SECOND ADDENDUM TO NOTICE OF NEED FOR PROFESSIONAL SERVICES

seeking

PROFESSIONAL SERVICES AND IT-SOLUTION IN CONNECTION WITH THE PUERTO RICO UCC COMMERCIAL TRANSACTIONS REGISTRY

for

GOVERNMENT OF PUERTO RICO

DEPARTMENT OF STATE

NPS Issuance Date: February 8, 2023
First Addendum Issuance Date: February 27, 2023
Second Addendum Issuance Date: March 15, 2023
Proposal Submission Deadline: March 21, 2023

www.estado.pr.gov

SECOND ADDENDUM TO

NOTICE OF NEED FOR PROFESSIONAL SERVICES

On February 8th, 2023, the Puerto Rico Department of State (hereinafter, the "Department") issued a Notice of Need for Professional Services ("NPS"), seeking to acquire an IT-solution for providing registry services for financing statements. Thereafter, on February 27, 2023, the Department issued a First Addendum to the NPS (the "First Addendum") to clarify questions regarding the NPS that were received via email as of February 22, 2023.The Department issues this Second Addendum to the NPS (the "Second Addendum") to address further questions submitted between February 23, 2023, until March 1, 2023.

Please note the Department reserves the right to answer the questions it deems pertinent to the NPS. All defined terms shall have the same meaning as those provided under the NPS. In the event there is a discrepancy between any provision of the NPS and the answers provided in this Second Addendum, the NPS shall prevail.

****

[THIS SPACE WAS INTENTIONALLY LEFT BLANK]

****

1. Can you elaborate on the scope of the Accounting System? Does it refer to an end-to-end solution that includes accounts payable, billings, accounts receivable, fixed assets, inventory, financial reporting, etc.? Is it only to cover processing and reporting of fee-based transactions, payment processing and the abilityto make the transactions available to a centralized accounting system?

Answer: The IT Solution should include an accounting system that allows users to submit payments, including a reporting module that details all transactions performed on the IT solution (i.e. UCC filings, report requests, certificate copies, among others).

2. Will GPR provide the necessary hardware to scan and digitize existing documents? Based on the volume, specialized high-volume scanners may be required.

Answer: No. All transactions are submitted online by the users through the IT solution platform.

3. Beyond usual payment options such as Paypal or Credit Cards, does GPR require acceptanceof local ATH Network payments?

Answer: No.

4. In case GPR requires ATH Móvil integration, will GPR get into direct contracting of the service? Proponent will integrate the contracted service.

Answer: No. The Department does not require "ATH Móvil" integration.

5. Will GPR provide the stress test tool and required licenses for usage and execution? (Section L, Item B)

Answer: No.

6. Integrate an accounting system built into the IT solution to accommodate the registry. Is this a full accounting system or an accounting module that includes reports associated with financial transactions? (Section A, point 2 of the NPS).

Answer: The IT solution should include an accounting system that allows users to submit payments, include reporting module of all financial transactions performed on the IT Solution.

7. We are assuming that operating hours for help desk will be Monday to Friday 8:00 AM to 5:00 PM AST. Is this correct? (Section B, 2)

Answer: Yes.

8. Please indicate the total number of internal users requested to access the proposed solution. Does this number include applicable IT staff?

Answer: The Department will need to be able to have internal user accounts (administrator accounts) as needed. It is estimated that a total of ten internal users should be sufficient at the moment.

9. Please identify all record types which require public access.

Answer: All UCC financing statements and supporting documentation shall be available to registered users through the IT solution.

10. Please indicate the total amount of vendor-hosted storage needed.

Answer: Please note that the Department will be in charge of providing the hosted storage needed for the IT Solution.

11. What is the approximate number of transactions added annually?

Answer: The approximate number of transactions added annually across all UCC forms (i.e. UCC-1, UCC-3, UCC-11, among others) is 25,000. However, the transactions will fluctuate annually.

12. Please provide additional details on which systems integrations are being requested. Is this anticipated to be accomplished utilizing your own resources, or do you require a 3rd party to create integrations?

Answer: The IT solution that is to be proposed is a new platform. No integration is anticipated at this time. However, please note that we foresee that migration of the current database will be needed.

13. Is there an expected start date and duration of the implementation?

Answer: The timeline in which the proponent intends to develop the IT Solution will be evaluated in conjunction with the proposal. Please note that the Department needs to obtain the shortest timeline possible, and in no event more than six (6) months.

14. When is your desired "go-live" date?

Answer: Please refer to the answer included in question No. 13. The Department intends to have an IT Solution that can "go live" in six (6) months or less.

15. Is the Department willing to sign an NDA to gain access to security-related documents, including a Security White Paper, prior to submission of Proponent response? If so, please advise the method by which to submit an NDA for review.

Answer: No. The Department may be able to engage in NDA discussions once the proponent has been selected.

16. Can you describe the challenges of your current process (e.g. matter creation, templating, reporting)? Of these challenges, which are your top three (3) most important to solve?

Answer: Currently, the Department's main challenges are the following: (i) obtain more detailed reports including transaction statistics, among others; (ii) recognize the expiration dates and/or continuations, as applicable, of the UCC financing statements in accordance with the law and regulations, to perform the corresponding actions (i.e. eliminate an expired UCC and/or approve the continuation of a UCC; and (iii) provide user-friendly data search and delivery of reports as well as certified copies.

17. Have you seen demos of any product(s)? If so, can you please share which product(s)?

Answer: No. For any demos please refer to the current platform, which is available at: https://www.statedepartment.pr.gov/commercial-transactions.

18. Can you please provide a copy of the relevant GPR and Puerto Rico Innovation & Technology Service's IT policies as referenced in Section A. Scope of Work?

Answer: Please refer to PRITS' IT policy guidelines titled: "Estándares para la seguridad cibernética" in Spanish, attached hereto as Annex A. In addition, refer to the "Proposal Evaluation Guidelines" issued by PRITS attached hereto as Annex B.

19. Section A Scope of work references, "Integrate an accounting system built into the IT solution to accommodate the registry." Please provide additional details on the accounting system.

Answer: The system must be able to process payments for transactions submitted through the IT solution.

20. Section A Scope of Work references, "IT solution should be hosted in a cloud-based system service provided by GPR to comply with PRITS regulations." Please clarify what is meant by "provided by GPR."

Answer: The IT solution will be hosted on a cloud-based system owned and to be provided by GPR.

21. Section A Scope of Work references, "Support should allow phone calls, ticketing service, and resources on our main office in the Department at San Juan, P.R." What is envisioned by support on the main office in the Department? Are remote support resources needed, or are support resources needed on-site?

Answer: Both will be considered. Please provided your proposed workplan.

22. Section A Scope of Work references, "Ability to share data with other state agencies." Please provide additional details on the other agencies and any identify any systems the other agencies are using to share data.

Answer: The Department periodically receives requests of information (RFIs) which are to be responded to with information contained in the Registry. Therefore, an easy-to-use reporting method would benefit the Department in sharing the information as needed.

23. Section A Scope of Work references the proposed solution being able to handle the current and future UCC forms. Please provide copies of the referenced UCC forms.

Answer: The current UCC forms can be accessed at: https://www.statedepartment.pr.gov/commercial-transactions

24. Section B. General SOW references electronic payment processing. Please provide additional details on what level of electronic payment processing is envisioned.

Answer: The electronic payment envisioned is Paypal. Credit cards may also be considered.

25. Section B. General SOW references Proponents adjusting their Proposal to what is already established in the Registry laws and regulations. Please provide additional details on Registry laws and regulations. Is the DOS willing to accept legal exceptions/assumptions/conditions as part of a proposal?

Answer: The Department is the administrator of the Registry pursuant to Act. No. 208-1995, as amended. Please refer to the aforementioned act for more details.

26. Section C. IT Practices, Data Security, and Integrity references the Proponent shall manage and maintain the virtual infrastructure. Please provide additional clarification as to what is requested by "manage and maintain."

Answer: The selected proponent shall provide administration and maintenance support to the IT solution (i.e. updates, servers, backup, Firewall, etc.).

27. Section I. Cybersecurity Plan - Does the Department have an IT compliance policy available for review?

Answer: Please refer to PRITS' IT policy guidelines titled: "Estándares para la seguridad cibernética" in Spanish, attached hereto as Annex A. In addition, refer to the "Proposal Evaluation Guidelines" issued by PRITS attached hereto as Annex B.

28. Section L. Systems Performance, Availability and Reliability - Since DOS is requesting a SaaS-type model, can we assume that the terms and SLAs can be further discussed and negotiated during contracting to align more closely with the Proponent's existing models and policies?

Answer: Yes. The SLAs can be further discussed and negotiated during the contracting process.

29. We understand that the Department is looking for a new IT solution to provide UCC registry services for financing statements. We also understand most of the technical infrastructure requirements (e.g., a clouded solution). However, we ask if there are any other technical requirements with which the system must comply. We ask if there is a preference for the following:

    a. Database management system
    b. Programming language

Answer: No, however take note that we expect this IT Solution should be implemented on: Amazon Web Services (AWS), Microsoft Azure, or Oracle Cloud Infrastructure (Gen-2). Please submit more details on your proposed workplan. In addition, current Database Management System is PostgreSQL. Please refer to page 5 section 4 of the NPS.

30. Our proposal will establish the assumption that, mainly on a reactive basis, the Department will provide most of the detailed-level knowledge of the Commercial Transactions Act that we will need in order to correctly develop the new solution. Is that assumption valid? Or does the Department expect us to bring legal personnel to the mix?

Answer: Yes. The Department will provide the business rules related to the Commercial Transactions Act. However, a local counsel experienced on the matter is strongly advisable.

31. The RFP states that we must integrate an accounting system into the solution. Does this refer strictly to a system to process UCC form transactions and process the corresponding payments? Or is it actually a full-fledged accounting system that handles billings, collections, invoices, payments, cash management, etc.?

Answer: The accounting system that is needed, is one that will allow users to submit payments, handle collections, invoices and payments, among others. Most importantly, the Department should be able to have access to this data, as needed.

32. We understand that there is a legacy system from which we are expected to convert data via OCR technologies. Is this because the source of data will be scanned UCC1 documents? Or will we be able to convert structured data in the legacy system as well? We ask you to please explain.

Answer: All UCC financing statements are filed by the users directly to our current

platform. Thus, all the documents are digitized and uploaded into the platform.

33. What would be the use of OCR, you want to extract data from images of some kind using OCR? Do you need to classify or manage it for a specific flow?

Answer: No. We expect the conversion of current document files, mostly PDFS and Microsoft Words, to OCR searchable ones. Current files are organized on a PostgreSQL database.

34. The RFP refers to support services, and mentions phone calls, ticketing service and resource at the Department's offices. Does this mean that the Department is asking us to provide personnel to run a help desk for the application? Or is it that the system must include a trouble-ticketing facility for Department employees to handle user issues? Please explain in detail.

Answer: The Department expects to be able to have a resource in its main office, who will be in charge of providing support to users as well as to employees of the Department. The system must also include a trouble-ticketing tool for the Department's employees to handle user issues.

35. Page 5 section 6 of the RFP refers to the Puerto Rico Uniform Commercial Code Solution (PRUCC). Please clarify whether this refers to the new intended solution (or whether it is some other system not previously mentioned).

Answer: The Department were referring to the new intended solution (the IT-solution).

36. Page 6 section 2 of the RFP mentions the documentation of UCC functional requirements, and states that they must be documented, actionable, etc. However, there is no mention of initial system design documentation to be submitted. We intend to describe such documentation as part of our proposal, yet we ask the Department whether it has a documentation standard with which we must comply in our design documents.

Answer: There is no standard documentation available at the time.

37. All Personally Identifiable Information also known as (PII) should be encrypted and protected. Does the database of the proposed IT Solution must be encrypted?

Answer: Yes. All data, files, user information and components related to the Registry are considered Personally Identifiable Information (PII) and must be protected and encrypted.

38. Transmission of Data should be encrypted and protected. Which data will be transmitted, to where?

Answer: All communications between the IT Solution and the users through the Portal or IT Solution to be provided, should be encrypted and protected. The information that is provided by the user, I.e., the UCC filing, should be transmitted from the user through

our portal and into the IT Solution.

39. Description of the service that the Service Desk will offer?

Answer: The Department expects to be able to receive technical assistance 24/7, as needed. Pursuant to the Department's assessment to date, one person will be sufficient to provide the assistance that is needed.

40. The IT solution platform shall use the pr.gov domain to comply with PRITS Circular Letter No. 2021-004. A URL provided by the Department?

Answer: Yes. Please refer to PRITS' Circular Letter No. 2021-004 re "Dominio oficial del Gobierno de Puerto Rico (pr.gov)" attached hereto as Annex C.

41. The IT solution platform shall comply with PRITS Interface and Design Guides PRITS No. 004. Please provide PRITS Interface and Design Guides PRITS No. 004.

Answer: Please refer to PRITS' Interface and Design Guides – PRITS No. 004 attached hereto as Annex D.

42. Section A. Scope of Work "IT Solution should be available 24/7/365." It is a URL where it will be up at all times?

Answer: Yes, the IT Solution must be always accessible through a URL.

43. Which is the preferred intuitive reporting tool? What kind of reports are required? Which is the format? Number of reports?

Answer: Please provide your proposed reporting tool on the work plan. Note that the reports needed should include detail on the UCC-1, UCC-3, and other related transactions, including time in which each is presented or filed and related costs.

44. A Project Manager is wanted to be assigned to this project, so it can provide information and project status reports?

Answer: Yes.

45. Is the Department is looking is a 5-year term? Renew annually after the 5-Year term or to another term?

Answer: The Department expects to engage in discussions regarding all contract aspects, including the term of the contract, once the proponent is selected.

46. Section B. General SOW "The Proponent shall manage all information and data associated with the Commercial Transactions Act with the Department." This means, that IT Solution shall be managed by the Proponent?

Answer: The IT Solution will be managed by the selected proponent and the

Department. The existing database should be migrated to the IT Solution.

47. The Department, will allow the proponent Operational Groups (servers, Backup, Firewall, etc.) to enter their environment to manage, configure their infrastructure?

Answer: Yes, the Department will provide the required access to the selected proponent's team members to maintain and work on the IT Solution.

48. Which are the Registry laws and regulations? Please provide them.

Answer: Please refer to Act No. 208-1995, as amended, and related regulations.

49. What are the detail requirements and specifications for the solution UCC financing statement system per Puerto Rico. UCC stands for Uniform Commercial Code?

Answer: Please refer to Act No. 208-1995 and the specific requirements in order to tailor your proposal to the Department's needs.

50. It is not very clear about the type of requirement regarding commercial transactions, it mentions amendments and financial statements, but it does not say what type of tax return amendments, customs payments or what? Daily amount, etc?

Answer: Act No. 208-1995, as amended, provides for the registry of all commercial transactions. Please note that tax returns are unrelated to the matter at hand.

51. Does the Department of State want to modify the existing portal or to create a new one?

Answer: This NPS aims to create a new portal through this IT Solution.

52. SLAs must be constructed and agreed between the Department and proponent?

Answer: Yes.

53. The type of backup the GPR chooses/assign it when opening their cloud subscription, as they are providing these infrastructures, or want the proponent to manage it through their cloud subscription?

Answer: Yes, all the resources needed to perform these tasks will be provided through the GPR's cloud-based subscription.

ANNEX A:
PRITS - Estándares para la Seguridad Cibernética v1.0

PR ITS cyber security

PUERTO RICO INNOVATION & TECHNOLOGY SERVICE

ESTÁNDARES PARA LA SEGURIDAD CIBERNÉTICA

V1.0

Para la Rama Ejecutiva del Gobierno de Puerto Rico

Según establecido por el Puerto Rico Innovation and Technology Service por virtud de la Ley 75-2019.

Título:	**Estándares para la Seguridad Cibernética**		
Aprobado por:	Enrique A. Völckers Nin		10/29/2021
Jefe responsable:	N'gai Oliveras Arroyo	Revisado:	10/29/2021
Oficina responsable:	Oficina *de Ciberseguridad*, Puerto Rico Innovation and Technology Service (PRITS)	Contacto:	soc@prits.pr.gov

Contenido

1. Trasfondo

La Política para la Seguridad Cibernética del Gobierno de Puerto Rico establece un marco con medidas de seguridad mínimas, define roles y responsabilidades e instaura los estándares para proteger la información gubernamental. Con estos fines, los requisitos técnicos aquí presentados fueron diseñados para respaldar la política y delinear los principios y procedimientos para proteger los sistemas y activos de información.

2. Definiciones

Para este documento, los siguientes términos tendrán el significado que se establece a continuación:

2.1 *"Acceso no autorizado"* – ocurre cuando una persona obtiene acceso lógico o físico sin aprobación o consentimiento a una red de infraestructura crítica, sistema, datos, aplicación u otro recurso de tecnología de la información del gobierno.

2.2 "Activos sensitivos" – significa información, equipo o medios donde la pérdida, mal uso, acceso o modificación no autorizados pudieran afectar adversamente los intereses del Gobierno de Puerto Rico y/o la privacidad de los ciudadanos.

2.3 *"Agencia"* – significa cualquier junta, organismo, junta examinadora, comisión, corporación pública, oficina, división, administración, negociado, departamento, autoridad, funcionario, empleado, persona, entidad o cualquier instrumentalidad de la Rama Ejecutiva del Gobierno de Puerto Rico.

2.4 "Arquitectura de confianza cero" (zero trust arquitecture, en inglés) – significa un plan de seguridad cibernética de una agencia, que, ante una red considerada comprometida, es diseñado para minimizar la incertidumbre en la aplicación de políticas precisas de acceso con privilegios mínimos y abarca las relaciones de los componentes y la planificación del flujo de trabajo.

2.5 *"Autenticación"* – significa una medida de seguridad diseñada para para proteger un sistema de información y verificar la identidad de un usuario, proceso o dispositivo. A menudo, es un requisito previo para permitir el acceso y proteger los recursos en un sistema de información.

2.6 "Autenticación multifactorial" (MFA) – significa un sistema de autenticación que utiliza dos o más factores distintos para una autenticación exitosa. La autenticación multifactorial se puede realizar utilizando un autenticador multifactorial o mediante una combinación de autenticadores que proporcionan diferentes factores. Los factores de autenticación son:

i. Algo que sepa (por ejemplo, contraseña / número de identificación personal (PIN),
ii. Algo que tenga (por ejemplo, dispositivo de identificación criptográfica, "token"),
iii. Algo que eres (por ejemplo, biométrico).

2.7 *"Autorización"* – significa el proceso de otorgar a un usuario privilegios de acceso a la información o a un sistema de información.

2.8 *"Confidencialidad"* – significa preservar las restricciones de acceso y divulgación, incluyendo los medios para proteger la privacidad personal e información confidencial.

2.9 *"Credenciales"* – el nombre de usuario y la contraseña únicos que se proporcionan a cada usuario autorizado para acceder a los recursos y aplicaciones de los sistemas de información del gobierno.

2.10 *"Cuenta administrativa"* – significa una cuenta de usuario con privilegios elevados destinada a realizar tareas legítimas de administración, como la instalación de actualizaciones y software de aplicación, la administración de cuentas de usuario, la configuración de aplicaciones y la modificación al sistema operativo (SO), entre otros.

2.11 *"Disponibilidad"* – significa garantizar el acceso y el uso oportuno y confiable a la información.

2.12 *"Infraestructura crítica"* – se refiere a los servicios, sistemas y activos esenciales, ya sean físicos o virtuales, cuya incapacidad o destrucción tendría repercusiones perjudiciales en la seguridad cibernética, la salud, la economía, la seguridad de Puerto Rico o cualquier combinación de esos asuntos.

2.13 *"Ciberseguridad"* – significa la prevención de daños a, protección y restauración de-computadoras, sistemas y/o servicios de comunicación electrónica, incluyendo la información contenida en ellos para garantizar su disponibilidad, integridad, autenticidad, confidencialidad y no repudio.

2.14 *"Datos"* – significa información registrada, independientemente de la forma o el medio en el que está registrada.

2.15 *"Dispositivo móvil"* – significa cualquier dispositivo de computación móvil como un teléfono inteligente, otros teléfonos celulares, tableta, lector electrónico, dispositivo de medios portátil, dispositivo de computación portátil o cualquier otro dispositivo móvil con capacidad para almacenamiento de datos y conexión de red.

2.16 *"Cifrado"* – significa un procedimiento criptográfico en el que el texto sin formato se convierte a un formato de texto cifrado para evitar que cualquier persona, excepto el destinatario previsto, lea dichos datos.

2.17 “Cuenta de usuario estándar” – significa una cuenta de usuario con privilegios limitados para tareas generales.

2.18 *“Equipo”* – significa cualquier propiedad tangible y duradera del gobierno relacionada con las tecnologías de la información y la comunicación, que es útil para llevar a cabo las funciones de comunicación o manejar la información de una agencia.

2.19 *“Firewall”* – significa una entrada que, siguiendo una política de seguridad local, limita el tráfico de comunicación de datos hacia y desde una de las redes conectadas para proteger los recursos del sistema de esa red contra las amenazas de la otra red.

2.20 “Firmware” - significa software y datos almacenados en hardware en una memoria de solo lectura (ROM, en inglés) o memoria programable de solo lectura (PROM, en inglés), de manera que los programas y datos no se pueden escribir o modificar durante la ejecución de los programas.

2.21 *“Gobierno”* – significa la Rama Ejecutiva del Gobierno de Puerto Rico.

2.22 *“Incidente”* o *“incidente de seguridad de la información”* – significa un suceso que (i) pone en riesgo real o inminente, sin autoridad legal, la integridad, confidencialidad o disponibilidad de la información o un sistema de información; o (ii) representa una violación o amenaza inminente de violación de la ley, políticas de seguridad, procedimientos de seguridad, políticas de uso aceptable o prácticas estándar de seguridad informática.

2.23 “Información de Identificación Personal” (IIP) significa cualquier representación de información que es legible sin la necesidad de una clave criptográfica especial para acceder a ella, permite o facilita el rastreo de la identidad de un individuo, incluyendo el nombre o la primera inicial y el apellido paterno de un individuo combinado con otra información que está vinculada o que se puede vincular a un individuo específico, como:

- Número de Seguro Social
- Número de licencia de conducir, tarjeta electoral u otra identificación oficial
- Números de cuentas bancarias o financieras de cualquier tipo, con o sin claves de acceso que puedan habérsele asignado
- Nombres de usuario y claves de acceso a sistemas informáticos públicos o privados
- Información médica protegida por la Ley HIPAA
- Información contributiva
- Evaluaciones laborales

2.24 “Información protegida de salud” (IPS) – significa cualquier representación de información que es legible sin la necesidad de una clave criptográfica especial para acceder a ella, contiene al menos el nombre de una persona o la primera inicial, y el apellido paterno combinado con información médica protegida por la Ley HIPAA, que incluye información demográfica, historial médico, resultados de análisis y laboratorio, afecciones de salud mental, información de seguros

o cualquier otro dato que los profesionales de la salud recopilan para identificar a una persona y determinar la atención adecuada.

2.25 "Integridad" – significa proteger la información contra la modificación o destrucción indebida, incluyendo garantizar el no repudio y la autenticidad de la información.

2.26 *"Malware"* – significa un software diseñado para obtener acceso no autorizado a un sistema de información y/o interrumpir, comprometer o dañar el funcionamiento de un sistema, al realizar una función o proceso no autorizado que afecta la confidencialidad, integridad o disponibilidad de un sistema de información.

2.27 "PRITS" – significa el Puerto Rico Innovation and Technology Service.

2.28 "Programa" o "software" – se refiere a los programas informáticos y datos asociados que pueden escribirse o modificarse dinámicamente durante su ejecución.

2.29 *"Recursos de información"* – significa información y los recursos relacionados, como, por ejemplo, personal, equipo y tecnología de la información.

2.30 *"Seguridad de la información"* – significa proteger la información y los sistemas de información para prevenir el acceso, utilización, divulgación, interrupción, modificación o la destrucción no autorizada que impida su confidencialidad, integridad y disponibilidad.

2.31 *"Sistema de información"* – significa un conjunto discreto de recursos de información para la recopilación, procesamiento, mantenimiento, uso, intercambio, difusión o disposición de información.

2.32 *"Tecnología de la Información"* (TI)

2.32.1 Para una agencia, significa cualquier sistema interconectado o subsistema de equipo utilizado en la adquisición, almacenamiento, análisis, evaluación, manipulación, manejo, movimiento, control, visualización, conmutación, intercambio, transmisión o recepción automática de datos o información por la agencia si el equipo es utilizado por la agencia directamente o por un tercero bajo un contrato con la agencia que requiere el uso (i) de ese equipo; o (ii) de ese equipo en una medida significativa para la prestación de un servicio o el suministro de un producto;

2.32.2 Incluye computadoras, equipos auxiliares (incluidos periféricos de imágenes, dispositivos de entrada, salida y almacenamiento necesarios para la seguridad y vigilancia), equipos periféricos diseñados para ser controlados por la unidad central de procesamiento de una computadora, software, firmware y procedimientos y servicios similares (incluyendo servicios de apoyo) y recursos relacionados.

3. Requisitos Técnicos

3.1 Internet

3.1.1 Está prohibido el uso de Internet para realizar actos ilícitos, incluido el acceso a sitios web con contenido ilegal, obsceno, de odio, difamatorio, indecente, objetable o inapropiado.

3.1.2 Las agencias establecerán controles para evitar el uso inadecuado del internet y una política de seguridad para al menos bloquear el acceso a sitios web con contenido pornográfico.

3.1.3 Se establecerán controles de autenticación, autorización, confidencialidad, integridad y monitoreo para proteger la información y los sistemas en aquellos casos en los que sea necesario acceder a la red interna desde fuera de las instalaciones de la agencia.

3.1.4 Se utilizará un "firewall" para controlar la comunicación con el internet desde dentro de la agencia.

3.1.5 Se establecerán los controles necesarios (por ejemplo, cifrado) para garantizar la confidencialidad de los datos sensibles en reposo y en tránsito en redes no seguras (por ejemplo, Internet, redes inalámbricas).

3.1.6 Las conexiones remotas a la red del gobierno se realizarán únicamente a través de una red privada virtual (VPN, en inglés) exclusivamente para uso oficial cuando las tareas relacionadas con el trabajo sean necesarias. Para el uso de la aplicación VPN, se establecerá un acuerdo que incluya una autorización de administrador de datos y un reconocimiento de las siguientes responsabilidades.

3.1.6.1 Proteger la información del gobierno evitando el acceso de usuarios no autorizados a las redes internas del gobierno a través del VPN.

3.1.6.2 Mantenimiento de parches y certificaciones de seguridad del sistema.

3.1.6.3 Asegurarse de que no haya información no cifrada y altamente confidencial almacenada en el dispositivo.

3.2 Software y Aplicaciones

3.2.1 Todo programa de aplicación desarrollado, por una agencia o mediante contrato con un tercero, para brindar servicios a los ciudadanos a través de Internet o facilitar las operaciones internas de la agencia, deberá asegurar que considera los siguientes elementos mínimos de seguridad para su implementación.

3.2.1.1 La integración de las mejores prácticas de seguridad para evitar accesos no autorizados y/o maliciosos a través del internet.

3.2.1.2 El uso de un firewall que controla el acceso al programa desde el internet.

3.2.1.3 Si el servicio a brindarse maneja datos sensibles, se deberá incluir e instalar en una red alternativa un sistema de prevención/detección de intrusiones para permitir el acceso controlado desde Internet y a la red interna para un intercambio de datos limitado y monitoreado.

3.2.1.4 Se deberá realizar una evaluación de vulnerabilidad antes de que la aplicación se ponga en producción y su certificación se incluirá como parte de la entrega de los servicios o productos.

3.2.2 Cualquier agencia que acepte pagos con tarjeta de crédito en sus portales a través de un motor de pago deberá cumplir con los estándares de seguridad de datos de la industria de tarjetas de pago (PCI DSS, en inglés). Además, la agencia deberá enviar los informes de cumplimiento requeridos por el proveedor de la cuenta o aplicación.

3.3 Autenticación multifactorial

Para garantizar las mejores prácticas de ciberseguridad, el uso de autenticación multifactorial (MFA, en inglés) será obligatorio para el siguiente tipo de usuarios:

- Todas las cuentas administrativas de TI.
- Cuentas de usuario del personal ejecutivo, directores y cualquier otro personal que administre información confidencial, IPS y/o IIP.
- Empleados que trabajan de forma remota.
- Contratistas y proveedores de servicios externos.

3.4 Servicios Contratados

3.4.1 Los contratos con terceros incluirán medidas para salvaguardar los activos sensibles. Los contratistas recopilarán y mantendrán información relevante para la prevención, detección, respuesta e investigación de la seguridad cibernética en todos los sistemas de información sobre los cuales tienen control u operan en nombre de las agencias.

3.4.2 Los proveedores de servicios externos de tecnología de la información y comunicaciones compartirán información y notificarán de inmediato al PRITS y a la agencia contratante cuando descubran un incidente de seguridad cibernética o un incidente potencial que pueda poner en riesgo los datos, productos de software y servicios confidenciales del gobierno.

3.4.3 Para cualquier contrato de servicios de ciberseguridad, el proveedor de servicios externo presentará a la Oficina Principal de Seguridad de la Información del gobierno informes mensuales sobre el estado de la ciberseguridad de los sistemas de información y los activos administrados en nombre de la agencia. Estos informes incluirán la información que se detalla a continuación.

- Las amenazas detectadas, los actores de amenazas y las vulnerabilidades.
- Las acciones de respuesta y remediación.
- El número total de incidentes de seguridad de la información que se informaron al PRITS a través de la plantilla para el Informe de Incidentes de Ciberseguridad.

3.4.4 Los proveedores cuyos servicios estén relacionados con la ciberseguridad o cuyos servicios requieran que información sensible de los ciudadanos resida en sus sistemas, deberán contar con una certificación de seguridad válida conocida como SOC 2 o ISO/IEC 27001. El PRITS tiene la autoridad única para solicitar esto o certificaciones adicionales en función de los productos o servicios a ser entregados.

3.4.5 La agencia será responsable de determinar cuándo un contratista o un tercero requiere acceso a una aplicación o sistema de información en particular, y cualquier otro aspecto del entorno de TI de la agencia. Una solicitud de privilegios de acceso será evaluada por el Oficial Principal de Informática o el personal de TI designado por éste, antes de otorgar acceso. El acceso será limitado en alcance y tiempo, de acuerdo con los servicios a ser prestados por el contratista, y será modificado o revocado cuando corresponda.

3.4.6 Si es necesario para llevar a cabo los servicios contratados, cada individuo tercero deberá tener una cuenta única establecida para ellos en el directorio activo, incluidas las credenciales de inicio de sesión. Se prohíben las cuentas genéricas o globales con credenciales de inicio de sesión compartidas.

3.5 Controles Adicionales de TI

3.5.1 Las agencias instalarán controles automáticos para la detección de programas no deseados (por ejemplo, virus, *adware*, *spyware*, *malware*, *ransomware*) y la prevención de eventos o actividades de intrusión que puedan afectar la seguridad de la información. Microsoft Defender AV será la primera opción para proteger los activos gubernamentales. El uso de otros productos antivirus deberá obtener la aprobación previa del PRITS. Los productos y servicios proporcionados por Kaspersky Lab están prohibidos.

3.5.2 Los sistemas de TI del gobierno se utilizarán estrictamente para realizar asuntos gubernamentales.

3.5.3 Las instalaciones y activos de procesamiento de información (por ejemplo, servidores, armarios de cableado para redes, conexiones telefónicas, áreas de impresión para datos sensitivos o

confidenciales) deberán estar alojados en áreas seguras, protegidas con un perímetro de seguridad apropiado y controles para evitar el acceso no autorizado y daños.

3.5.4 La información confidencial (por ejemplo, IIP, IPS) no quedará expuesta ni desprotegida bajo ninguna circunstancia. Deberá estar encriptada en todos sus estados (es decir, en tránsito y en reposo).

3.5.5 Los usuarios no deberán usar la misma contraseña para múltiples cuentas (por ejemplo, cuentas de correo electrónico personales y laborales, cuentas de sitios web, etc.).

3.5.6 Los usuarios evitarán abrir y ejecutar archivos de fuentes desconocidas o no confiables. Deberán validar con el personal de TI de su agencia antes de descargar y ejecutar archivos de sitios web no gubernamentales.

3.5.7 Los privilegios de acceso de los usuarios se reevaluarán periódicamente. El acceso empleará el principio de privilegio mínimo, permitiendo a los usuarios autorizados acceder solo a los datos y aplicaciones que son necesarios para realizar sus tareas y funciones.

3.5.8 Los programas de aplicación y la información tendrán controles de acceso que incluirán mecanismos de autenticación y autorización.

3.5.9 Todos los mecanismos de autenticación incluirán una contraseña de no menos de ocho (8) caracteres, que incluya una combinación de números, letras y caracteres especiales.

3.5.10 Todas las contraseñas de las cuentas administrativas se cambiarán al menos cada cuatro (4) meses y todas las de cuentas de usuario estándar se cambiarán al menos cada seis (6) meses.

3.5.11 No se instalará ningún software en dispositivos y equipos de TI del gobierno a menos que lo apruebe el Oficial Principal de Informática (OPI) de la agencia o el personal de TI autorizado por éste. Solo se instalará software debidamente aprobado y con licencia. Se prohíbe cualquier software no autorizado, sin licencia o copiado ilegalmente.

3.5.12 La disposición de todo el equipo con información sensitiva debe realizarse con métodos seguros, de tal manera que no se pueda acceder a los datos una vez que el equipo se encuentre fuera de las instalaciones de la agencia.

3.5.13 Si un dispositivo o equipo de TI del gobierno se pierde o es robado, la Oficina de Informática de la agencia tomará las medidas apropiadas para borrar de forma remota, cuando sea posible, cualquier dato alojado en dicho hardware. Además, la Oficina de Informática de la agencia deberá completar un Informe de Incidente de Ciberseguridad para notificar al PRITS sobre la situación y la posible seguridad de la información en riesgo.

3.5.14 El uso de equipo fuera de las instalaciones de la agencia requerirá la autorización previa del Oficial Principal de Informática de la agencia o el personal de TI designado por éste. Las

agencias establecerán los controles y monitoreo necesarios para asegurar que el equipo que ha estado fuera de la agencia se esté utilizando legítimamente para cumplir con las obligaciones gubernamentales del personal autorizado y que el uso externo del equipo no represente un riesgo para los sistemas de la agencia. Esto incluye la evaluación del equipo y la realización de auditorías al conectarse a los sistemas o redes de la agencia.

3.5.15 Se requerirá la aprobación previa del Oficina de Informática de la agencia para las reubicaciones y transferencias de equipos.

3.5.16 El acceso a las instalaciones de los sistemas de información (por ejemplo, servidores, áreas de almacenaje de equipo) estará controlado de manera que solo el personal autorizado pueda accederlos.

En consonancia con la creciente complejidad y sofisticación del entorno de amenazas cibernéticas, se exhorta a las agencias a desarrollar un plan para implementar la Arquitectura de Confianza Cero de una manera coordinada para prevenir, detectar, evaluar y remediar incidentes cibernéticos.

3.6 Dispositivos Móviles

3.6.1 Controles Generales para Dispositivos Móviles Propiedad del Gobierno

Para evitar actividades maliciosas, violaciones de datos y otros incidentes de seguridad de la información, se tomarán las siguientes medidas para el uso adecuado de los dispositivos móviles.

3.6.1.1 Todos los dispositivos móviles se registrarán en la Oficina de Informática de la Agencia antes de ser asignados a empleados específicos. Esta Oficina mantendrá una lista de los dispositivos móviles asignados y las aplicaciones de software y utilidades instaladas antes de ser entregadas al usuario.

3.6.1.2 Los dispositivos móviles se utilizarán solo para tareas oficiales legítimas relacionadas con los roles y responsabilidades de los empleados.

3.6.1.3 Los usuarios no realizarán modificaciones en el hardware o software instalados, incluyendo las reconfiguraciones, sin la aprobación de la Oficina de Informática.

3.6.1.4 Según sea necesario, la Oficina de Informática podrá establecer mecanismos de auditoría para acceder y utilizar sin previo aviso con fines de investigación y detección de posibles infracciones y/o uso indebido.

3.6.1.5 Los usuarios instalarán, sólo de las tiendas de aplicaciones oficiales, exclusivamente aquellas aplicaciones necesarias para realizar asuntos gubernamentales. Las fuentes de aplicaciones confiables incluyen el Company Portal, Google Play Store, Apple Store

y Microsoft Store. Las aplicaciones de cualquier otra fuente están prohibidas y no deben usarse.

3.6.1.6 Todos los usuarios de dispositivos móviles emplearán medidas de seguridad física razonables, ya sea que el dispositivo esté en uso o sea transportado. Los dispositivos no deben dejarse desatendidos.

3.6.1.7 Cuando se utilizan dispositivos móviles para acceder a información confidencial, se tendrá especial cuidado para garantizar que la información a la que se accede no se vea comprometida (por ejemplo, personas no autorizadas que ven información en la pantalla).

3.6.1.8 El software se mantendrá con las actualizaciones más actualizadas y aprobadas.

3.6.1.9 Se prohíben los dispositivos liberados (“rooted”) o con "jailbreak".

3.6.1.10 Las capacidades de red, por ejemplo, Bluetooth y comunicación de campo cercano (NFC, en inglés) se desactivarán cuando no estén en uso.

3.6.1.11 Se evitarán las redes no seguras y las redes Wi-Fi públicas con problemas de seguridad. Los dispositivos no se conectarán a redes no seguras o no confiables a través de conexiones inalámbricas, de radio, Bluetooth o USB mientras estén acoplados, emparejados o conectados a las redes o dispositivos de la agencia.

3.6.1.12 Los dispositivos estarán protegidos con fuertes controles de seguridad, como contraseñas, datos biométricos o códigos de acceso (PIN, en inglés). Se prohíbe la divulgación de las credenciales de inicio de sesión.

3.6.1.13 Los usuarios configurarán cada dispositivo para que se bloquee automáticamente cuando esté inactivo.

3.6.1.14 Las opciones de autorellenar o autocompletar en los navegadores web no se utilizarán para recuperar automáticamente las credenciales de inicio de sesión (es decir, nombre de usuario y/o contraseñas).

3.6.1.15 Al acceder a información o utilizar cuentas, los usuarios deberán cerrar sesión y desconectarse al final de ésta.

3.6.1.16 La Oficina de Informática de la agencia podrá instalar software de seguridad adicional, administrar políticas de seguridad, redes, aplicaciones y acceso a datos más estrictos utilizando soluciones tecnológicas adecuadas, incluyendo controles remotos.

3.6.1.17 Los usuarios notificarán inmediatamente a la Oficina de Informática de la agencia en las siguientes circunstancias.

- El dispositivo se pierde o es robado. Se podrá solicitar información específica, como información, cuentas y aplicaciones susceptibles de acceso no autorizado.
- Se sospecha que el dispositivo está o ha sido atacado con malware, virus o cualquier otro ataque cibernético.
- Existe un problema de seguridad con respecto a los datos confidenciales o la información de las agencias.

3.7 Evaluación Periódica de Ciberseguridad

Según sea requerido por PRITS, las agencias realizarán periódicamente evaluaciones de ciberseguridad, que incluyen, entre otras, la evaluación de amenazas y vulnerabilidades, controles de TI existentes e inventario de activos de TI, etc. Los usuarios garantizarán actualizaciones periódicas de los sistemas operativos y aplicaciones primarias (por ejemplo, navegadores web, software de productividad, clientes de correo electrónico y software de seguridad).

3.8 Informes

3.8.1 Informe de Incidente de Ciberseguridad

Una vez que se descubre un incidente o amenaza de seguridad de la información, la agencia notificará inmediatamente al PRITS y enviará el Informe de Incidente de Ciberseguridad que incluirá la información descrita en la Guía para Informar Incidentes de Ciberseguridad.

3.8.2 Informes Mensuales

Las agencias que no son monitoreadas por PRITS deberán enviar informes mensuales de ciberseguridad, con una breve descripción de los puntos finales, ataques, vulnerabilidades críticas, detecciones de malware, intentos fallidos de autenticación y conexiones denegadas. Según sea necesario, los PRITS pueden requerir información adicional.

Historial de Revisiones

Los estándares para la seguridad cibernética pertenecen y son mantenidos por la Oficina del Principal Oficial de Ciberseguridad del Gobierno de Puerto Rico adscrita a PRITS.

Fecha	*Descripción del cambio*	*Revisado por*	*Aprobado por*

ANNEX B:
PRITS - Proposal Evaluation Guidelines (PEG) PRITS-001

PROPOSAL EVALUATION GUIDELINES

PRITS-001

for the Executive Branch of the Government of Puerto Rico

As established by the Puerto Rico Innovation and Technology Service

By virtue of Act 75-2019

Revised on: 10-15-2020

TABLE OF CONTENTS

1 Objectives

The PRITS Proposal Evaluation Guidelines ("PEG" or the "Guidelines") refer to the criteria that the Puerto Rico Innovation and Technology Service ("PRITS") will use to evaluate innovation and technology proposals submitted for approval by the Agencies[1] of the Government of Puerto Rico.

The Guidelines are to be used as a reference to comply with Act 75, as amended, enacted on July 25, 2019 ("Act-75"), creating the PRITS. The Guidelines are published to assist the requesting Agencies and serve as a complement to Circular Letter 2020-003 ("PRITS-2020-003"), published on August 31, 2020. PRITS-2020-003 establishes the process that entities under the purview of Act-75 must follow for the evaluation, authorization, acquisition and implementation of technologies mandated by Act-75.

PRITS is fully aware and recognizes that proposals vary greatly depending on the goods or services being acquired, and therefore, not every criteria will apply to all submissions. Similarly, the Guidelines are non-exclusive, therefore PRITS can incorporate other criteria, if applicable.

The Guidelines were built upon the Government of Puerto Rico's innovation and technology public policy and legal mandates, plus observations and experience gathered by PRITS as related to the wide-ranging deployment of technology solutions at the government. Additionally, it incorporates concepts from the Information Technology Infrastructure Library v4 ("ITIL"). ITIL is a set of detailed practices for IT service management ("ITSM") that focuses on aligning IT services with the needs of the organization. ITIL describes processes, procedures, tasks, and checklists that can be applied by an organization toward strategy, delivering value, and maintaining a minimum level of competency. It allows the organization to establish a baseline from which it can plan, implement, and measure.

To expedite the evaluation process, PRITS strongly recommends Agencies to review the PEG prior to a) creating a procurement document such as an RFI, RFQ, RFP or formal bid, b) directly requesting proposals to prospective vendors, and/or c) submitting Form PRITS-001. PRITS

[1] Article 3(a) Act-75 defines Agency as any board, bodies, examination board, commissions, public corporations, offices division, administration, bureau, department, authority, official, employee, person, entity or any government instrumentality of the Executive Branch of the Government of Puerto Rico (collectively the "Agency" or "Agencies").

encourages Agencies to review the PEG with their prospective vendors to ensure they are aware and can meet the requirements outlined within this document.

Also, PRITS strongly recommends Agencies to conduct a proper needs and viability assessment and planning phase in accordance to findings and recommendations from the Special Report TI-17-02 of the Office of the Comptroller of the Government of Puerto Rico. This is also emphasized in the PEG.

2 Authority

PRITS is created with the purpose and responsibility of establishing public policy on the preparation, management, development, coordination and effective interagency integration of innovation and technology.

Pursuant to section (ff) of Article 6 of Act-75, PRITS will "review, evaluate and approve any project for the creation, implementation, modification, migration and update of databases, innovation, information and technology to be adopted by the agencies." In addition, Article 15 of the PRITS Act provides that:

> [PRITS] will have the power to review, evaluate and approve any project for the creation, implementation, modification migration and update of databases, innovation, information, and technology to be adopted by the agencies. PRITS will issue in writing the corresponding recommendations and standards, as the case may be, so that the agencies' database, innovation, information and technology projects comply with the purposes of this Act and will forward such communication to the head of the agency and the chief information officer of the agency. The agencies will have to design, develop, adopt, and implement their database, innovation, information, and technology projects in accordance with the parameters and specifications established by PRITS. Likewise, said Office must evaluate and approve any contracting of services or purchase of equipment by the agencies to be used or destined for a database, innovation, information, and technology project.

3 Scope

Following PRITS-2020-003, the Guidelines are to be used in the evaluation and authorization request for the acquisition and implementation of the following products and services:

a. Professional services related to:
    - Software development and related services
    - Infrastructure development and deployment
    - Hardware configuration and deployment
    - Operating and maintenance agreements services
    - Other consulting and professional services performed related to IT projects or any other projects containing an IT component
b. Data centers (hardware, infrastructure and related goods and services)
c. Computers, peripherals and other technology equipment
d. Highly specialized technology equipment
e. Cloud services
f. Telephony systems
g. Network infrastructure
h. IT Security equipment and services
i. Data management and/or analytics platforms
j. Portals and webpages
k. Mobile applications
l. COTS (Commercial Off-the-Shelf)
m. Licensed products
n. Any “as a service” acquisition (e.g. SaaS, PaaS, IaaS etc.)

These are common categories in IT, but the list is non-exclusive as PRITS’ scope covers a comprehensive range of information systems, technology and innovation goods or services.

4 Roles and Responsibilities

4.1 Agencies and CIO’s

Article 12 of Act-75 outlines the Agency’s duties and responsibilities for complying with the requirements of Act-75. Said duties and responsibilities include liaising with PRITS regarding innovation and technology strategy, technology services and standards, among others. In addition, the Agency’s Chief Information Officer (“CIO”) will be responsible for compliance with Article 13 of Act-75 which outlines their responsibilities as they pertain to leading their respective organization and ensuring compliance. As part of that responsibility, the Agency’s CIO is required to evaluate the proposed acquisition prior to the submission to the PRITS for approval.

This means that by filing the PRITS-001, the Agency's CIO certifies that a review of the proposed acquisition has been done, and after careful review, it is in the Government's best interest that the good(s) or service(s) be acquired. No Agency shall file a PRITS-001 without previously reviewing and analyzing the proposed acquisition with their Agency's CIO.

PRITS-2020-003 is clear in that Agencies are responsible for engaging with PRITS as a first step in the process, including prior to publishing RFPs, RFIs, RFQs, or formal bids. Procurement documents that are not approved by PRITS can result in lost efforts due to misalignment with the technology and innovation public policy and might not procure adequate goods or services. Final acquisition approval could be denied. Therefore, Agencies are required to engage with PRITS in the early stage, as established in PRITS-2020-003. The final selection of an RFP, RFI, RFQ or formal bid must also be notified and submitted to PRITS.

According to the goods or services being procured, if no formal procurement document will be published, PRITS requires that form PRITS-001 is submitted together with the selected proposal(s).

It is highly recommended that Agencies allocate or identify funding sources prior to filing PRITS-001, except in the case of projects that don't require additional funds. This is relevant because PRITS must evaluate proposals for technology and innovation projects even when these don't require the use of public funds in order to assure public policy alignment.

Once approved by PRITS, Agencies are fully responsible for following all other acquisition procedures and request the necessary approvals, as applicable. Also, it is important to note that most Agencies also are to be in compliance with the requirements of Act 73, as amended, enacted on July 23, 2019, known as the General Administration for the Centralization of Procurement of the Government of Puerto Rico of 2019 ("Act-73"), to the extent applicable, and/or with any other (local and/or federal) procurement and contracting requirements applicable to the Agency.

4.2 PRITS

PRITS is responsible for evaluating in a timely manner all proposals and PRITS-001 forms submitted in full compliance with PRITS-2020-003 for evaluation. PRITS conducts the internal evaluation and approval procedure, and can request more information or revision if necessary, In the case of a non-authorized proposals, PRITS shall include the issues that failed to be addresses and/or the reasons for the denied request.

Agencies need to be advised that PRITS' approval will have an expiration date to continue with the next step in the acquisition process. Also, the final acquisition shall not vary from the PRITS-001, as specified in PRITS-2020-003.

PRITS' role in evaluating proposals is limited exclusively to the evaluation enclosed by Act-75. Therefore, no authorization from PRITS shall be deemed as a legal review of any proposal or contract. PRITS does not evaluate actual contract documents and does not participate in any way in the Agency's procurement or contracting process. That is the sole responsibility of the Agency.

PRITS can have a direct involvement in different project phases as necessary, from the initial strategic discussion to supporting operational tasks. This can occur when requested by an Agency, in complex or interagency projects, or as determined by PRITS. PRITS can inquire on project or acquisition status, progress and results as necessary.

4.3 Others

General Services Administration of Puerto Rico ("GSA-PR"), Fortaleza & Office of Management and Budget ("OMB") must verify, per applicable law(s) and regulation(s), that purchases related to innovation and technology have been reviewed and approved by PRITS per PRITS-2020-003 prior to approving any and all related requests that fall within the scope of the policy as listed above in Section 2 and Act-75.

5 Proposal Evaluation Guidelines

PRITS will be seeking to understand supporting details for the following questions to guide the evaluation process and the discussion with the Agency, as applicable.

The following terms are used in this section and are defined below for reference:

- *Proposals*: Form PRITS-001, draft of procurement documents, vendor proposals or quotations for the acquisition of goods or services, and any other documentation submitted for evaluation.
- *Resources*: Personnel, contractors, services, application, systems, infrastructure, data, etc.
- *Solution*: the services, goods, applications, systems, platform, databases, licenses, etc., or the combination of these, being evaluated.

5.1 Public Policy Alignment

- Is this solution aligned with the strategic priorities established by PRITS?
- Is this solution aligned with the IT strategic plan established by the agency?
- Is this solution maximizing existing resources and investment in the same agency?
- Is this solution maximizing existing resources and investment in other Agencies?
- Is this solution contributing to simplify existing government processes?
- Is this solution impacting intra and/or interagency productivity?
- Is this solution maximizing the sharing of intra and interagency information?
- Is this solution contributing to the effective integration and interoperability of information systems?
- Is this solution contributing to minimize information systems redundancy and duplication of investments, efforts and projects?
- Does this solution have the potential to be expanded or leveraged by other Agencies?
- Is this solution in conflict with other projects or solutions in other Agencies?
- Is this solution contributing to simplify and enhance citizen experience and the quality of government services?
- Is this solution helping to promote the use of technology among citizens?
- Is this solution considered innovative or uses innovative technology?
- Is this solution aligned with the goals of developing of an innovation and technology ecosystem in Puerto Rico?

5.2 Needs Assessment, Design and Requirements

- Was a needs assessment completed?
- Are there similar needs identified in other Agencies?
- Were functional requirements identified and clearly documented by functional and subject matter experts? Were these prioritized or categorized as required and nice-to-have?

- Were the processes or services managed within the solution analyzed in their as-is state versus to-be state?
- Were technical requirements identified and clearly documented by qualified experts?
- Were policies, regulations and laws evaluated in the way these could introduce non-negotiable requirements? Does the solution comply with all applicable local, state, and federal laws? For example, does the solution comply with Law 229-2003 and/or Section 508 of the Rehabilitation Act to guarantee information use and access?
- Does the proposal include the complete lifecycle of the solution: analysis, design, development, testing, deployment, support and change/release management?

5.3 Agency Preparedness

- Is the Agency capable to embark in all tasks associated to all phases of the solution?
- Does the Agency have knowledgeable personnel and adequate supervision levels to ensure solution implementation success?
- Has the agency identified a dedicated and knowledgeable project manager(s)?
- Has the agency identified a clear owner responsible of the solution success?
- Are there any identified risks associated with management or administrative changes in the Agency that can hinder success? What is the plan to mitigate them?

5.4 Vendor and Solution Selection

- If a vendor has been selected, how was this selection done? Was more than one vendor/solution evaluated?
- Does the vendor have proven expertise, recognized reputation and/or is a recognized market leader in the type of solution being evaluated?
- Else, is this vendor an emerging start-up or innovator? How would this be beneficial for the government in the acquisition of this type of solution?
- Is the vendor or solution ranked by third-party researchers (Gartner, Forrester Research, etc.)?

- Is there an exclusive reseller agreement associated with the vendor or solution? Is this vendor a sole source for the solution?
- Are there relevant references for the vendor or solutions in other Agencies or government branches?
- Are there relevant references for the vendor or solution in other jurisdictions (municipal, state or federal jurisdictions, or other countries)?
- Are there relevant references for the vendor or solution in the private sector?
- Are there any identified risks associated with the vendor and/or the solution selection? What is the plan to mitigate them?
- Are there any identified conflict of interest with the vendor and/or the solution selection? What is the plan to mitigate them?

5.5 Cost

- Is the cost of the solution reasonable in relationship to its specialized nature?
- Is the cost of the solution reasonable in comparison to other alternatives?
- What is the financial/cost model? Is it based on time and materials, fixed monthly or annual rate, by subscription fees, by deliverables, by transactions, by usage volume, etc.?
- If the solution is implemented in other Agencies, has the cost been compared and negotiated to guarantee the best rate?
- What are the initial costs or setup fees of this solution?
- Are there any licensing costs associated with the solution? If yes, are they perpetual or recurring? If recurring, can the Agency guarantee long-term budget?
- In case of licensing or other services in existing government master contracts, is it benefiting from negotiated prices?
- In case of licensing, can the needs be fulfilled with available licenses administered by PRITS?
- Have maintenance, upgrade and support costs for the solution been considered? Can the Agency guarantee long-term budget for these? Can the solution be sustained without recurring budget for these concepts?

5.6 Implementation Timeline

- What is the high-level implementation timeline?
- Is the solution optimizing the time to deliver desired value? Will it use agile methodologies for rapid value delivery?
- Is this solution ready to be deployed? What needs to happen for rapid implementation in case of readily available solutions?
- Is this solution based on new development? Will development be done with existing components or will it be developed from scratch? Why is custom development needed instead of acquiring proven solutions that minimize inherent risks of new development?

5.7 Service Level Agreements (SLAs) and Warranties

- What are the SLAs related to the solution? As an example, consider uptime and incident response time.
- Is service availability and response time adequate according to Agency requirements and or according to industry standards?
- What are the penalties for SLA breaches?
- What are the warranties to assure expected service delivery?
- Are there scheduled downtime/maintenance time windows?
- What are the warranties for the goods provided by the vendor? Are all good repairs and/or maintenance covered during the contracted period?

5.8 Knowledge Transfer

- What is the knowledge transfer plan to train and enable government employees?
- How will employees be certified in the solution?
- How will training manuals, user guides, maintenance procedures and other relevant documentation be delivered and stored?
- Does the documentation follow known methodologies and/or standards?

- Have the key employees who will be trained been identified?
- What is the process to transfer knowledge at service termination?

5.9 Interoperability and Ecosystem

- Does the solution provide documented Application Programming Interface ("API")?
- What are the types of API protocols available? For example, SOAP, REST, GraphQL?
- How are APIs secured and how is access managed? How is API traffic throttled?
- Does the solution provide public and open APIs to be leverage by other systems?
- What plug-ins or extensions exists or have been considered for the solution to leverage existing ecosystems?

5.10 Security Design and Monitoring

- What is the solution's design to ensure confidentiality, integrity and availability of information and service?
- What testing has been performed to validate the security controls in place?
- What is the process to report information security incidents?
- Who will be monitoring security advisories and implementing corrective actions?
- Has the agency identified dedicated and knowledgeable technicians and support staff for tasks related to security measures and configuration of the solution?
- What is the access management process? How will authorized users be defined and configured?
- How will transfer or removal of accesses occur at service termination?

5.11 Metrics

- Which are the Key Performance Indicator ("KPI") to ensure the solution is adding value and is delivering the desired results from the functional perspective?

- Which are the KPIs focused on tracking system capacity, availability, security, and performance?
- Which are the KPIs focused on tracking the operational aspects of the solution that aids in the daily operational optimization?
- Which are the KPIs focused on assuring the desired ROI of public funds, focusing on anticipated benefits to citizens?
- Who will be measuring these KPIs and how these will be monitored and reported?

5.12 Quality Assurance, Service Validation and Testing

- Has a Proof of Concept (PoC) been performed? What were the results?
- What is the testing plan? Consider details for functional, integration, stress, and regression testing.
- How will the solution be validated against the original intent of the needs and requirements?
- Does the solution include any type of automated testing?
- Who will be responsible of documenting and executing test cases and test scripts? Where will this evidence be stored?
- Who will be responsible for validating and signing off on the test results?

5.13 Release Management and Change Management

- What is the process to implement configuration changes and/or minor changes that don't require a formal release/go-live?
- What is the process to develop, test, validate, and coordinate go-live deployments? Who will be performing these tasks?
- What training will need to occur for end-users and operating staff for new releases? How will documentation be updated with every new release?
- What is the process for hypercare post deployment?
- Will there be development, test and production environments?

- How will the source code for custom development be stored, managed, versioned and documented?

5.14 Service Continuity and Disaster Recovery

- What is the backup or replication mechanism?
- What is the disaster recovery plan? Does the plan take into account different types of disasters? For example, data loss, system loss, connectivity loss, data center loss.
- How often will the plan be tested and revised for this solution?
- What is the Recovery Time Objective (RTO) for the solution?
- What is the Recovery Point Objective (RPO) for the solution?

5.15 Data Architecture, Access and Ownership

- What is the data architecture for the solution?
- How is the data schema documented?
- What is the data governance process? Who can use the data? How can the data be used?
- How is data integrity and confidentiality guaranteed?
- Is the ownership of the data clearly established?
- How are audit logs stored? What type of detailed data is stored in these logs?
- How long is the data retained?
- How is data made available in case of audits and investigations?
- How will data be managed, or transferred if necessary, at service termination?
- In the case of SaaS, PaaS, IaaS or related models, how will data be accessed if there is no active subscription?
- Is the solution aligned with the Open Data Law (Act 122-2019)?

5.16 Infrastructure and Delivery Model

- Was existing infrastructure analyzed? Is the solution maximizing existing infrastructure capabilities?
- Will the solution be provided as Software-as-a-Service ("SaaS"), Platform-as-a-Service ("PaaS") or Infrastructure-as-a-Service ("IaaS")?
- In the case of SaaS, PaaS, IaaS or other related models, is the vendor committed to the continued investment, improvement and innovation of the solution? Has the vendor shared a product road map?
- In the case of SaaS, PaaS, IaaS or related models, is the vendor open to incorporate feedback and new requirements?
- In the case of SaaS, PaaS, IaaS or related models, are there configurations that can be administered directly by Agency?
- Will the solution be hosted in a public or private cloud or on-premise government-owned infrastructure? In what geography will the solution be hosted?
- Does the solution incorporate highly-scalable and highly-available design principles?
- Who is responsible for monitoring and implementing changes to hardware, system patches, and other infrastructure components?
- Are all components and versions of the solution properly tracked and documented, for example, with a configuration management database (CMDB) tool?
- Will the solution be under the main government portal and domain, pr.gov, as required for all digital services and transactions?

5.17 Monitoring, Support, Service Desk and Operational Model

- What's the plan for monitoring the end-to-end health of the solution once it's implemented?
- Has the agency identified dedicated and knowledgeable technicians and support staff for monitoring and support tasks?
- How will warranties be enforced for incidents and issues that come up after go-live?
- How will issues be reported, tracked, and fixed?

- What KPIs will be in place for problem and incident resolution?
- What is the continuous service improvement method?
- Who is responsible for monitoring, avoiding, and curing obsolescence?

5.18 Emergency Proposals

- What is the type of emergency? Cybersecurity threat/attack? System failure? Infrastructure damage? Is it related to a localized or to widespread event or disaster?
- Why is this solution needed to support the emergency?

6 Document Maintenance

The Chief Innovation & Information Officer of the Government of Puerto Rico is the authority on any changes to this document. The Guidelines shall be reviewed from time to time, as technology and innovation procedures evolve. Recurrent revisions in the short and medium term might be expected as PRITS continue to incorporate requirements and refine the criteria based on best practices and recognized standards, incorporate tools to optimize the process, and as feedback is incorporated. Documents, such as PRITS-2020-003 and PRITS 001, can be found on prits.pr.gov.

ANNEX C:

PRITS - Circular Letter 2021-004 Dominio Oficial del Gobierno de Puerto Rico

GOBIERNO DE PUERTO RICO
PUERTO RICO INNOVATION AND TECHNOLOGY SERVICE

VIA CORREO ELÉCTRONICO

20 de septiembre de 2021

CARTA CIRCULAR NÚM. 2021-004

Secretarios, Jefes de Agencias y Directores Ejecutivos
Departamentos, Agencias, Comisiones, Juntas, Administraciones, Autoridades, Corporaciones Públicas, Instrumentalidades y demás organismos o entidades componentes de la Rama Ejecutiva del Gobierno de Puerto Rico ("Entidad(es) Gubernamental(es)")

Enrique A. Völckers-Nin
Principal Ejecutivo de Innovación e Información, Gobierno de Puerto Rico
Director Ejecutivo, Puerto Rico Innovation and Technology Service

Re: DOMINIO OFICIAL DEL GOBIERNO DE PUERTO RICO (PR.GOV)

Base Legal

Esta Carta Circular se promulga en virtud de las facultades delegadas al Puerto Rico Innovation and Technology Service ("PRITS"), conforme la Ley Núm. 75 de 25 de julio de 2019, según enmendada ("Ley-75"). El inciso (a) del Artículo 6 de la Ley-75, faculta a PRITS a implantar, desarrollar y coordinar la política pública del Gobierno sobre la innovación, información y tecnología. Por su parte, el inciso (e) de dicho Artículo 6 dispone como mandato el mejorar el portal principal del Gobierno de Puerto Rico (el "Gobierno") con miras a maximizar la accesibilidad e integración de éste redundando en un beneficio para la ciudadanía y el mismo Gobierno.

La Ley-75 en su Artículo 7, inciso (3) autoriza la promulgación órdenes administrativas, opiniones y/o cartas circulares por parte de PRITS con el fin de garantizar el cumplimiento de cualquier ley. De la misma forma, la Ley 151 del 22 de junio de 2004, según enmendada, Ley de Gobierno Electrónico ("Ley 151") faculta a PRITS a establecer las guías o directrices necesarias para implantar las normas y los procedimientos relativos al uso de las tecnologías de información a nivel gubernamental. Dichas guías habrán de ser utilizadas por las Entidades Gubernamentales al dar cumplimiento al Artículo 7 de la Ley 151, que incluye el que se incorpore el uso de tecnologías de información y telecomunicaciones en el funcionamiento gubernamental.

Propósito y Determinación

La Ley 75 establece como una de las responsabilidades de PRITS la implementación de controles efectivos con relación a la seguridad de los sistemas de información que sustentan las operaciones y los activos gubernamentales. A su vez, la Ley 151 requiere que el Gobierno incorpore las tecnologías de información necesarias para que la ciudadanía, el sector empresarial y la interoperabilidad gubernamental cuenten con un sistema accesible, efectivo y transparente. Como herramienta complementaria, en abril de 2021, PRITS publicó las Guías de Interfaz y Diseño ("GUIDI")[i], versión 0.1 bajo el número PRITS-004, vigentes a la fecha de la presente Carta Circular.

Todo portal de Gobierno y/o de cualquiera de las Entidades Gubernamentales debe de residir en el dominio oficial designado: **pr.gov** (Ej: **agencia.pr.gov**). Para otros esfuerzos tácticos como dashboards o programas específicos se debe hacer uso del subdominio. (Ej: **programa.agencia.pr.gov**). En fiel cumplimiento con la normativa aplicable y la política pública establecida, PRITS no autoriza el uso de alteraciones u opciones adicionales al dominio y subdominio anteriormente establecido. Ejemplo de alteraciones u opciones no permitidas son: gobierno.pr o gov.pr, y el uso de otros dominios que acaben en .com, .net o .org.

El fiel cumplimiento con la presente Carta Circular y la normativa aplicable logrará de una manera uniforme seguir el estándar utilizado por la mayoría de las dependencias gubernamentales en el Gobierno Federal de los Estados Unidos y el resto de los gobiernos estatales. El uso de un dominio .gov es para uso exclusivo de entidades gubernamentales, lo cual redunda en impartir una legitimidad a las páginas del Gobierno. Mediante dicho proceder le facilitamos a la ciudadanía una manera fácil de constatar que el portal utilizado es legítimo y que su información está protegida.

Uniformado el uso del dominio pr.gov logramos que las páginas oficiales del Gobierno sean de fácil identificación, reduciendo así la posibilidad de diferentes modalidades de fraude y mitigar el peligro de las páginas maliciosas cuyo objetivo es sustraer información del ciudadano y/o estafar a los mismos. El uso del dominio pr.gov abona a la confianza del ciudadano y añade una capa de seguridad a la presencia del Gobierno en el internet.

La supervisión y seguridad de la infraestructura del dominio .gov está centralizada y se encuentra a cargo de la Administración de Servicios Generales de los Estados Unidos. La centralización de dicha supervisión y seguridad permite que dicha agencia federal auxilie a los gobiernos estatales en la notificación y resolución de incidentes de seguridad. En la esfera estatal, PRITS tiene la facultad de manejar el dominio pr.gov, y en caso de tener que responder a alguna situación de seguridad con respecto a dicho dominio cuenta con los recursos para de ser procedente realizar toda gestión o acción necesaria en conjunto con las autoridades estales y federales.

El fiel cumplimiento con el uso del dominio pr.gov es una gestión mandatoria y prioritaria, pues el Gobierno no puede asegurar la integridad y seguridad de los datos y transacciones que se encuentren en páginas externas, ya que recaen fuera de su alcance. El uso del dominio pr.gov permite que PRITS valide el cumplimiento con las políticas de seguridad, incluyendo, pero no limitado a, configuraciones y certificados adecuados.

En caso de que la Entidad Gubernamental desee hacer uso del **.pr** para algún esfuerzo publicitario debe obtener una autorización temporal previa de PRITS. Para obtener dicha autorización la Entidad Gubernamental deberá coordinar con PRITS, quien establecida la solicitud de autorización asistirá a

la Entidad Gubernamental en las alternativas disponibles e implementación de la selección autorizada. De la misma manera, toda Entidad Gubernamental que necesite activar un dominio o subdominio bajo **pr.gov**, o requiera de la asesoría en seguridad cibernética debe comunicarse con PRITS para encausar dicho trámite. Todos los servicios y/o solicitudes a ser realizados por la Entidad Gubernamental deberán remitirse al "Service Desk" de PRITS a: support@prits.pr.gov.

Reiteramos que es mandatorio que toda Entidad Gubernamental lleve a cabo las configuraciones y acciones necesarias para que los sistemas de correos electrónicos y su presencia en el internet utilice el dominio pr.gov. Toda Entidad Gubernamental que esté utilizando un dominio diferente tiene que, de forma inmediata, redirigir el mismo a un dominio pr.gov.

Tanto la Ley 75 como la Ley 151, facultan a PRITS a llevar a cabo las investigaciones necesarias, y tomar toda medida que entienda pertinente para asegurar el cumplimiento de sus directrices. Fuera del ámbito investigativo, la Ley 75 establece un deber afirmativo de la Entidades Gubernamentales bajo la jurisdicción de PRITS de cumplir con las leyes aplicables y las directrices impartidas en la presenta Carta Circular.

Es responsabilidad del Gobierno velar con gran celo la integridad de sus sistemas lo cual incluye la data que cualquier usuario provea en el uso de sus páginas. En la consecución de tal objetivo las Entidades Gubernamentales cuentan con la colaboración y asistencia de PRITS. Siendo la utilización del dominio pr.gov de tal importancia, urgimos a las Entidades Gubernamentales fuera de la jurisdicción de PRITS a utilizar el dominio pr.gov y proteger la integridad de sus páginas y sus respectivos usuarios.

Derogación

Esta Carta Circular deja sin efecto cualquier otra Carta Circular, Memorando, Orden Administrativa, Políticas, Normativas, comunicación escrita o instrucción anterior de PRITS o publicada por la OGP como su predecesora antes de la aprobación de la Ley-75, que en todo o en parte sea incompatible con ésta, hasta donde existiera tal incompatibilidad.

Vigencia

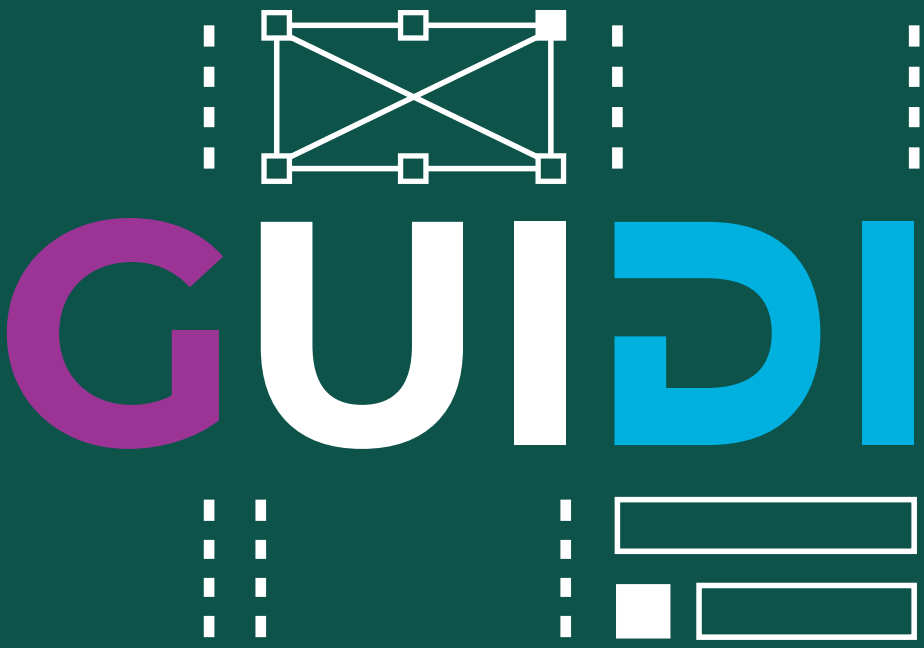
Esta Carta Circular tendrá vigencia inmediata.

---

[i] Las GUIDI pueden ser obtenidas a través del siguiente enlace: https://assets-global.website-files.com/606ce22566af383df2754cf8/60823478d257af0966f6045c_PRITS%20GUIDI%20%20Guias%20de%20Interfaz%20y%20Diseno.pdf

ANNEX D:
PRITS 004 - Guías de Interfaz y Diseño (GUIDI)

PUERTO RICO
INNOVATION &
TECHNOLOGY
SERVICE



Guías de
Interfaz y
Diseño

Versión 0.1 / Rev 04.2021

PR
ITS

GUIDI

Guías de Interfaz y Diseño

PRITS ha desarrollado un sistema de módulos para ser utilizado, tanto internamente como por recursos externos, como el estándar en el diseño y estructuración de todo portal del **Gobierno de Puerto Rico.**

Cada módulo está diseñado para funcionar como una pieza independiente, pero a su vez tienen la capacidad de formar parte de un conjunto de módulos más complejo, así ampliando las posibilidades a la hora de diseñar y estructurar cada portal. Esto permite que las combinaciones entre módulos tengan variaciones ilimitadas, lo que ayuda a cubrir las necesidades de cada agencia u oficina de manera creativa e independiente, pero manteniéndose bajo los parámetros que definen cómo se deben diseñar los portales del Gobierno de Puerto Rico.

Estas guías estarán en constante revisión para así proveer nuevos módulos y mejorar los existentes solucionando cada una de las necesidades del cuidadano a la hora de utilizar el portal diseñado.

GUIDI ha sido diseñado siguiendo las Guías de Accesibilidad de la Ley 229 para páginas web de Agencias del Gobierno de Puerto Rico, siguiendo los parámetros de tamaños de letras, contrastes, legibilidad e interpretación de lectores de pantallas.

¿Cómo utilizar las guías?

Todo texto explicativo en cada sección de éstas guías será destacado con el color azul claro como aquí marcado.

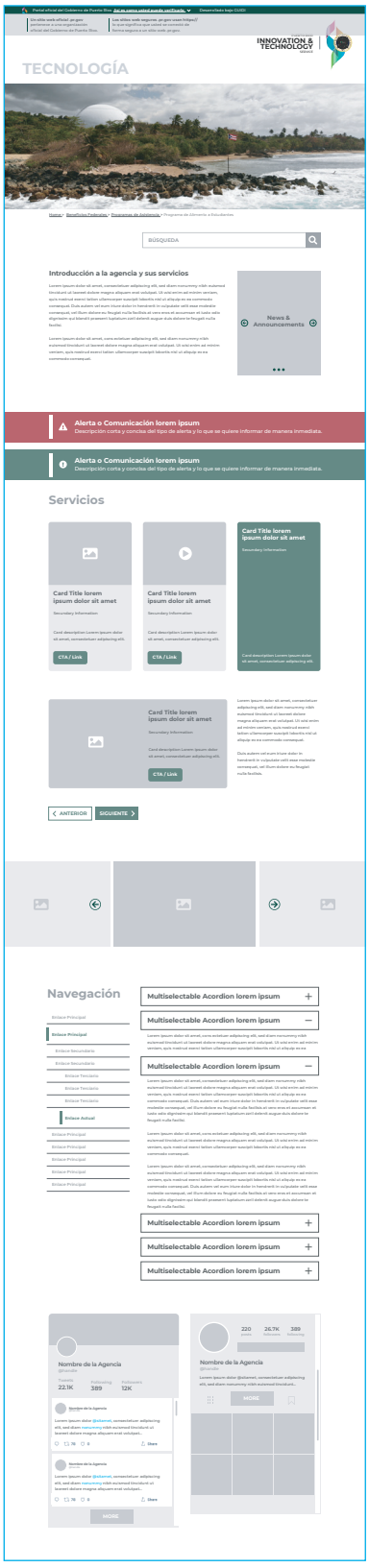
Los colores y fotos utilizadas en estas guías han sido seleccionados para explicar la funcionalidad de los módulos de una manera sencilla y neutral. Le proveemos varias combinaciones de colores que han sido escogidas específicamente para que el diseño del portal esté fuera de cualquier interpretación de índole político-partidista.

Cada módulo está compuesto de un bloque de contenido horizontal, el cual a su vez está divido en tres (3) columnas verticales (en algunos casos es de 2 o 4 columnas). Todos los módulos ocupan el mismo ancho, excepto donde se indique.

Módulo horizontal con contenido en 3 columnas verticales

Módulo con contenido que ocupa el ancho completo de las 3 columnas

Módulo horizontal con contenido en 2 columnas verticales



Titulares y Secciones

HEADLINES DE LAS PÁGINAS
MONTSERRAT BOLD
HEX #999999
62 pnts con 70 pnts de leading

Títulos o Subtítulos

Títulos o Subtítulos de Secciones
Montserrat Semibold
HEX #666666
36 pnts con 42 pnts de leading

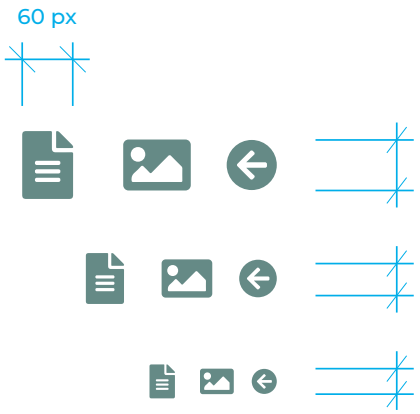
Lorem ipsum dolor sit amet, cons ectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat.

Bloques de textos
Montserrat medium
HEX #333333
20 pnts con 35 pnts de leading

Texto con un tamaño menor de 18 pnts, el contraste es de 4.5:1
Texto con un tamaño mayor de 18 pnts tiene que tener un contraste de 3:1.

Íconos

Los íconos a utilizarse serán basados en la biblioteca estándar de íconos, FontAwesome.com. Esto para mantener una estandarización en todos los portales del Gobierno de Puerto Rico.



Íconos Grandes
60 pixeles en su lado más corto

Íconos Medianos
45 pixeles en su lado más corto

Íconos Pequeños
30 pixeles en su lado más corto

Botones y Navegacíon

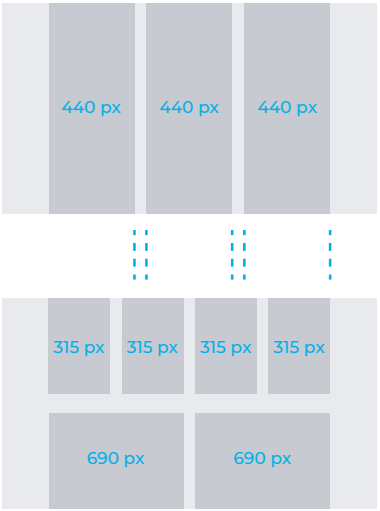
< ANTERIOR

SIGUIENTE >

Botones que requieran presionarse deben tener una altura de 70 px máx / 60 px min. El largo va a depender del texto o función que dicho botón tenga designado. Debe existir una separación entre cada botón. Debe distinguirse con el uso de colores cuál es el botón que se presionaría para un próximo paso La función de cada botón se distinguirá con el uso de colores, indicando la funcionalidad de cada uno.

Cuadrícula Base

Utilizar como base un Grid de 3 columnas de 440 px cada una con un separación (*padding*) de 60 px entre ellas para ocupar un espacio de 1,440 px en total.

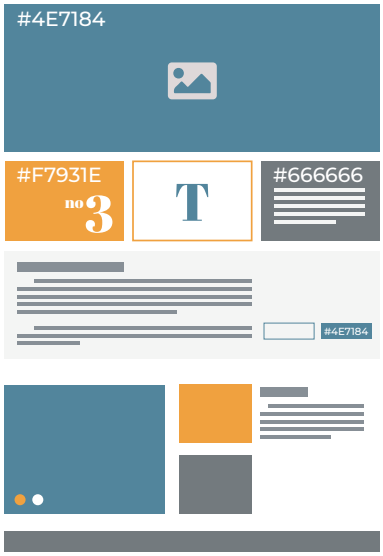


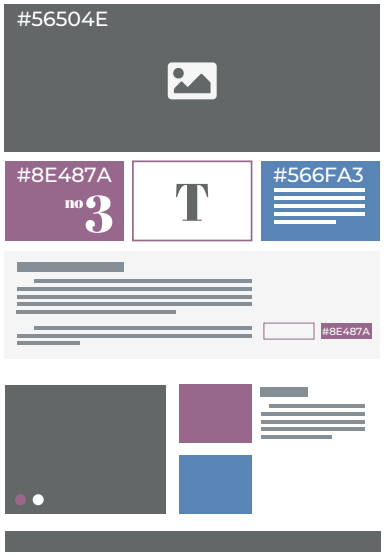
Cuando lo amerite, el grid se ajustará a 4 columnas de 315 px de ancho c.u. con una separación de 60 px ó 2 columnas de 690 px c.u. con una separación de 60 px

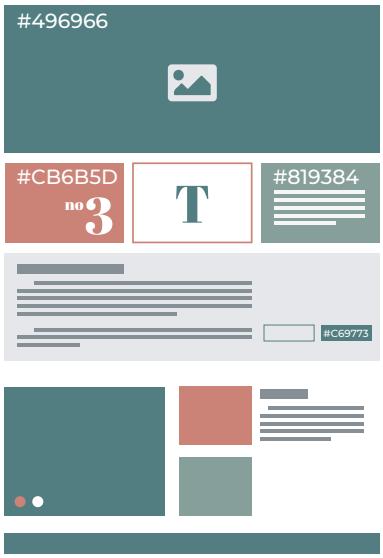
El esquema de colores puede variar dependiendo del diseño particular de cada portal. Los colores aquí mostrados son sugerencias basadas en distintios análisis realizados por PRITS. Estas combinaciones de colores han sido escogidas específicamente para que el diseño del portal esté fuera de cualquier interpretación de índole político-partidista.

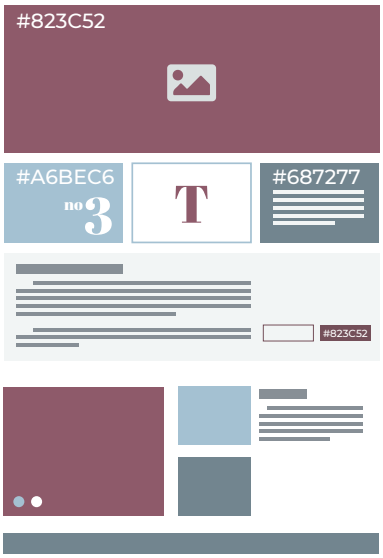
El esquema de colores final dependerá del "look and feel" particular de cada agencia y el diseño que se trabaje para la misma. Todo esquema de colores propuestos deben ser evaluados y aprobados por PRITS.

Esquema de Colores









Todo portal será identificado con el logo oficial del Gobierno de Puerto Rico en conjunto al nombre de la Agencia correspondiente según establecido en el Manual de Identidad del Gobierno de Puerto Rico.

PUERTO RICO INNOVATION & TECHNOLOGY SERVICE

TECNOLOGÍA

Todas las páginas deben mostrar el "breadcrumbing" dentro del portal

BÚSQUEDA

Introducción

Sobre la Agencia y sus servicios

Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat.

Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi.

Anuncios, promociones, ofertas, etc. (relacionados o no a la agencia) deberán ser todos del mismo tamaño y ubicados dentro de un carrusel que no ocupe un área mayor de una columna. Esta sección es para elementos que no requieran una página adicional.

Noticias, anuncios y avisos

Información adicional

Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi.

Lorem ipsum dolor sit amet, cons ectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat.

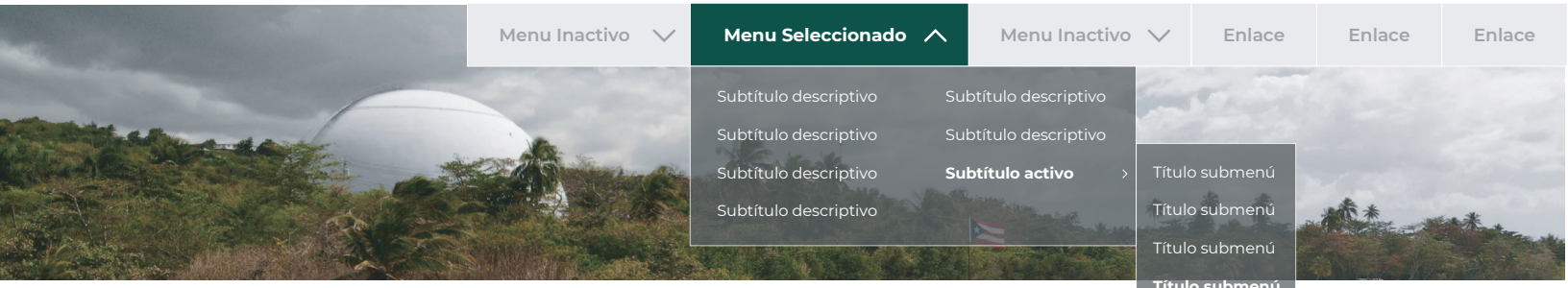
Portal oficial del Gobierno de Puerto Rico.

Un sitio web oficial .pr.gov pertenece a una organización oficial del Gobierno de Puerto Rico.

Los sitios web seguros .pr.gov usan HTTPS, lo que significa que usted se conectó de forma segura a un sitio web.

PUERTO RICO INNOVATION & TECHNOLOGY SERVICE

Todo portal será identificado en la parte superior con una barra explicativa de cómo identificar un portal oficial del Gobierno de Puerto Rico. Esta barra se expane para dar más información al respecto.



Home > Beneficios Federales > Programas de Asistencia > Programa de Alimento a Estudiantes

Descripción de Servicio

La navegación se mantendrá estándar a través de todos los portales. Cuando la cantidad de enlaces sea extensa, la navegación se desplegará de manera horizontal para evitar listados de enlaces fuera del marco de visibilidad del navegaor.

Descripción del Servicio

Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi.

Lorem ipsum dolor sit amet, cons ectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat.

SOLICITAR

Descripciones de servicios (o similares) utilizarán el ancho completo de las 3 columnas. Servicios cuyas descripciones sean muy cortas o el contenido no sea el suficiente, éstos no ameritan páginas independientes. Si este es el caso, evaluar el uso de otros elementos como las Tarjetas o agrupar información similar con secciones de Acordeones Multiseleccionables. Incluir botones si el servicio requiere hacer alguna connección a un portal externo el cual debe abrir en una pastaña separada a la actual para no cerrar la sessión del portal actual.

Información

Title lorem ipsum dolor sit amet

Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi.

Title lorem ipsum dolor sit amet

Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat.

Title lorem ipsum dolor sit amet

Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat.

Servicios

Todas las tarjetas que hablen de un tema en específico el cual amerite una página nueva dentro del portal deberá tener solo la información necesaria y un “Call to Action / CTA” que lleve a esa página por separado, de esta manera se evita sobrecargar de información la pantalla actual.

Card Title lorem ipsum dolor sit amet

Secundary Information

Card description Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

CTA / Link

Card Title lorem ipsum dolor sit amet

Secundary Information

Card description Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

CTA / Link

Card Title lorem ipsum dolor sit amet

Secundary Information

Card description Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

Las tarjetas pueden ir acompañadas por fotos, ilustraciones o videos. También se pueden trabajar en colores sólidos que vayan con el tema del diseño escogido para la Agencia. Siempre hay que tomar en consideración el contraste entre el texto y el color de fondo que se utilice. Si el fondo del texto es una imágen, esta no puede interferir en la legibilidad del texto que esté sobre la mismo.

Card Title lorem ipsum dolor sit amet

Secundary Information

Card description Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

CTA / Link

Card Title lorem ipsum dolor sit amet

Secundary Information

Card description Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

CTA / Link

Card Title lorem ipsum dolor sit amet

Secundary Information

Card description Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

CTA / Link

Card Title lorem ipsum dolor sit amet

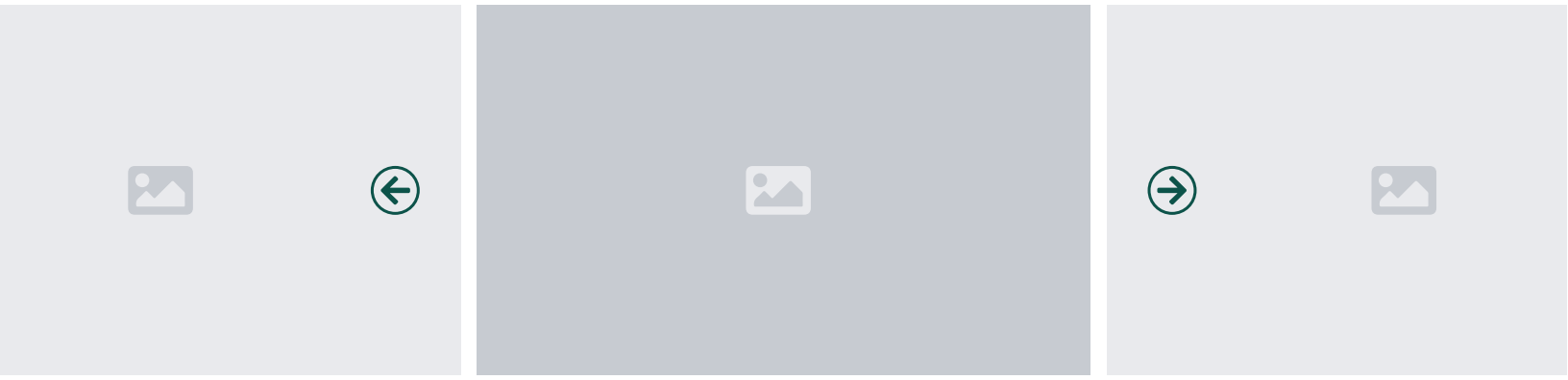
Secundary Information

Card description Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

CTA / Link

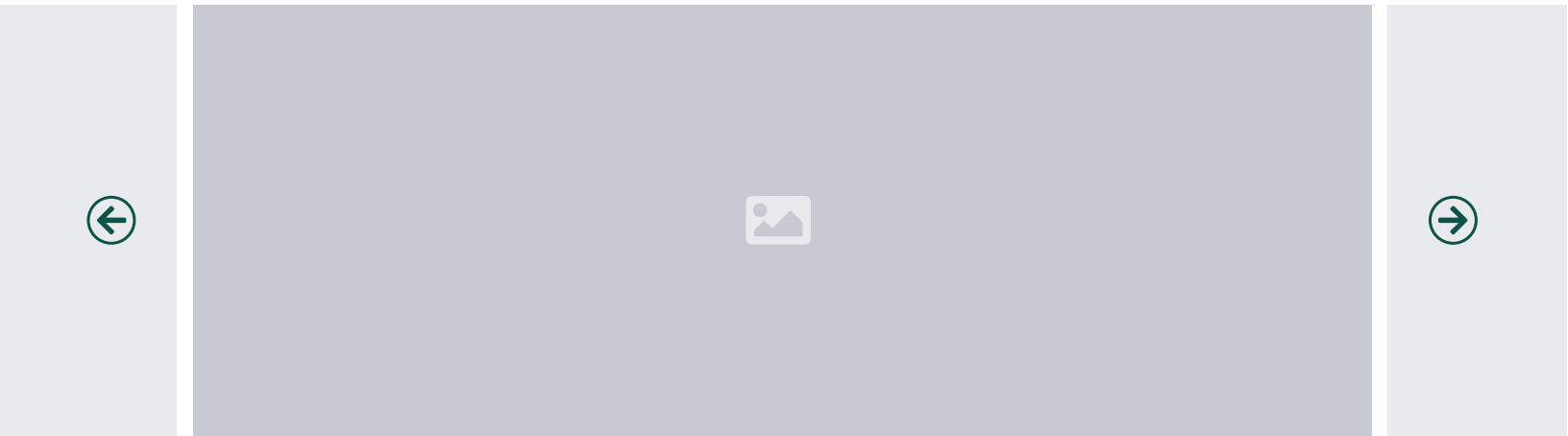
Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat.

Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis.



Title lorem ipsum dolor sit amet

Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio.



Las galerías de fotos se trabajarán a modo de carrusel, esto evitará la saturación de imágenes en los portales cuando los temas sean parecidos. En casos de galerías de fotos de eventos particulares, es responsabilidad de la Agencia hacer un escogido conciso de las imágenes a ser publicadas para así hacer que la experiencia del usuario sea más agradable.

Documentos

BÚSQUEDA DE DOCUMENTO

ORGANIZAR POR NOMBRE ↑↓

Forma #000000
Descripción oficial del documento gubernamental

Nombre del Documento
Descripción oficial del documento gubernamental

Forma #000000
Descripción oficial del documento gubernamental

Forma #000000
Descripción oficial del documento gubernamental

Nombre del Documento
Descripción oficial del documento gubernamental

Nombre del Documento
Descripción oficial del documento gubernamental

Forma #000000
Descripción oficial del documento gubernamental

Forma #000000
Descripción oficial del documento gubernamental

Forma #000000
Descripción oficial del documento gubernamental
Descargar

Forma #000000
Descripción oficial del documento gubernamental
Descargar

Forma #000000
Descripción oficial del documento gubernamental
Descargar

< ANTERIOR

SIGUIENTE >

Cuando el servicio es acompañado por formularios o documentos, se proveerán los mismos junto a la información general del servicio y con toda la información necesaria para identificar de manera inmediata dicho formulario o documento. Acompañar e identificar claramente algún ícono o botón de descarga para provocar esta acción de parte del usuario.

Lorem ipsum dolor sit amet

Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat.

Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, dignissim qui blandit praesent luptatum.

Imágenes o videos de gran importancia que se deseen utilizar para resaltar algún tema, pueden sobrepasar el sistema de columnas establecido en las guías, siempre y cuando se tome en consideración el ajuste de las pantallas (desktop vs mobile).

Todo video tiene que tener la capacidad de activarse dentro del mismo portal y no salir a páginas externas. Ningún video debe empezar de manera automática, excepto que el audio esté desabilitado.

Procesos y Formas

Paso #1 Lorem ipsum

Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit.

Paso #2 Lorem ipsum

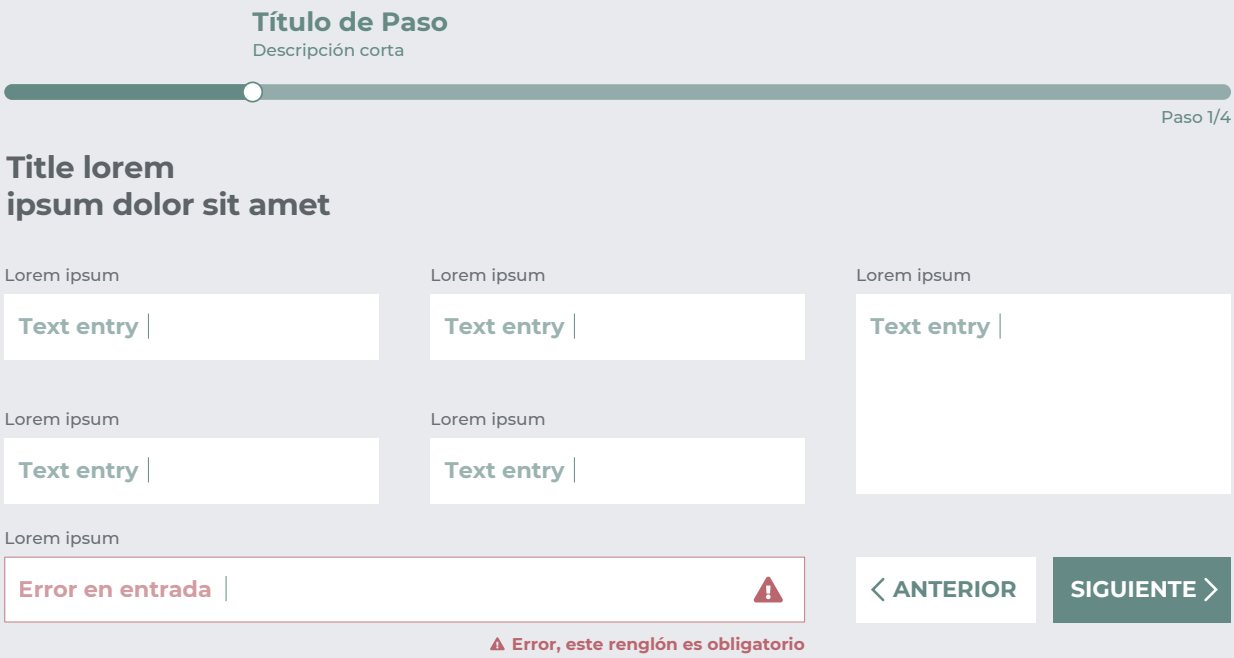
Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit.

- Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh.
- Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh.
- Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh.

Paso #3 Lorem ipsum

Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit.

Todo proceso que se necesite completar dentro del portal requiere una explicación concisa de los pasos a seguir para así orientar de manera eficiente al cuidadano. De esta manera se evita la confusión en los pasos a seguir para completar formularios.



Como buena práctica en la experiencia del usuario, cuando se llenan encasillados de manera errónea o se dejan sin completar renglones obligatorios, el usuario debe tener una visualización de que el encasillado necesita atención o ser completado.

Formas

Title lorem ipsum dolor sit amet

Lorem ipsum
Text entry

Lorem ipsum
Text entry

Lorem ipsum
Text entry

Lorem ipsum
Text entry

Lorem ipsum
Text entry

Lorem ipsum
Text entry

ANTERIOR

SIGUIENTE

Acordeones

- Enlace Principal
- **Enlace Principal**
  - Enlace Secundario
  - Enlace Secundario
    - Enlace Terciario
    - Enlace Terciario
    - Enlace Terciario
      - **Enlace Actual**
- Enlace Principal
- Enlace Principal

Multiselectable Acordion lorem ipsum +

Multiselectable Acordion lorem ipsum +

Multiselectable Acordion lorem ipsum —

Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi.

Lorem ipsum dolor sit amet, cons ectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat.

Multiselectable Acordion lorem ipsum +

Se utilizarán acordeones multi-seleccionables en los casos que se necesite proveer información extensa sobre múltiples temas. Estos acordeones permiten expander o reducir el texto, de esta manera darle al usuario más control de la información que va a consumir, sin la necesidad de que se vea cargado el portal.

Catálogo de Documentos

BÚSQUEDA DE DOCUMENTO

ORGANIZAR POR NOMBRE ↑↓

Título del Documento	Descripción	Año
Título del Documento	Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis.	Año
Título del Documento	Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis.	Año
Título del Documento	Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis.	Año
Título del Documento	Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis.	Año
Título del Documento	Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis.	Año
Título del Documento	Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis.	Año

< ANTERIOR   SIGUIENTE >   1 / 12 páginas

- Enlace Principal
- **Enlace Principal**
  - Enlace Secundario
  - Enlace Secundario
    - Enlace Terciario
    - Enlace Terciario
    - Enlace Terciario
    - **Enlace Actual**
- Enlace Principal
- Enlace Principal

Título del Documento

- Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis.
- Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis.
- Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis.
- Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis.
- Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis.
- Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis.
- Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis.

Este tipo de módulos se utilizarán cuando la Agencia necesita proveer al ciudadano un catálogo extenso de documentos, formularios, leyes, guías, cartas, memorandos, órdenes administrativas, etc. En estos casos es extremadamente importante proveer un sistema de navegación o búsqueda que facilite el encontrar estos documentos. Con el uso de paginación (según se requiera) se evitarán el uso de listas interminables

Equipo de Trabajo

Nombre Apellidos
Posición que ocupa dentro de la agencia.

Nombre Apellidos
Posición que ocupa dentro de la agencia.

Nombre Apellidos
Posición que ocupa dentro de la agencia.

Nombre Apellidos
Posición que ocupa dentro de la agencia.

Persona destacada (ej. Director/a Ejecutivo/a)

Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat.

Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi.

Nombre Apellidos
Posición que ocupa dentro de la agencia.

Nombre Apellidos
Posición que ocupa dentro de la agencia.

Nombre Apellidos
Posición que ocupa dentro de la agencia.

Nombre Apellidos
Posición que ocupa dentro de la agencia.

Nombre Apellidos
Posición que ocupa dentro de la agencia.

Nombre Apellidos
Posición que ocupa dentro de la agencia.

Contáctenos

Lorem ipsum

Text entry |

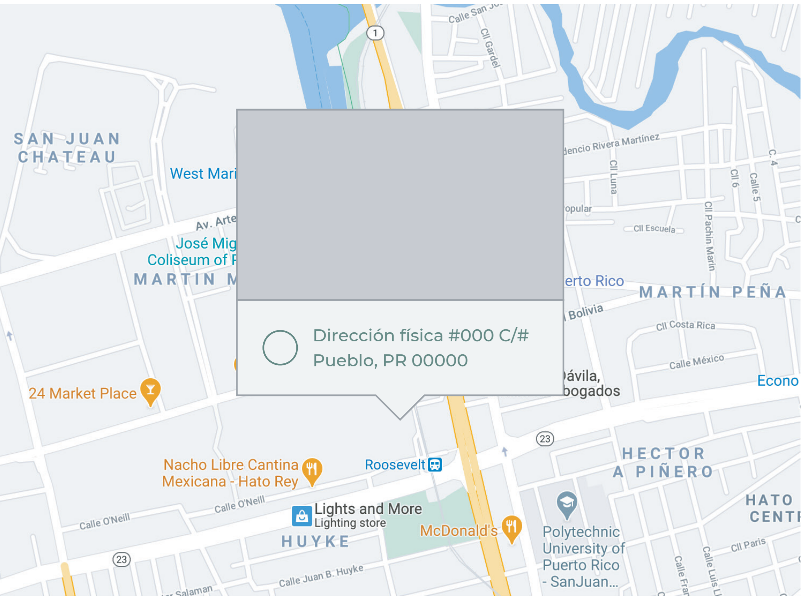
Lorem ipsum

Text entry |

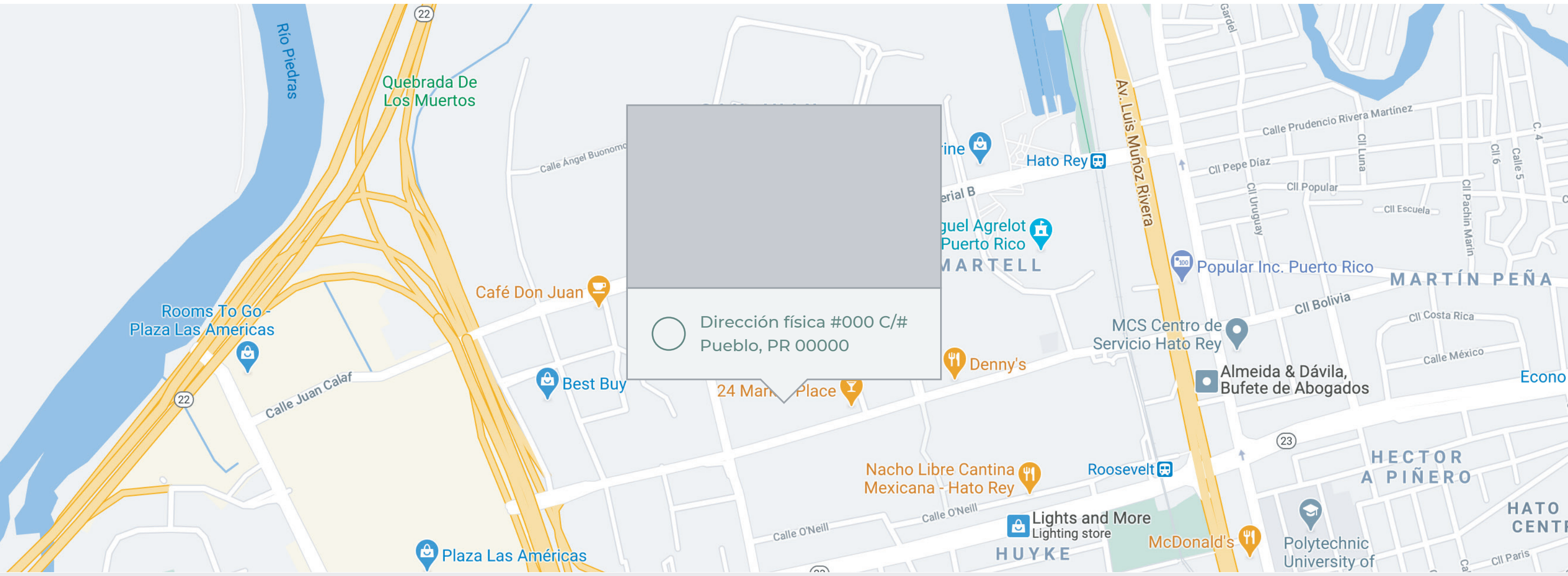
Lorem ipsum

Text entry |

< ANTERIOR   SIGUIENTE >



Cuando existen múltiples opciones de Oficinas con información propia, el mapa de localización debería cambiar dependiendo de la oficina o dependencia que se ecoja.



Oficina Central
Dirección física #000 C/#
Pueblo, PR 00000

tel. (787) 000-0000

Oficina Regional
Dirección física #000 C/#
Pueblo, PR 00000

tel. (787) 000-0000

Oficina Regional
Dirección física #000 C/#
Pueblo, PR 00000

tel. (787) 000-0000

Oficina Regional
Dirección física #000 C/#
Pueblo, PR 00000

tel. (787) 000-0000

Oficina Regional
Dirección física #000 C/#
Pueblo, PR 00000

tel. (787) 000-0000

Oficina Regional
Dirección física #000 C/#
Pueblo, PR 00000

tel. (787) 000-0000

Oficina Regional
Dirección física #000 C/#
Pueblo, PR 00000

tel. (787) 000-0000

Oficina Regional
Dirección física #000 C/#
Pueblo, PR 00000

tel. (787) 000-0000

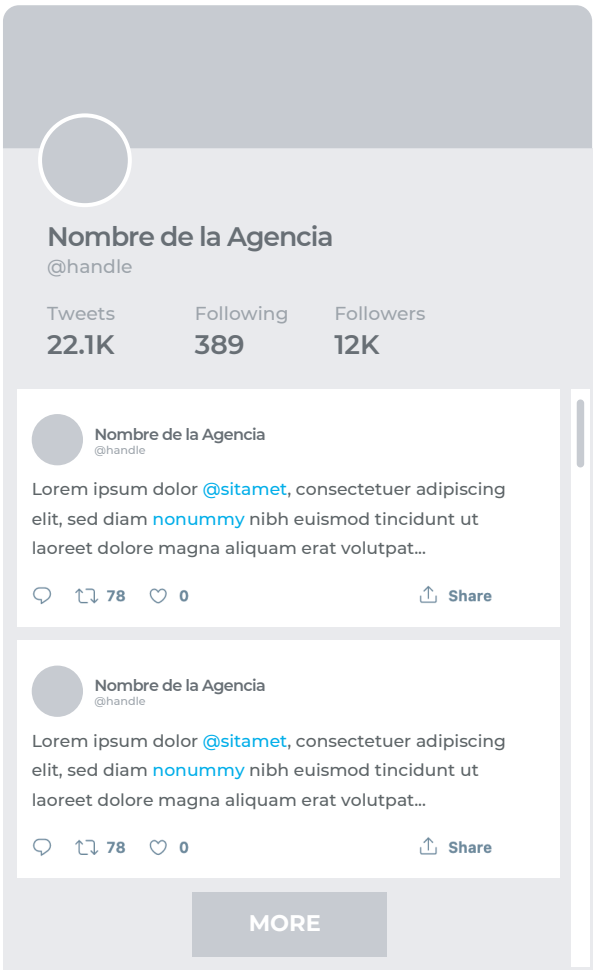
Toda Alerta debe ocupar el ancho completo de la pantalla, es de las pocas variaciones en que se rompa con el sistema de 3 columnas para darle énfasis sobre cualquier otro elemento que esté presente en la página.

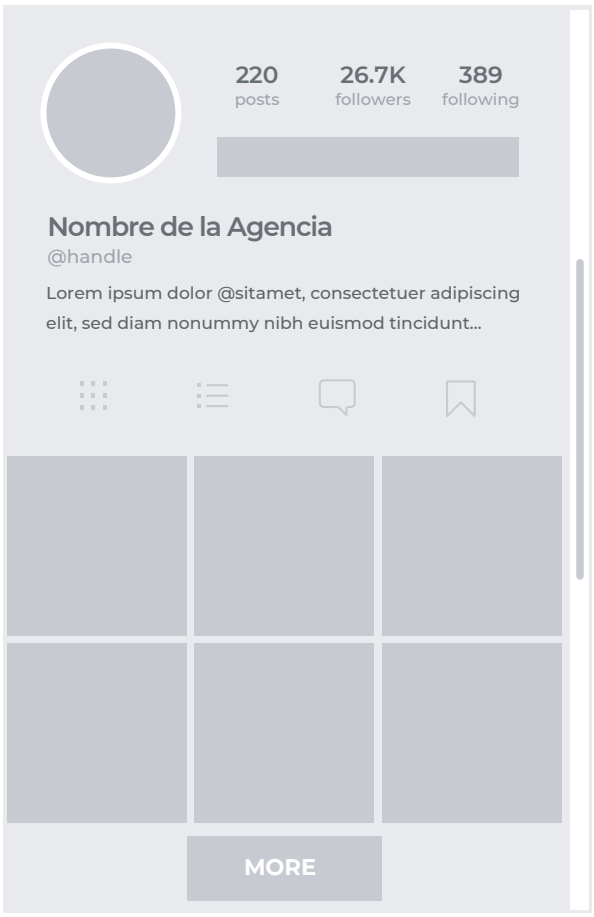
Alerta o Comunicación lorem ipsum
Descripción corta y concisa del tipo de alerta y lo que se quiere informar de manera inmediata.

Alerta o Comunicación lorem ipsum
Descripción corta y concisa del tipo de alerta y lo que se quiere informar de manera inmediata.

Social Media Feeds deben estar al final de la página especialmente si se contempla el desplazamiento infinito (el cuál no es recomendado). De ésta manera se evitan problemas mayores a las personas no videntes con lectores de pantalla. Estos alimentadores deberán tener un límite de desplazamiento automático para evitar el “infinite scroll”. El tamaño recomendado es de una columna en una cuadrícula de 2 columnas (caso especial).

Los alimentadores de medios sociales sirven para tener una presencia en la página. El consumo de la información en general debe darse en la application o website del medio social, no del portal de la Agencia.





Todo portal utilizará el footer oficial de los Portales del Gobierno de PR con su información básica y enlaces.

Contact Agency

Dirección física #000 C/#
Pueblo, PR 00000

emailoficial@agencia.pr.gov

tel. (787) 000-0000

Social Media

pr.gov

Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat.