informe proporciona una actualización sobre el progreso del acuerdo de colaboración entre la Biblioteca Nacional Pedro Henríquez Ureña y el Centro Nacional de Ciberseguridad (CNCS). Se incluyen las comunicaciones recientes, la coordinación de reuniones, los servicios habilitados y los pasos a seguir.

Comunicaciones Recientes

Correo 1: Solicitud de Actualización del Catálogo de Servicios

- **Remitente:** Juan José Díaz
- **Destinatario:** contacto@cncs.gob.do
- **Fecha:** 13 de mayo de 2024

Contenido del Correo: Se solicitó una actualización del catálogo de servicios del CNCS y se exploró la posibilidad de habilitar servicios adicionales para fortalecer la postura de ciberseguridad de la biblioteca. Las áreas de interés incluyen:

1. Extended Detection & Response (XDR)
2. Monitoreo de Eventos de Seguridad para Entornos de Microsoft 365
3. Web Application Firewall (WAF)
4. Feeds de Inteligencia de Amenaza
5. Análisis de Vulnerabilidades Web
6. Centro de Operaciones de Ciberseguridad

Correo 2: Respuesta del CNCS y Coordinación de Reunión

- **Remitente:** Karla Yofraciel Aquino Merán (CNCS)
- **Destinatario:** Juan José Díaz, contacto@cncs.gob.do
- **Fecha:** 15 de mayo de 2024

Contenido del Correo: El CNCS agradeció el interés en sus servicios y propuso agendar una sesión el jueves 16 de mayo a las 9:00 AM para presentar el catálogo de servicios y discutir las necesidades de la biblioteca.

Confirmación de Reunión:

- **Remitente:** Juan José Díaz
- **Destinatario:** Karla Yofraciel Aquino Merán, contacto@cncs.gob.do
- **Fecha:** 15 de mayo de 2024

Contenido del Correo: Se confirmó la disponibilidad para la reunión propuesta a las 9:00 AM del jueves 16 de mayo.

Progreso Actual

Reunión de Presentación y Servicios Habilitados:

- **Fecha de la Reunión:** 16 de mayo de 2024
- **Participantes:** Juan José Díaz, Karla Yofraciel Aquino Merán, y otros representantes del CNCS.
- Durante la reunión, se habilitaron los siguientes servicios:
    1. **Extended Detection & Response (XDR):** Monitoreo del XDR SOPHOS.
    2. **Monitoreo de Eventos de Seguridad para Entornos de Microsoft 365.**
    3. **Análisis de Vulnerabilidades Web.**
    4. **Centro de Operaciones de Ciberseguridad.**
    5. **Web Application Firewall (WAF):** Se inició el proceso de implementación para los servicios en línea.

Próximos Pasos

1. **Monitoreo y Evaluación:**
    - Supervisar la eficacia de los servicios habilitados, especialmente el XDR y el monitoreo de eventos de seguridad.
    - Realizar evaluaciones periódicas del análisis de vulnerabilidades web y los reportes del Centro de Operaciones de Ciberseguridad.
2. **Implementación del WAF:**
    - Continuar con el proceso de implementación del Web Application Firewall (WAF).
    - Coordinar con el CNCS para asegurar una configuración óptima y pruebas exhaustivas.
3. **Reuniones de Seguimiento:**
    - Programar reuniones periódicas con el CNCS para discutir el progreso y resolver cualquier problema que surja durante la implementación y operación de los servicios.
    - Revisar y ajustar los servicios habilitados según sea necesario para mejorar la seguridad cibernética.
4. **Planificación de Futuras Colaboraciones:**
    - Explorar nuevas oportunidades de colaboración con el CNCS para fortalecer aún más la ciberseguridad de la biblioteca.

Conclusión

La colaboración con el Centro Nacional de Ciberseguridad ha permitido la habilitación de varios servicios cruciales para la ciberseguridad de la Biblioteca Nacional Pedro Henríquez Ureña. Continuaremos supervisando y evaluando estos servicios para asegurar que nuestra infraestructura digital se mantenga segura y protegida.

Atentamente, Juan José Díaz
Encargado del Departamento de Tecnologías de la Información y Comunicación
Biblioteca Nacional Pedro Henríquez Ureña

Lic. Juan José Díaz Nerio MIS
Encargado Departamento de TIC
Tel.: (829) 946-2674 Ex.: 2494
Flota: 829-568-2231/Cel: 809-431-0050
Biblioteca Nacional Pedro Henríquez Ureña
C/ César Nicolás Penson #91 Santo Domingo, D.N.

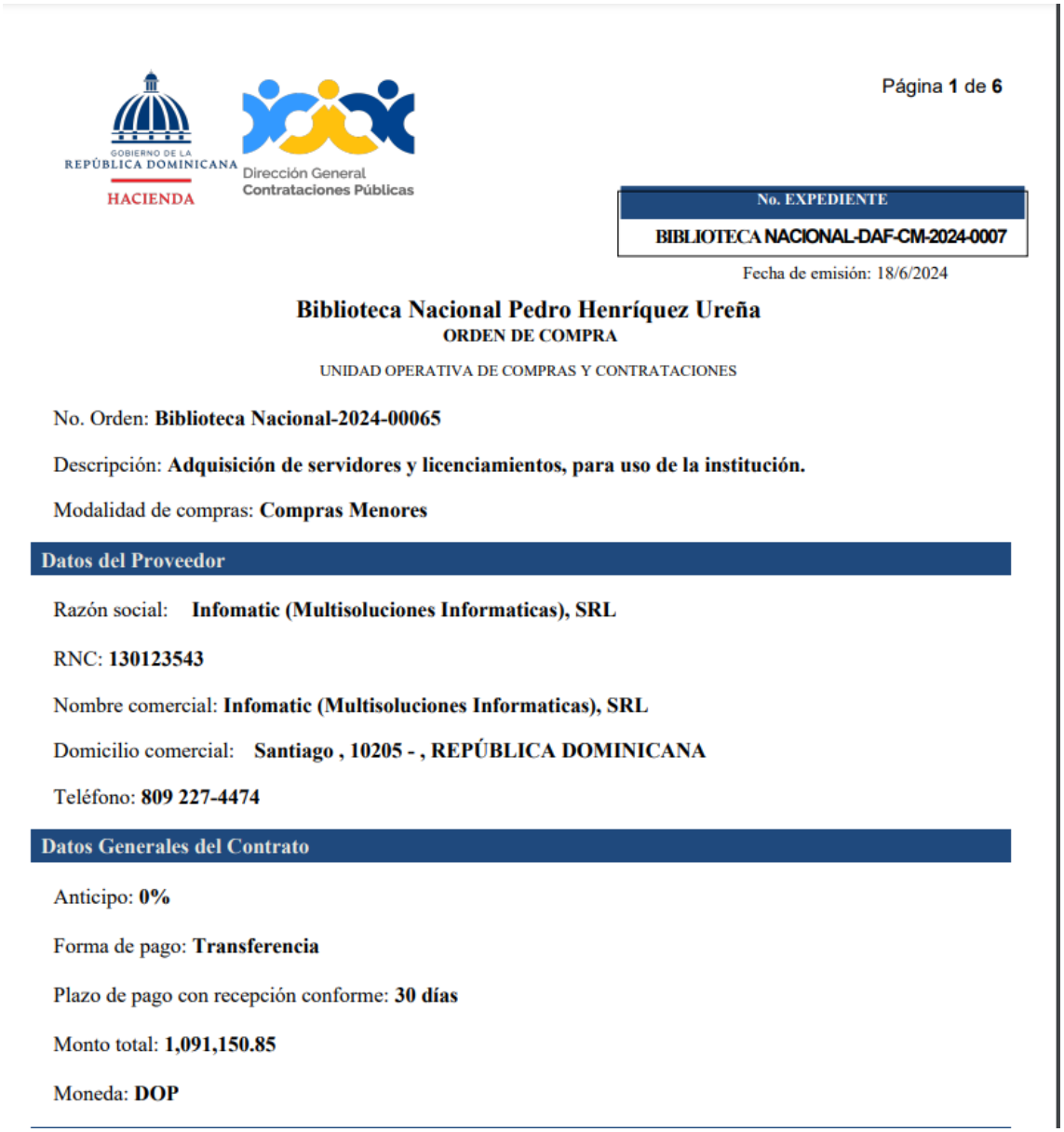
Criterio 4: Alianzas y Recursos.

Subcriterio 4.5.5 No se evidencia renovación de la infraestructura tecnológica.

- **Acción realizada:** La institución procedió a comprar un servidor para el buen funcionamiento del Departamento de Tecnología y garantizar la continuidad de los servicios operacionales y los servicios de nuestros grupos de interés tanto interno como externos. Con un nivel de cumplimiento al 100%.

- **Evidencias:**

Evidencia 1: Adquisición de servidores y licenciamientos para uso de la institución.



GOBIERNO DE LA REPÚBLICA DOMINICANA
HACIENDA

Dirección General Contrataciones Públicas

Página **1** de **6**

No. EXPEDIENTE
BIBLIOTECA NACIONAL-DAF-CM-2024-0007

Fecha de emisión: 18/6/2024

Biblioteca Nacional Pedro Henríquez Ureña
ORDEN DE COMPRA

UNIDAD OPERATIVA DE COMPRAS Y CONTRATACIONES

No. Orden: **Biblioteca Nacional-2024-00065**

Descripción: **Adquisición de servidores y licenciamientos, para uso de la institución.**

Modalidad de compras: **Compras Menores**

Datos del Proveedor

Razón social: **Infomatic (Multisoluciones Informaticas), SRL**

RNC: **130123543**

Nombre comercial: **Infomatic (Multisoluciones Informaticas), SRL**

Domicilio comercial: **Santiago , 10205 - , REPÚBLICA DOMINICANA**

Teléfono: **809 227-4474**

Datos Generales del Contrato

Anticipo: **0%**

Forma de pago: **Transferencia**

Plazo de pago con recepción conforme: **30 días**

Monto total: **1,091,150.85**

Moneda: **DOP**

Item	Código	Descripción	Cantidad	Unidad	Precio Unit s/ITBIS	Imp Moneda Orig s/ITBIS	% Descuento	ITBIS Moneda Orig	Otros Impuestos Moneda Orig	Sub Total Moneda Orig
1	43211501	Servidor HP Proliant DI 180 G10, para virtualización. Rackmount, 2 procesadores de 12 core C/U mínimo, 256 GB RAM, 2 x 960 GB HD 10K SAS, tarjeta de fibra óptica 16 GB 2p FC HBA, tarjeta 1 Ethernet de 4 puertos 1 GB, Tarjeta Ethernet 2 puertos 10 GB, cables, power supply redundante. 3 años de garantía, soporte 24/7 y servicio de instalación. La solución debe estar respaldada por un motor de anpalisis y monitoreo, habilitado en la nube con las siguientes capacidades: 1. Recomendaciones de actualización de firmware y actualización de parches de manera proactiva. 2. Análisis de tendencias de rendimiento y capacidad histórica por minuto extremadamente granular de forma	1.00	UD	615,895.70	615,895.70		110,861.23	0.00	726,756.93

Item	Código	Descripción	Cantidad	Unidad	Precio Unit s/ITBIS	Imp Moneda Orig s/ITBIS	% Descuento	ITBIS Moneda Orig	Otros Impuestos Moneda Orig	Sub Total Moneda Orig
		de habilitar un registro adicional, instalar ningún dispositivo (físico o virtual) o instalar ningún software. 3. Capacidad de aprendizaje automático (machine learning) y análisis proactivo de datos para prevenir y evitar problemas en los servidores. 4. Capacidad de recopilar ininterrumpidamente parámetros del sistema y datos de telemetría de diagnóstico de la base instalada del fabricante de manera que pueda ofrecer recomendaciones para resolver problemas y mejorar el rendimiento. 5. Capacidad de visualización de históricos de mínimo 6 meses. 6. El motor de análisis ofrecido debe estar respaldado por una base instalada de recolección global que supere los 1,200 trillones de Data Points. 7. Los equipos deben								