MINISTERIO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES

GOBIERNO DE COSTA RICA

CÓDIGO NACIONAL DE

TECNOLOGÍAS DIGITALES

MICITT

2026

Control de versiones

Fecha	Versión	Autores	Aprobado	Descripción
16-02-2020	1.0	Colaboradores indicados en la página 7 MICITT Luis Diego Vega Rojas	Jorge Mora Flores, Director de Gobernanza Digital	Oficialización y entrada en vigencia.
18-07-2021	2.0	Edgar Mora Erick David Mora Alvarado Jorge Mora Flores	Jorge Mora Flores, Director de Gobernanza Digital	Se corrige en la tabla de control de cambios en la casilla de autores de la versión 1.0. Se actualiza el contenido acerca del CNTD. Se incorpora en el capítulo de Interoperabilidad el Marco de Interoperabilidad Nacional. Se actualiza el nombre del MICITT.
28-01-2022	3.0	Dayanna Mejía Estefani Valverde Rojas Jorge Mora Flores	Jorge Mora Flores, Director de Gobernanza Digital	Se ajusta la información acerca de la instancia encargada en otorgar el Sello de Gobierno Digital. Se incorporan herramientas para verificar el cumplimiento en cada capítulo. Se incorpora el nombre de una persona colaboradora en la versión 1.0, que se omitió por un error material.
08-04-2022	3.1	Dayanna Mejía	Paula Brenes, Director de Gobernanza Digital	Se ajusta la información acerca de la instancia encargada en otorgar el Sello de Gobierno Digital.
01-02-2023	3.2.	CyberSec Clúster	Paula Brenes, Director de Gobernanza Digital	Se ajusta la información de los capítulos de Identificación y Autenticación Ciudadana y Seguridad Tecnológica, Seguridad de la Información y Ciberseguridad.
16-10-2023	4	Dayanna Mejía	Aldo González Miranda, Director de Gobernanza Digital y Certificadores de firma digital	Se ajusta e incluye información en la sección de antecedentes, equipo de trabajo, así como en los capítulos de Seguridad Tecnológica (con base en insumos recibidos por CyberSec Clúster) e Interoperabilidad. Se

Fecha	Versión	Autores	Aprobado	Descripción
				actualizan logos del Ministerio y nombre de la Dirección. Se ajusta forma en todo el documento.
8-01-2024	4.1	Erick David Mora	Aldo González Miranda, Director de Gobernanza Digital y Certificadores de Firma Digital	Se ajusta e incluye información en las secciones: Capitulo 1 Accesibilidad Digital Usabilidad y experiencia de usuario, Capitulo 3 Seguridad Tecnológica, seguridad de la Información & Ciberseguridad, Capitulo 6 Neutralidad Tecnológica, (con base en los insumos obtenidos de la consulta pública no vinculante del presente documento, posterior a la revisión, análisis aprobación por parte de los responsables correspondientes, según la temática. Se ajustaron las fechas del documento.
15-01-2024	4.1		Gezer Ramiro Molina Colomer, Director Nacional de Ciberseguridad	Se ajusta y se incluye información al Capítulo 3 Seguridad Tecnológica, seguridad de la información y ciberseguridad.
24-10-2024	5	Antonette Williams Barnett Margarita Vargas Ramos Orlando Vega Quesada Marlon Ávalos Elizondo Diego Leiva Dayanna Mejía	Marlon Ávalos Elizondo, Director de Investigación, Desarrollo e Innovación	Inclusión de capítulo 7 - Inteligencia Artificial Se actualiza la versión y texto indicados para el PNDT y la Directriz del capítulo 1 de accesibilidad.
30-04-2026	6	Rosa Zúñiga Quesada César Díaz	Diego Leiva Alfaro Director de Gobernanza Digital y Certificadores de Firma Digital Francisco Troyo Rodríguez, Director de Espectro Radioeléctrico y Redes de Telecomunicaciones	Inclusión del capítulo 8 – Implementación del Protocolo de Internet IPv6 en el Sector Público Costarricense.

Aprobado por

Diego Antonio Leiva Alfaro
Director de Gobernanza Digital y Certificadores de Firma Digital

Ultima actualización

Francisco Troyo Rodríguez
Director de Espectro Radioeléctrico y Redes de Telecomunicaciones

Contenido

EQUIPO DE TRABAJO

Accesibilidad digital, usabilidad y experiencia de usuario
Karla Araya – CONAPDIS
Raquel Cantillo - MICITT
Mario Chacón - TEC, INCLUTEC
Eduardo Eduarte Vásquez - CONAPDIS
Luis Carlos Naranjo - TEC, INCLUTEC
Keren Ramírez Acosta - Asesora independiente

Identificación y autenticación ciudadana

Gabriel Alcázar - Registro Nacional
Miguel Carballo - BCCR
Patricia Chacón - TSE
Dayanna Mejía - MICITT
Óscar Solís - ICT

Seguridad Tecnológica
Ana María Castro - CCSS
Mario Robles - White Jaguars
Marvin Soto - Cybercom CR

Infraestructura y tecnología en la Nube
Job Céspedes – UCR
Ricardo Villalón - UCR
Roberto Lemaitre - MICITT
Edgar Mora - MICITT

Interoperabilidad
Marco Jiménez - UCR
Edgar Mora – MICITT
Erick David Mora Alvarado – MICITT
Jorge Mora – MICITT
Aldo González – MICITT

Neutralidad tecnológica
Roberto Lemaitre – MICITT
Mauricio Oviedo – SOCIUM
Glenn Peace – NIC-CR

Inteligencia Artificial
Antonette Williams Barnett – MICITT
Margarita Vargas Ramos – MICITT
Orlando Vega Quesada – MICITT
Marlon Ávalos Elizondo – MICITT

Implementación del Protocolo de Internet IPv6 en el Sector Público Costarricense

Rosa Zúñiga Quesada – MICITT
César Díaz – LACNIC

*Se aclara que la institución indicada para cada persona responde al momento en el cual la persona colaboró en la construcción o mejora del documento y no necesariamente las personas se encuentran actualmente en dichas entidades.

ANTECEDENTES

La Presidencia de la República ha posicionado la Transformación Digital del Estado dentro de sus prioridades como una forma de potenciar el ejercicio de los derechos y las responsabilidades, la innovación y el desarrollo de la ciudadanía a través de una concepción de gestión pública acorde con los principios del Gobierno Abierto, es decir, un Gobierno centrado en la transparencia, la accesibilidad y la simplificación para ofrecer servicios de mayor calidad a sus ciudadanos.

Debido al motivo recién mencionado, el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) emite la Estrategia de Transformación Digital, con la intención de definir las acciones en esta materia que se recomiendan, incorporando trabajo conjunto con otras entidades del Sector Público, el Sector Privado y la Academia para hacer efectivo un avance en la digitalización en el periodo definido.

El Sello de gobierno Digital responde a uno de estos lineamientos. Dicho sello se trata de una aprobación otorgada por la Comisión de Alto Nivel en colaboración con una secretaría técnica, a instituciones que sometan a análisis un determinado proyecto y este cumpla con lo definido en el Código Nacional de Tecnologías Digitales (CNTD), además de que evidencie el impacto que tendrá su implementación a nivel nacional. Si se brinda el Sello de Gobierno Digital a un proyecto, la Comisión de Alto Nivel de Gobierno Digital sugerirá su priorización dentro de la Cartera Nacional de Proyectos de Gobierno Digital. Una vez que es implementado, en el caso de los servicios digitales al ciudadano, la Dirección de Gobernanza Digital y Certificadores de firma digital (DGDCFD) realizará el proceso correspondiente para registrarlo en el Portal Nacional de Gobierno Digital (https://gob.go.cr).

Así, ante la necesidad de definir los criterios que utilizará la Comisión de Alto Nivel de Gobierno Digital para valorar objetivamente los proyectos que aspiran obtener este sello, y con la intención de ir formando el camino para una transformación digital en el sector público, surge este documento, el cual hace referencia a los principios que deben tomar en cuenta las instituciones a la hora de planificar un proyecto tecnológico.

ACERCA DEL CÓDIGO NACIONAL DE TECNOLOGÍAS DIGITALES

¿Qué es el Código Nacional de Tecnologías Digitales?

La ETD define el CNTD como un compendio de buenas prácticas que establecen los mínimos deseables para la adquisición, desarrollo y gestión de las tecnologías y los servicios digitales en el sector público costarricense.

¿Para qué funciona?

Su importancia y su propósito residen en brindar los criterios técnicos básicos que todo proyecto digital debe contemplar para su desarrollo dentro de las instituciones de la administración pública. El CNTD es también la guía base para que la Comisión de Alto Nivel de Gobierno Digital y la Secretaría Técnica puedan valorar objetivamente los proyectos tecnológicos de importancia nacional y de cumplir con los criterios expuestos, puedan contar con el Sello de Gobierno Digital.

En última instancia, esto posibilitará la estandarización de un marco de referencia que les permitirá a las Instituciones Públicas brindar servicios digitales de calidad, lo cual se traduce en eficiencia y eficacia, generando facilidades a los usuarios y así un mayor bienestar para la población costarricense.

Aplicación al Sello de Gobierno Digital

Tanto la Comisión de Alto Nivel de Gobierno Digital como una institución interesada pueden proponer una iniciativa de Gobierno Digital para su posible implementación. La institución revisa la iniciativa y construye la propuesta con base en lo estipulado por el CNTD, y luego la Dirección de Gobernanza Digital y Certificadores de firma digital del MICITT evalúa el cumplimiento o no de dichos criterios técnicos. Cada uno de los capítulos tiene una serie de herramientas que le ayudarán a las instituciones poder autoevaluar su cumplimiento y que serán utilizadas por la DGD parala evaluación de cada propuesta que solicite el Sello de Gobierno Digital.

De cumplir con los requisitos, la DGDCFD le otorga el Sello de Gobierno Digital a la propuesta de proyecto y se procede a comunicar a la institución. A continuación, la Comisión de Alto Nivel de Gobierno Digital evalúa el proyecto y recomienda priorizar dentro de la Cartera

Nacional de Proyectos en Gobierno Digital. Entonces la DGDCFD registra el proyecto en la Cartera.

Cabe agregar que, en el caso de concluir y completar un proyecto concerniente con los servicios digitales al ciudadano, la DGDCFD además lo ha de registrar en el Portal Nacional de Gobierno Digital.

En las páginas siguientes se encuentran los capítulos que contienen cada uno de los siete temas que dan sustento al CNTD, en cada uno de estos viene una lista de políticas generales y políticas específicas cuyo cumplimiento será necesario correspondientemente a la hora de definir por parte de la Comisión de Alto Nivel en conjunto con la asesoría de la Dirección de Gobernanza Digital y Certificadores de firma digital, si una institución está en condiciones de recibir el Sello de Gobierno Digital.

Los temas que serán desarrollados con posterioridad se enumeran a continuación:

1. Accesibilidad, Usabilidad y Experiencia de Usuario.
2. Identificación y Autenticación Ciudadana.
3. Seguridad Tecnológica.
4. Infraestructura y Tecnología en la Nube.
5. Interoperabilidad.
6. Neutralidad Tecnológica.
7. Inteligencia Artificial.

¿Hacia dónde vamos?

- Potenciar el aprovechamiento eficiente de las capacidades y los datos del Estado para facilitar la prestación de servicios ciudadanos
- Mejorar la calidad de los trámites y servicios de gobierno digital
- Mejorar la resiliencia de los servicios digitales frente a los riesgos tecnológicos
- Mejorar la gestión de los procesos de adquisición de tecnologías en el Estado
- Facilitar la accesibilidad e interacción de los usuarios con servicios estandarizados

OBJETIVO

Establecer las mejores prácticas aplicadas a la gestión de iniciativas y proyectos que incorporen componentes de tecnologías de información y comunicaciones a nivel nacional en el sector público, que generen una inclusión digital en los servicios digitales del Estado.

ALCANCE

Este documento presenta pautas para el desarrollo de proyectos tecnológicos en el sector público costarricense que contemplen los temas mencionados anteriormente.

Se insta al sector privado y a la academia a tomarlas en consideración, toda vez que su implementación representa ganancia para todos los entes involucrados en el desarrollo del país, con especial importancia para el usuario final.

METODOLOGÍA

Para la elaboración del CNTD se conformó, por parte del MICITT, un grupo de trabajo interinstitucional integrado por expertos en el campo, tanto del Sector Público como del Privado. Dentro de las instituciones participantes se encuentran las siguientes: MICITT, UCR, BCCR, OWASP, NIC.CR, ICT, Intel, INCAE, CCSS, TSE, PRODHAB, Inclutec, CONAPDIS, Registro Nacional y FSecurity Academy. También se ha contado con la colaboración de pasantes universitarios que han contribuido con el desarrollo de este importante documento.

A su vez, se realizó una división en siete subgrupos para desarrollar cada uno de los temas que sustentan el Código: Accesibilidad, Usabilidad y Experiencia de Usuario; Identificación y Autenticación Ciudadana; Seguridad Tecnológica, Infraestructura y Tecnología en la Nube; Interoperabilidad; Neutralidad Tecnológica e Inteligencia Artificial.

Dichos subgrupos, partiendo de los lineamientos establecidos en la ETD, se encargaron de estudiar tanto las fuentes documentales disponibles en sus respectivas áreas, como las herramientas normativas presentes en el país en torno a Gestión Pública y Gobierno Digital, y también identificaron instrumentos ideados en los países líderes en lo relativo a digitalización del Gobierno. Con estos insumos a mano, cada equipo adaptó las mejores herramientas a la realidad nacional y se definieron estos principios para el desarrollo de proyectos en materia

de Gobierno Digital siguiendo un cronograma previamente establecido.

Cabe agregar que se definieron dos talleres generales para la versión 1.0: El primero de ellos tenía el propósito de dar seguimiento en conjunto a los avances de cada subgrupo, y el segundo fue concebido para pulir colectivamente los productos finales de cada equipo, así como para integrarlos dentro del documento final del CNTD.

Además, durante el año 2019 se contó con la colaboración de la Escuela de Ciencias Políticas de la Universidad de Costa Rica, por medio una pasantía que contribuyo con la elaboración del documento.

El CNTD también ha sido fortalecido en el capítulo de Interoperabilidad, gracias a una Cooperación Técnica de Instituto Latinoamericano y del Caribe de Planificación Económica y Social / Comisión Económica para América Latina y el Caribe (ILPES/CEPAL), brindada desde agosto del 2019 por medio de dos talleres de trabajo y durante el año 2020 y parte del 2021, por medio de una serie de sesiones de trabajo con 15 instituciones para definir la propuesta del Marco de Interoperabilidad Nacional.

Así mismo, a finales del año 2021 se contó con la colaboración de la Escuela de Administración Pública de la Universidad de Costa Rica, por medio una pasantía que contribuyo con la elaboración de las herramientas que permiten verificar el cumplimiento de cada capítulo del Código. Luego de recibir las herramientas, fueron enviadas para su revisión y ajustes a los miembros del grupo interinstitucional que participaron en la elaboración de la primera versión de este documento y se aplicaron los aportes sugeridos. Finalmente, en el año 2024 se incorpora el capítulo de inteligencia artificial.

Finalmente, se presenta a continuación un diagrama con metodología aplicada para el desarrollo del CNTD:

Ilustración 1. Elaboración propia, 2019.

MINISTERIO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES | GOBIERNO DE COSTA RICA

CAPÍTULO 1:

ACCESIBILIDAD DIGITAL, USABILIDAD Y EXPERIENCIA DE USUARIO

EQUIPO DE TRABAJO

Integrante	Institución
Karla Araya	CONAPDIS
Raquel Cantillo	MICITT
Mario Chacón	TEC, INCLUTEC
Eduardo Eduarte Vásquez	CONAPDIS
Luis Carlos Naranjo	TEC, INCLUTEC
Keren Ramírez Acosta	Asesora independiente
David Zamora	INCAE

INTRODUCCIÓN AL TEMA

El CNTD, en cumplimiento con la normativa nacional vigente y con respeto de los derechos humanos, contempla como una de sus líneas de estandarización el acceso universal de todas las personas, independientemente de su condición, a la información generada o adquirida por medios digitales, incluyendo escenarios en donde el intermediario podría ser un agente no humano (o humanoide), el cual produce y facilita información que será consumida por cualquier persona usuaria.

En este documento se especifican las pautas por considerar para el desarrollo de plataformas digitales accesibles y usables, partiendo de la experiencia de las personas usuarias, en concordancia con las leyes y políticas en los ámbitos relacionados con tecnología e inclusión, con el fin de generar un claro incremento en los niveles de satisfacción de todos los usuarios, incluyendo personas con alguna discapacidad.

Las pautas estipuladas en este documento responden a tres preguntas fundamentales:

- ¿Qué hay que hacer o no hacer?
- ¿Por qué hay que hacerlo o no hacerlo?
- ¿Cómo se hace o se evita?

Esta aclaración reviste gran relevancia, pues las preguntas sobre el cómo hacer o evitar algo podrían considerarse invasivas en las decisiones diarias de administración de tecnologías. Debido a ello, se establecerán pautas generales y normas que conformen la base estándar de esta línea. Queda fuera del ámbito de este documento recomendar marcas o tecnologías específicas.

PRINCIPIOS

Los Principios del Diseño Universal

El diseño universal se concibe para productos y entornos de tal manera que pueda ser utilizado por todas las personas, en la mayor medida posible, sin la necesidad de adaptación o diseño especializado (NCSU, 1997).

Son siete principios que pueden aplicarse para evaluar los diseños existentes, guiar el proceso de diseño y educar tanto a los diseñadores como a los consumidores sobre las características de los productos y entornos más utilizables, estos son:

Primer principio: Uso equitativo

El diseño es útil y comercializable para personas con capacidades diversas. Pautas:

1a. Proporcionar los mismos medios de uso para todos los usuarios siempre que sea posible, equivalentes cuando no.

1b. Sin discriminar a cualquier usuario.

1c. Las disposiciones de privacidad, y seguridad de la información deben estar igualmente disponibles para todos los usuarios.

1d. Alinearse a buenas prácticas o estándares de diseño para equilibrar la funcionalidad con la perspectiva estética.

Segundo principio: Flexibilidad en el uso

El diseño se adapta a una amplia gama de preferencias y necesidades individuales. Pautas:

2a. Proporcionar elección en los métodos de uso.

2b. Acomodar el acceso y uso de la mano derecha o izquierda.

2c. Facilitar la exactitud y precisión del usuario.

2d. Proporcionar adaptabilidad al ritmo del usuario.

Tercer principio: Uso simple e intuitivo

El uso del diseño es fácil de entender, independientemente de la experiencia del usuario, los conocimientos, las habilidades lingüísticas o el nivel de concentración actual.

Pautas:

3a. Eliminar la complejidad innecesaria.

3b. Ser coherente con las expectativas del usuario y la intuición.

3c. Acomodar una amplia gama de habilidades de alfabetización y lenguaje. 3d.

Organizar información acorde con su importancia.

3e. Proporcionar indicaciones y comentarios efectivos durante y después de la finalización de la tarea.

Cuarto principio: Información perceptible

El diseño comunica la información necesaria de manera efectiva al usuario, independientemente de las condiciones ambientales o las capacidades sensoriales del usuario.

Pautas:

4a. Utilizar diferentes modos (pictórico, verbal, táctil) para la presentación redundante de información esencial.

4b. Proporcionar contraste adecuado entre la información esencial y su entorno.

4c. Maximizar la "legibilidad" de la información esencial.4d. Diferenciar los elementos de manera que se puedan describir (es decir, facilitar el dar instrucciones).

4e. Proporcionar compatibilidad con una variedad de técnicas o dispositivos utilizados por personas con limitaciones sensoriales.

Quinto principio: Tolerancia al error

El diseño minimiza los peligros y las consecuencias adversas de acciones accidentales o involuntarias.

Pautas:

5a. Organizar los elementos para minimizar los peligros y errores: los elementos más utilizados, los más accesibles; elementos peligrosos eliminados, aislados o blindados.

5b. Proporcionar advertencias de peligros y errores. 5c. Proporcionar características a prueba de fallos.

5d. Desalentar la acción inconsciente en tareas que requieren vigilancia.

Sexto principio: Esfuerzo físico bajo

El diseño se puede usar de manera eficiente, cómoda y con un mínimo de fatiga. Pautas:

6a. Permitir al usuario mantener una posición del cuerpo neutral. 6b. Usar fuerzas operativas razonables.

6c. Minimizar acciones repetitivas.

6d. Minimizar el esfuerzo físico sostenido.

Sétimo principio: Tamaño y espacio para aproximación y uso

Se proporciona el tamaño y el espacio apropiados para aproximación, alcance, manipulación y uso independientemente del tamaño corporal, la postura o la movilidad del usuario.

Pautas:

7a. Proporcionar una línea de visión clara de los elementos importantes para cualquier usuario sentado o de pie.

7b. Hacer que todos los componentes sean cómodos para cualquier usuario sentado o de pie.

7c. Acomodar variaciones en mano y tamaño de agarre.

7d. Proporcionar espacio adecuado para el uso de dispositivos de asistencia o asistencia personal.

Hay que tener en cuenta que los Principios del Diseño Universal se refieren únicamente al diseño de uso universal, mientras que la práctica del diseño implica más que una consideración por la facilidad de uso. Los diseñadores también deben incorporar otras consideraciones como las preocupaciones económicas, de ingeniería, culturales, de género y ambientales en sus procesos de diseño. Estos Principios ofrecen orientación a los diseñadores para integrar mejor las funciones que satisfacen las necesidades de tantos usuarios como sea posible.

Se trata de un campo multidisciplinario, caracterizado por un bajo nivel de consenso en cuanto a las áreas que cubre y bajo cuáles principios se rige. Es claro, no obstante, que se relaciona directamente con las percepciones del usuario. Para efectos de este documento, se partirá precisamente de esta concepción de UX en relación directa con las percepciones.

Se ha elaborado la siguiente herramienta de control para guiar el cumplimiento de los principios del diseño universal:

Herramienta para verificar el cumplimiento de los principios del diseño universal				
Fecha de aplicación:				
Principio	**Definición**			
Uso equitativo	El diseño es útil y comercializable para personas con capacidades diversas.			
Pautas		**¿Cumple?**		**Acción por Realizar**
		Sí	**No**	
1a	Proporcionar los mismos medios de uso para todos los usuarios siempre que sea posible, equivalentes cuando no.			
1b	Evitar segregar o estigmatizar a cualquier usuario.			
1c	Las disposiciones de privacidad, seguridad de la información deben estar igualmente disponibles para todos los usuarios.			
1d	Hacer el diseño atractivo para todos los usuarios.			
Flexibilidad en el uso	El diseño se adapta a una amplia gama de preferencias y habilidades individuales.			

Pautas		¿Cumple?		Acción por realizar
		Sí	No	
2a	Proporcionar elección en los métodos de uso.			
2b	Acomodar el acceso y uso de la mano derecha o izquierda.			
2c	Facilitar la exactitud y precisión del usuario.			
2d	Proporcionar adaptabilidad al ritmo del usuario.			
Uso simple e intuitivo	El uso del diseño es fácil de entender, independientemente de la experiencia del usuario, los conocimientos, las habilidades lingüísticas o el nivel de concentración actual.			
Pautas		**¿Cumple?**		**Acción por realizar**
		Sí	**No**	
3a	Eliminar la complejidad innecesaria.			
3b	Ser coherente con las expectativas del usuario y la intuición.			
3c	Acomodar una amplia gama de habilidades de alfabetización y lenguaje.			
3d	Organizar información acorde con su importancia.			
3e	Proporcionar indicaciones y comentarios efectivos durante y después de la finalización de la tarea.			
Información perceptible	El diseño comunica la información necesaria de manera efectiva al usuario, independientemente de las condiciones ambientales o las capacidades sensoriales del usuario.			
Pautas		**¿Cumple?**		**Acción por realizar**
		Sí	**No**	
4a	Utilizar diferentes modos (pictórico, verbal, táctil) para la presentación redundante de información esencial.			
4b	Proporcionar contraste adecuado entre la información esencial y su entorno.			
4c	Maximizar la "legibilidad" de la información esencial.			
4d	Diferenciar los elementos de manera que se puedan describir (es decir, facilitar el dar instrucciones).			

4e	Proporcionar compatibilidad con una variedad de técnicas o dispositivos utilizados por personas con limitaciones sensoriales.			
Tolerancia al error	El diseño minimiza los peligros y las consecuencias adversas de acciones accidentales o involuntarias.			
Pautas		**¿Cumple**		**Acción por realizar**
		Sí	**No**	
5a	Organizar los elementos para minimizar los peligros y errores: los elementos más utilizados, los más accesibles; elementos peligrosos eliminados, aislados o blindados.			
5b	Proporcionar advertencias de peligros y errores.			
5c	Proporcionar características a prueba de fallos.			
5d	Desalentar la acción inconsciente en tareas que requieren vigilancia.			
Esfuerzo físico bajo	El diseño se puede usar de manera eficiente, cómoda y con un mínimo de fatiga.			
Pautas		**¿Cumple?**		**Acción por realizar**
		Sí	**No**	
6a	Permitir al usuario mantener una posición del cuerpo neutral.			
6b	Usar fuerzas operativas razonables.			
6c	Minimizar acciones repetitivas.			
6d	Minimizar el esfuerzo físico sostenido.			
Tamaño y espacio para aproximación y uso	Se proporciona el tamaño y el espacio apropiados para aproximación, alcance, manipulación y uso independientemente del tamaño corporal, la postura o la movilidad del usuario.			
Pautas		**¿Cumple?**		**Acción por realizar**
		Sí	**No**	
7a	Proporcionar una línea de visión clara de los elementos importantes para cualquier usuario sentado o de pie.			
7b	Hacer que todos los componentes sean cómodos para cualquier usuario sentado o de pie.			

7c	Acomodar variaciones en mano y tamaño de agarre.			
7d	Proporcionar espacio adecuado para el uso de dispositivos de asistencia o asistencia personal.			

Herramienta de Accesibilidad digital, usabilidad y experiencia de usuario, 1. Elaboración propia.

Usabilidad:

Se mide a partir de cinco componentes o parámetros (Nielsen, 2012):

a. Aprendizaje: ¿Qué tan fácil es para las personas usuarias realizar tareas la primera vez que se encuentran con el diseño?

b. Eficiencia: Una vez que aprendieron, ¿con qué rapidez pueden realizar estas tareas?

c. Memorabilidad: Cuando las personas usuarias no utilizan el diseño por un periodo de tiempo ¿con qué facilidad pueden recordar cómo se realizaban las tareas?

d. Errores: ¿Cuántos errores comete la persona usuaria, ¿qué tan graves son tales errores y con qué facilidad puede recuperarse de estos?

e. Satisfacción: ¿Qué tan agradable es usar el diseño?

La siguiente herramienta permite medir la usabilidad de un diseño específico, incluye los cinco componentes o parámetros; aprendizaje, eficiencia, memorabilidad, errores y satisfacción. Se cuenta con una escala del 1 al 5, donde 1 es el nivel más bajo y 5 el más alto.

Herramienta para medir la usabilidad de un diseño						
Fecha de aplicación:						
Nombre del diseño:	**Nivel**					**Acción por realizar**
Parámetro	**1**	**2**	**3**	**4**	**5**	
Aprendizaje						
¿Qué tan fácil es para las personas usuarias realizar las tareas la primera vez que se encuentran con el diseño?						
Eficiencia						
Una vez que aprendieron ¿Con qué rapidez pueden realizar estas tareas?						
Memorabilidad						

Cuando las personas usuarias no utilizan el diseño por un periodo de tiempo ¿Con qué facilidad pueden recordar cómo se realizaban las tareas?						
Errores						
¿Cuántos errores comete la persona usuaria?						
¿Qué tan graves son tales errores?						
¿Con qué facilidad puede recuperarse de estos errores?						
Satisfacción						
¿Qué tan agradable es usar el diseño?						

Herramienta de Accesibilidad digital, usabilidad y experiencia de usuario, 2. Elaboración propia.

POLÍTICAS GENERALES

A continuación, se hace referencia a las normas nacionales vigentes vinculadas con el tema en cuestión que se consideraron para el desarrollo del Código, haciendo referencia a dos grandes áreas: por un lado, la tecnología y la brecha digital existente en la sociedad costarricense y por otro los derechos humanos y las personas con discapacidad, siendo este segmento poblacional el más vulnerable en cuanto a acceso a la información se refiere.

Constitución Política de la República de Costa Rica

Es el instrumento jurídico con mayor peso en nuestro país, y establece de manera particular lo siguiente para las poblaciones en condición de vulnerabilidad:

> Artículo N°51:
> "La familia, como elemento natural y fundamento de la sociedad, tiene derecho a la protección especial del Estado. Igualmente tendrá derecho a esa protección la madre, el niño, el anciano y el enfermo desvalido".

De acuerdo con lo interpretado por la Sala Constitucional (2000) en la Resolución N°11516, enfermo desvalido es el equivalente a la Persona con Discapacidad.

Establecida como una población vulnerable, las personas con discapacidad son sujetas de protección especial, es decir, el Estado debe brindarles apoyo para equiparar sus condiciones a las del resto de la población. De ahí que el desarrollo e implementación de una política con la naturaleza del presente Código puede considerarse parte de esas medidas dirigidas

concretamente a la población en función de apoyar y mediar en su derecho a la información y comunicación.

Ley N°8661 Aprobación de la Convención sobre los Derechos de las Personas con Discapacidad y su Protocolo

Promulgada en setiembre de 2008 con el fin de aprobar y dar rango de Ley a aquello que ya se encontraba establecido en la Convención sobre los derechos de las personas con discapacidad y su protocolo facultativo. Esta Ley, según el orden jurídico establecido en nuestro país, es la norma jurídica más importante referente a derechos humanos de esta población, después de lo estipulado en la Constitución Política de Costa Rica. En lo pertinente al Código, en ella se establece:

> Artículo N°2. Definiciones:
>
> La "comunicación" incluirá los lenguajes, la visualización de textos, el braille, la comunicación táctil, los macro tipos, los dispositivos multimedia de fácil acceso, así como el lenguaje escrito, los sistemas auditivos, el lenguaje sencillo, los medios de voz digitalizada y otros modos, medios y formatos aumentativos o alternativos de comunicación, incluida la tecnología de la información y las comunicaciones de fácil acceso;
>
> Por "discriminación por motivos de discapacidad" se entenderá cualquier distinción, exclusión o restricción por motivos de discapacidad que tenga el propósito o el efecto de obstaculizar o dejar sin efecto el reconocimiento, goce o ejercicio, en igualdad de condiciones, de todos los derechos humanos y libertades fundamentales en los ámbitos político, económico, social, cultural, civil o de otro tipo. Incluye todas las formas de discriminación, entre ellas, la denegación de ajustes razonables;
>
> Por "ajustes razonables" se entenderán las modificaciones y adaptaciones necesarias y adecuadas que no impongan una carga desproporcionada o indebida, cuando se requieran en un caso particular, para garantizar a las personas con discapacidad el goce o ejercicio, en igualdad de condiciones con las demás, de todos los derechos humanos y libertades fundamentales; (…) (Ley N°8661, 2008).

Según las definiciones anteriores, el Código en cuestión puede promover el desarrollo de herramientas basados en el diseño universal, o bien, plataformas que puedan fungir como instrumentos alternativos para facilitar la comunicación y la información, pudiendo ser

consideradas como un ajuste razonable que brindaría una alternativa comunicativa para evitar la discriminación por motivos de discapacidad.

Artículo N°4. Obligaciones generales:

1. Los Estados Parte se comprometen a asegurar y promover el pleno ejercicio de todos los derechos humanos y las libertades fundamentales de las personas con discapacidad sin discriminación alguna por motivos de discapacidad. A tal fin, los Estados Parte se comprometen a:

(…)

f) Emprender o promover la investigación y el desarrollo de bienes, servicios, equipos e instalaciones de diseño universal (…)

g) Emprender o promover la investigación y el desarrollo, y promover la disponibilidad y el uso de nuevas tecnologías, incluidas las tecnologías de la información y las comunicaciones, ayudas para la movilidad, dispositivos técnicos y tecnologías de apoyo adecuadas para las personas con discapacidad (...) (Ley N°8661, 2008).

Artículo N°9. Accesibilidad:

1. A fin de que las personas con discapacidad puedan vivir en forma independiente y participar plenamente en todos los aspectos de la vida, los Estados Partes adoptarán medidas pertinentes para asegurar el acceso de las personas con discapacidad, en igualdad de condiciones con las demás, alentorno físico, el transporte, la información y las comunicaciones, incluidos los sistemas y las tecnologías de la información y las comunicaciones, y a otros servicios e instalaciones abiertos al público o de uso público, tanto en zonas urbanas como rurales

(…)

2. Los Estados Parte también adoptarán las medidas pertinentes para: (…)

f) Promover otras formas adecuadas de asistencia y apoyo a las personas con discapacidad para asegurar su acceso a la información;

g) Promover el acceso de las personas con discapacidad a los nuevos sistemas y tecnologías de la información y las comunicaciones, incluida Internet (...) (Ley N°8661, 2008).

Artículo 21. Libertad de expresión y de opinión y acceso a la información:

Los Estados Parte adoptarán todas las medidas pertinentes para que las personas con discapacidad puedan ejercer el derecho a la libertad de expresión y opinión, incluida la libertad de recabar, recibir y facilitar información e ideas en igualdad de condiciones con las demás y mediante cualquier forma de comunicación que elijan con arreglo a la definición del artículo 2 de la presente Convención, entre ellas:

(…)

b) Aceptar y facilitar la utilización de la lengua de señas, el Braille, los modos, medios, y formatos aumentativos y alternativos de comunicación y todos los demás modos, medios y formatos de comunicación accesibles que elijan las personas con discapacidad en sus relaciones oficiales; (…) (Ley N°8661, 2008).

En los artículos mencionados se constituye la obligatoriedad de contemplar la accesibilidad a la información y a la comunicación como aspecto fundamental para garantizar la equiparación de oportunidades en los procesos comunicativos para las personas sordas.

Ley N°7948 Ratificación de la Convención Interamericana para la Eliminación de todas las Formas de Discriminación contra las PcD

Promulgada en el año 1999, tercera en importancia al ser suscrita por la Organización de Estados Americanos, establece que los Estados parte deben promulgar medidas para que los entes públicos y privados brinden bienes y servicios que incluyan a las personas con discapacidad.

Artículo N°3:

Para lograr los objetivos de esta Convención, los Estados parte se comprometen a:

1. Adoptar las medidas de carácter legislativo, social, educativo, laboral o de cualquier otra índole, necesarias para eliminar la discriminación contra las personas con discapacidad y propiciar su plena integración en la sociedad, incluidas las que se enumeran a continuación sin que la lista sea taxativa:

a. Medidas para eliminar progresivamente la discriminación y promover la integración por parte de las autoridades gubernamentales y/o entidades privadas en la prestación o suministro de bienes, servicios, instalaciones, programas y actividades, tales como el empleo, el transporte, las comunicaciones, la vivienda, la recreación, la educación, el deporte, el acceso a la justicia y los servicios policiales, y las actividades políticas y de administración (...) (Ley N°7948, 2009)

Ley N°7600 Igualdad de Oportunidades para las Personas con Discapacidad

Emitida en mayo de 1996. A pesar de ser anterior a la mencionada convención y tener un rango jurídico inferior a ésta, ambos estatutos son complementarios, debido a que ésta es un instrumento que establece requisitos para ejecutar la accesibilidad en diferentes ejes.

Artículo N°50. Información accesible:

"Las instituciones públicas y privadas deberán garantizar que la información dirigida al público sea accesible a todas las personas, según sus necesidades particulares".

Al señalar la obligatoriedad de brindar información a toda la población a partir de sus necesidades particulares, la Ley N°7600 permite que un Código como este tenga justificación en respuesta al apoyo que debe darse a la población con discapacidad.

Decreto N°26831 Reglamento Ley de Igualdad de Oportunidades para Personas con Discapacidad

Esta norma instrumental, decretada en 1998, complementa lo establecido en la Ley N°7600 y pacta con mayor detalle los medios tecnológicos que deben adaptarse a las necesidades de la población con discapacidad.

Artículo N°177. Sistemas informativos:

Todas las instituciones públicas y privadas que brinden servicios al público adaptarán, a las necesidades de las personas con discapacidad y sus familias, todos los sistemas de información y comunicación, materiales divulgativos, así como los medios tecnológicos utilizados para esos fines, entre ellas el uso del Braille y el Lenguaje de Señas Costarricense.

Ley N°8642 General de Telecomunicaciones

Esta Ley, mencionada anteriormente, hace especial énfasis en promover acciones que favorezcan la universalidad, la reducción de la brecha digital y la inclusión de personas en

condición de vulnerabilidad, ligando estas obligaciones con el Plan Nacional de Desarrollo de las Telecomunicaciones (PNDT).

Artículo N°2. Objetivos de esta Ley:

Son objetivos de esta Ley:

a) Garantizar el derecho de los habitantes a obtener servicios de telecomunicaciones, en los términos establecidos en esta Ley.

b) Asegurar la aplicación de los principios de universalidad y solidaridad del servicio de telecomunicaciones.

c) Fortalecer los mecanismos de universalidad y solidaridad de las telecomunicaciones, garantizando el acceso a los habitantes que lo requieran.

d) Proteger los derechos de los usuarios de los servicios de telecomunicaciones, asegurando eficiencia, igualdad, continuidad, calidad, mayor y mejor cobertura, mayor y mejor información, más y mejores alternativas en la prestación de los servicios, así como garantizar la privacidad y confidencialidad en las comunicaciones, de acuerdo con nuestra Constitución Política.

(…)

f) Promover el desarrollo y uso de los servicios de telecomunicaciones dentro del marco de la sociedad de la información y el conocimiento y como apoyo a sectores como salud, seguridad ciudadana, educación, cultura, comercio y gobierno electrónico. (Ley N°8642, 2008).

Artículo N°32. Objetivos del acceso universal, servicio universal y solidaridad:

Los objetivos fundamentales del régimen de acceso universal, servicio universal y solidaridad son los siguientes:

(…)

d) Reducir la brecha digital, garantizar mayor igualdad de oportunidades, así como el disfrute de los beneficios de la sociedad de la información y el conocimiento por medio del fomento de la conectividad, el desarrollo de infraestructura y la disponibilidad de dispositivos de acceso y servicios de banda ancha. (Ley N°8642, 2008).

Artículo N°33. Desarrollo de objetivos de acceso universal, servicio universal y solidaridad:

Corresponde al Poder Ejecutivo, por medio del PNDT, definir las metas y las prioridades necesarias para el cumplimiento de los objetivos de acceso universal, servicio universal y solidaridad establecidos en el artículo anterior. Con este fin, dicho Plan deberá contener una agenda digital, como un elemento estratégico para la generación de oportunidades, el aumento de la competitividad nacional y el disfrute de los beneficios de la sociedad de la información y el conocimiento, que a su vez contenga una agenda de solidaridad digital que garantice estos beneficios a las poblaciones vulnerables y disminuya la brecha digital. (Ley N°8642, 2008).

POLÍTICAS ESPECÍFICAS

Plan Nacional de Desarrollo de las Telecomunicaciones (PNDT) 2022-2027

El ya mencionado Plan hace énfasis en la accesibilidad de las telecomunicaciones parala población con discapacidad, donde se menciona la ratificación del país a la *Convención sobre los Derechos de las Personas con Discapacidad (por medio de la Ley N° 8661, Ley de Aprobación de la Convención sobre los Derechos de las Personas con Discapacidad y el Decreto Ejecutivo N° 34780 "Ratificación de la República de Costa Rica a la Convención sobre los Derechos de las Personas con Discapacidad y su Protocolo"). En dicha norma se abordan los temas de accesibilidad, movilidad personal, libertad de expresión, de opinión y acceso a la información, así como a la participación en la vida política, todos para los cuales las TIC son de vital importancia para el acceso en igualdad de condiciones al desarrollo (pág.24, PNDT, 2022).*

Directriz Presidencial Nº 036-MTSS-MICITT Implementación de accesibilidad de la red de los sitios del sector público

Esta normativa se creó con el fin de que el Ministerio de Ciencia Innovación Tecnología y Telecomunicaciones (MICITT) y el Consejo Nacional de Personas con Discapacidad (CONAPDIS) emitieran los lineamientos técnicos requeridos para facilitar que las personas con discapacidad tengan acceso a la información y a las Tecnologías de Información y Conocimiento (TIC), de manera oportuna, sin ningún costo adicional al usuario final, y con formatos accesibles para los diferentes tipos de discapacidad, con el fin de garantizar la igualdad real de oportunidades, evitando así todo tipo de discriminación.

La Directriz instruye a las personas jerarcas de toda la Administración Pública Central e insta

a las personas jerarcas de la Administración Pública Descentralizada, a partir de su publicación, a implementar la accesibilidad de la red en los sitios de las instituciones públicas que representan, en estricto acatamiento de los lineamientos técnicos emitidos por el CONAPDIS y el MICITT.

El sector público costarricense velará porque el desarrollo y/o mantenimiento de sus sitios web, cumplan los lineamientos técnicos emitidos por el CONAPDIS y el MICITT. Por lo que, en toda contratación de servicios tecnológicos, o incluso aquellos sitios web cuyo desarrollo ha sido resultado de una donación, deberá garantizarse que se apeguen a lo establecido en dichos lineamientos técnicos. Los sitios web deberán ser desarrollados o implementados de manera tal que garanticen la disponibilidad y la accesibilidad a la información.

ESTÁNDARES

ISO 9241-210: Ergonomía de la interacción humano-sistema. Parte 210: Diseño centrado en el hombre para sistemas interactivos

A nivel de interfaces de App o de aplicaciones escritorio, se pueden utilizar la mayoría de estas pautas y complementar con algunas normas de usabilidad, como las propuestas por la norma ISO 9241-210.

La norma ISO 9241-210 proporciona requerimientos y recomendaciones para los principios y actividades de diseño centrados en el ser humano a lo largo del ciclo de vida de los sistemas interactivos basados en computadora. Está destinado a ser utilizado por aquellos que gestionan los procesos de diseño y se ocupa de las formas en que los componentes de hardware y software de los sistemas interactivos pueden mejorar la interacción entre el ser humano y el sistema (ISO, 2010).

WCAG 2.1

Las Pautas de Accesibilidad para el Contenido Web (WCAG) 2.1 definen una amplia gama de recomendaciones para crear contenido Web más accesible. Seguir estas pautas permite crear un contenido más accesible para un mayor número de personas con discapacidad, tales como ceguera y baja visión, sordera y deficiencias auditivas, deficiencias del aprendizaje, discapacidad cognitiva, discapacidad motora, deficiencias del habla, foto sensibilidad y combinaciones de las anteriores. Seguir estas pautas puede a menudo ayudar a que el contenido Web sea más usable para cualquier tipo de persona usuaria.

Las WCAG 2.1 se han desarrollado mediante el proceso del World Wide Web Consortium

(W3C) en cooperación con individuos y organizaciones en todo el mundo, con el fin de proporcionar un estándar compartido para la accesibilidad del contenido web que logre satisfacer las necesidades de personas, organizaciones y gobiernos a nivel internacional.

Niveles de orientación de las WCAG 2.1

Los individuos y organizaciones que emplean las WCAG son un grupo amplio y variado que incluye diseñadores y desarrolladores web, reguladores, agentes de compra, profesores y estudiantes. Para poder satisfacer las necesidades tan variadas de esta audiencia, se proporcionan varios niveles de orientación: principios generales, pautas generales y criterios de éxito verificables.

Principios: En el nivel más alto se sitúan los cuatro principios que proporcionan los fundamentos de la accesibilidad web: perceptible, operable, comprensible y robusto.

Pautas: Por debajo de los principios están las pautas. Las doce pautas proporcionan los objetivos básicos que los autores deben lograr con el fin de crear un contenido más accesible para las personas usuarias con distintas discapacidades. Estas pautas no son verificables, pero proporcionan el marco y los objetivos generales que ayudan a los autores a comprender los criterios de conformidad y a implementar las técnicas adecuadamente.

Criterios de Éxito: Para cada pauta se proporcionan los Criterios de Éxito verificables que permiten emplear las WCAG 2.1 en aquellas situaciones en las que existan requisitos y necesidad de evaluación de conformidad como: especificaciones de diseño, compras, regulación o acuerdos contractuales. Con el fin de cumplir con las necesidades de los diferentes grupos y situaciones, se definen tres niveles de conformidad: A (el más bajo), AA y AAA (el más alto).

Todos estos niveles de orientación (principios, pautas y criterios de éxito) actúan en conjunto para proporcionar una orientación sobre cómo crear un contenido más accesible.

A continuación, se detallan los 4 principios de esta norma:

Perceptible: la información y los componentes de la interfaz deben ser presentados a las personas usuarias de modo que ellas puedan percibirlos. Pauta asociada:

Alternativas textuales: proporcionar alternativas textuales para todo contenido no textual de modo que se pueda convertir a otros formatos que las personas necesiten, tales como textos ampliados, braille, voz, símbolos o un lenguaje más simple. Nivel de conformidad que se alcanza: Nivel A.

Operable: los componentes de la interfaz del usuario y la navegación deben ser operables. Pauta asociada:

Tiempo suficiente (re-autenticación): cuando expira una sesión autenticada, la persona usuaria puede continuar la actividad sin pérdida de datos tras volver a identificarse. Nivel de conformidad que se alcanza: Nivel AAA.

Comprensible: la información y la operativa del interfaz de usuario debe ser comprensible. Pauta asociada:

Legible (idioma de la página): el idioma predeterminado de cada página web puede ser determinado por software. Nivel de conformidad que se alcanza: Nivel A.

Robusto: el contenido debe ser suficientemente robusto como para poder ser interpretado de forma fiable por una amplia variedad de agentes de usuario, incluyendo las ayudas técnicas. Pauta asociada:

> Compatible (procesamiento): en los contenidos implementados mediante el uso de lenguajes de marcado, los elementos tienen las etiquetas de apertura y cierre completas; los elementos anidados de acuerdo con sus especificaciones; los elementos no contienen atributos duplicados y los ID son únicos, excepto cuando las especificaciones permitan estas características. Nivel de conformidad que se alcanza: Nivel A.

Niveles de conformidad:

Nivel A: Para la conformidad con el Nivel A (el nivel mínimo de conformidad), la página web satisface todos los Criterios de Éxito del Nivel A, o se proporciona una versión alternativa conforme.

Nivel AA: Para la conformidad con el Nivel AA, la página web satisface todos los Criterios de Éxito de Nivel A y Nivel AA, o se proporciona una versión alternativa que cumple con el Nivel AA.

Nivel AAA: Para la conformidad con el Nivel AAA, la página web satisface todos los Criterios de Éxito de Nivel A, Nivel AA y Nivel AAA, o se proporciona una versión alternativa que cumple con el Nivel AAA.

Aunque la conformidad sólo puede alcanzarse en los niveles mencionados, se alienta a los autores a notificar en sus declaraciones cualquier avance que hayan realizado para satisfacer los criterios de conformidad de un nivel de conformidad mayor al que hayan alcanzado.

No se recomienda que el Nivel de Conformidad AAA sea requerido como política general para la totalidad de un sitio web, ya que para algunos contenidos no es posible satisfacer todos los Criterios de Conformidad de Nivel AAA.

La siguiente herramienta permite, por medio de los 4 principios de la norma WCAG 2.1, que las instituciones cuenten con una guía para crear contenido accesible para los usuarios. Contiene requisitos establecidos en los principios, y un espacio para indicar el nivel de conformidad alcanzado para cada principio.

Herramienta para verificar los principios que proporcionan los fundamentos de la accesibilidad web				
El contenido web de las instituciones es accesible para personas con discapacidad según las Pautas de Accesibilidad para el contenido Web (WCAG) 2.1				
Fecha de aplicación:				
Principio	**Requisito**	**Nivel de conformidad**	**¿Cumple?**	
			Sí	**No**
Perceptible	¿Se proporcionan alternativas textuales para todo contenido no textual (textos ampliados, braille, voz, símbolos o lenguaje más simple)?			
Operable	¿Al terminar la sesión autenticada, la persona usuaria puede continuar la actividad sin pérdida de datos tras volver a identificarse?			
Comprensible	¿El idioma de la página web puede ser determinado por software?			
Robusto	¿En los contenidos implementados mediante el uso de lenguajes de marcado, los elementos tienen las etiquetas de apertura y cierre completas?			
	¿En los contenidos implementados mediante el uso de lenguajes de marcado, los elementos están anidados de acuerdo con sus especificaciones?			
	¿En los contenidos implementados mediante el uso de lenguajes de marcado, los elementos no contienen atributos duplicados y los ID son únicos?			

Herramienta de Accesibilidad digital, usabilidad y experiencia de usuario, 3. Elaboración propia.

Los esfuerzos incluyen procesos de transición entre los medios tradicionales y los digitales; además de accionables claros para que las instituciones públicas logren buenos servicios y plataformas digitales basados en tres principios fundamentales: Experiencia de Usuario, Accesibilidad y Buenas Prácticas Tecnológicas. Además, se fomenta un sistema de diseño nacional para todas las instituciones públicas, el cual se recomienda trabajar a nivel país.

Para efectos de este código, se explican tales estándares y los puntos más importantes de la estrategia con el fin de tomarlos como puntos de referencia para la creación de licitaciones que tengan el fin de contratar empresas de desarrollo de productos digitales para el Gobierno de Costa Rica.

a. Estándares de Servicios Digitales

Estos estándares están basados en distintos criterios para ayudar al gobierno a crear e implementar buenos servicios digitales. Estos criterios son:

I. Entender las necesidades de las personas usuarias

Se debe desarrollar un entendimiento profundo de las personas usuarias y los problemas que estamos intentando resolver para ellas. Es importante entender la mayor parte del contexto ya que esto da una mayor oportunidad de satisfacer las necesidades de las personas usuarias.

Concentrarse en la persona usuaria y en el problema que está intentando resolver, en lugar de concentrarse en una solución particular; y probar las suposiciones en etapas tempranas del proceso para reducir el riesgo de construir herramientas incorrectas.

Para esto se debe invertir tiempo realizando investigación de personas usuarias, construir prototipos para probar hipótesis y utilizar la *web Analytics* y otros datos disponibles para lograr comprender el problema central que se busca resolver.

II. Hacer investigación de personas usuarias de manera constante

Realizar constante investigación permitirá revisar si las plataformas digitales están ayudando a las personas usuarias a realizar las tareas que satisfacen sus necesidades; además de poder seguir realizando mejoras en los servicios y sistemas.

Es importante realizar investigación y pruebas de usabilidad durante toda la etapa de diseño y también después que sea implementado. Además, se debe establecer claramente qué tan seguido se realizarán estas pruebas y la investigación para mantener una mejora constante.

Al finalizar cada etapa, se debe presentar un plan de investigación para la siguiente fase o iteración además de un informe de la etapa concluida que incluya: cómo se realizó la investigación, una sección de la investigación y pruebas en personas usuarias con discapacidades, cómo se utilizaron los datos disponibles para la mejora de la siguiente iteración, los problemas que se encontraron y cómo se solucionaron y todos aquellos problemas que no se pudieron solucionar en esta etapa y cómo se manejan en el sistema en vivo; además del plan para abordarlos en la siguiente etapa.

III. Se recomienda contar con un equipo multidisciplinario

Con el fin de construir mejores plataformas digitales, mejorar según las necesidades de las personas usuarias y tomar decisiones rápidas, es recomendable que el equipo encargado sea multidisciplinario.

Cada equipo encargado de plataformas digitales puede estar conformado por: un product owner, project manager, manager de implementación, arquitecto técnico, líder de asistencia digital, diseñador de experiencia de usuario, investigador de usuario, diseñador de contenido, desarrollador back-end y desarrollador front-end.

Debe aclararse cómo realizar transferencia de información entre roles durante todas las etapas del proceso y que cada miembro del equipo entienda las responsabilidades de cada rol. Es importante que el equipo pueda seguir mejorando en futuras iteraciones y que cada miembro del equipo comprenda por completo el producto entregado.

IV. Utilizar metodologías ágiles

Con el objetivo de lograr satisfacer las necesidades de las personas usuarias, que los sistemas sean sencillos y convenientes, que se puedan cambiar rápidamente en futuras iteraciones y que tengan menor costo, es de gran importancia utilizar metodologías ágiles.

Cada equipo debe definir cómo estará utilizando las metodologías, y qué herramientas y técnicas utilizará. Además, la metodología de trabajo se revisará constantemente con el fin de mejorar el trabajo y la comunicación del equipo.

Se debe mostrar en cada etapa del proceso ágil que el equipo tiene metas claras y medibles, y que se encuentra enfocado en manejar cambios y riesgos en tiempo real. Deben quedar siempre documentadas las diferentes opciones de diseño que fueron exploradas y las razones por las que se descartaron algunas de ellas.

V. Iterar y mejorar frecuentemente

Para asegurar que la plataforma continúe satisfaciendo las necesidades de las personas usuarias a pesar de cambios en legislación o política pública, debe haber un proceso de iteración y mejora constante y frecuente.

Cada equipo debe explicar qué se ha construido en cada etapa, el proceso que se llevó a cabo, cómo esta iteración satisface las necesidades de las personas usuarias basada en la investigación realizada, y debe demostrar que esta ha sido analizada y utilizada para mejorar los sistemas.

Además, es de suma importancia lograr que, gracias a mejoras anuales, se puede realizar un *despliegue* del sistema frecuente con interrupciones mínimas para las personas usuarias.

VI. Evaluar herramientas y sistemas

Para minimizar el riesgo o restricciones asociadas con las herramientas que se utilizarán, se hará una evaluación de cuáles utilizar durante el proceso de diseño e implementación. Esto para evitar contratos que limitan la mejora del sistema y permitir construir un sistema sostenible fácil de manejar.

Los lenguajes de programación, *frameworks* y otras decisiones técnicas deben decidirse tomando en cuenta cómo afectarán las siguientes iteraciones y mejoras en el sistema.

VII. Comprender los problemas de seguridad y privacidad

Es importante comprender que las personas usuarias no van a utilizar los productos digitales a menos que se garantice que es confidencial y seguro; y que pueden acceder a la información y los servicios cuando lo requieran.

Por lo tanto, es vital identificar posibles amenazas y vulnerabilidades dentro del sistema y realizar pruebas para reducirlas; asimismo, se ha de establecer un plan para mantener actualizado el sistema a nivel de seguridad.

Todo el equipo debe tener clara la gestión de seguridad, además de conocer las posibles amenazas de seguridad y privacidad, así como describir las preocupaciones legales (por ejemplo: ¿cómo se manejan los datos o la política para compartirlos).

Además, debe presentarse a las personas usuarias la política de privacidad y *cookies* apenas ingresan al sistema.

VIII. Realizar todo código nuevo, abierto

Todo código nuevo debe ser abierto, para que otras plataformas gubernamentales se puedan construir reutilizando lo que se ha creado y así reducir costos en todo el sector público al evitar duplicar esfuerzos construyendo cosas iguales o similares.

Cada institución deberá planear cómo realizará un código abierto y reutilizable, cómo compartir el código en repositorios de código abiertos, además de confirmar que se posee la propiedad intelectual y de trabajar en conjunto con equipos de otras instituciones para resolver cómo reutilizar el código.

IX. Utilizar estándares abiertos y plataformas comunes

Esto permite ahorro de tiempo y dinero al reutilizar cosas que ya se encuentran disponibles dentro de las instituciones públicas, además de facilitar moverse entre diferentes tecnologías de ser necesario y no quedarse encerrado en contratos difíciles de terminar.

Asimismo, utilizar plataformas comunes permitiría entregar a las personas usuarias experiencias consistentes en las plataformas gubernamentales, lo cual construye confianza.

X. Realizar pruebas con personas usuarias

Realizar pruebas permite encontrar problemas y errores anticipadamente, y con ello, asegurarse de que funciona para el mayor porcentaje posible de personas usuarias, complementando así los datos que se tienen disponibles. De esta manera, si con los datos podemos saber qué está pasando, a través de las pruebas con personas usuarias se puede saber el porqué.

Las pruebas con personas usuarias deberán hacerse en los diferentes dispositivos que las personas usuarias utilizan para asegurar una experiencia unificada en todas las plataformas.

Las pruebas serán realizadas con personas usuarias con o sin discapacidades, asegurando mejoras continuas para todas ellas.

XI. Hacer un plan para cuando el servicio en línea no esté disponible.

Las personas usuarias esperan que una plataforma esté disponible en todo momento, por lo que es necesario hacer un plan en caso de que la plataforma sufra una interrupción en su funcionamiento. Esto debe incluir los siguientes puntos:

- Un plan en medios no digitales en caso de que alguna de las plataformas sea indispensable para las personas usuarias.
- Una estrategia de recuperación de datos y pruebas a la misma.
- Las causas más probables por las que la plataforma podría fallar y cómo se planea evitar que sucedan.
- Una estrategia para hacer frente a las interrupciones de la plataforma, incluyendo responsables y las decisiones que pueden tomar.

XII. Propiciar que las personas usuarias logren sus objetivos al primer intento

Es importante que las personas usuarias puedan completar tareas en las plataformas desde la primera vez que lo intentan. Esto incluye personas con discapacidad.

Se debe tener en cuenta flujos de personas usuarias de principio a fin, tomando en cuenta opciones de diseño que cumplan con accesibilidad web y buenas prácticas de usabilidad.

Cada flujo dentro de la plataforma debe haber sido diseñado con base en la investigación de personas usuarias, probado a través de pruebas de usabilidad y mejorado de manera frecuente gracias a los resultados de estas pruebas, de la investigación y de datos de *analytics*.

Si una persona usuaria encuentra difícil completar alguna tarea dentro de la plataforma, evitará utilizarla en un futuro. Una manera de reducir esta posibilidad es cumpliendo con los puntos II, V y X del presente apartado.

XIII. Generar una experiencia consistente entre las diferentes plataformas gubernamentales

Utilizar patrones de diseño similares a través de las páginas gubernamentales propicia que las personas usuarias perciban unidad, lo cual llevará a tener una experiencia consistente.

El punto IX de estos estándares permite facilitar el cumplimiento de la experiencia consistente. De esta manera, no necesariamente se debe construir algo desde cero, sino que es posible concentrarse en puntos específicos de su propia plataforma digital.

Para lograr tal objetivo es importante trabajar en un sistema de diseño a nivel nacional, por lo tanto, es altamente recomendado dirigir esfuerzos en esta línea.

XIV. Incentivar a todas las personas el uso de medios digitales

Incentivar el uso de plataformas digitales dentro del área gubernamental ayuda a un mejor uso del presupuesto al reducir el número de personas utilizando canales no digitales, además de empoderar a las personas usuarias y ayudarles a mejorar sus habilidades en medios digitales.

Se debe generar un plan para aumentar el uso de las plataformas, indicando acciones claras de cómo se va a realizar. Dentro de este plan se debe establecer todos los otros canales no digitales que las personas usuarias utilizan y los datos que se recolectan en estos canales, que nos permitan realizar la transición. Además, este plan debe incluir métricas para los próximos 5 años de trabajo.

También es importante identificar esos actores que apoyan a las personas usuarias tanto en medios tradicionales como en digitales, e involucrarles en

los procesos de investigación para realizar una mejora continua en las plataformas.

XV. Identificar, recolectar e informar datos e indicadores del rendimiento de las plataformas

Al recolectar dichos datos, vamos a poder aprender las fortalezas y debilidades de nuestras plataformas y así poder hacer posible el punto V de estos estándares. La utilización de datos fortalece la toma de decisiones para la mejora de plataformas digitales.

Se debe decidir qué datos se necesitan capturar, de dónde se deben capturar y cómo se recolectarán. Se ha de realizar una ruta para el análisis de este rendimiento y se asignará un responsable dentro del equipo, que pueda identificar accionables derivados de dichos datos.

No se debe confiar solamente en datos cuantitativos sino también en información cualitativa que la investigación de personas usuarias ha permitido obtener durante el proceso, con el fin de demostrar comprensión de las necesidades de estas personas.

Es importante demostrar que se ha abordado el tema de seguridad y privacidad de manera adecuada, tomando en cuenta las consideraciones éticas dentro de la recolección de datos.

Los datos que se utilicen también deben mostrar si se está abordando el tema de accesibilidad de manera correcta.

Además, se debe presentar un plan para saber los datos que se recolectarán, los indicadores de rendimiento, las métricas para indicar el éxito y cómo abordar una segunda iteración de las plataformas digitales; e incluir cómo se va a monitorear la transición de las personas usuarias de medios tradicionales a medios digitales.

XVI. Realizar pruebas con el ministro / ministra o persona encargada de la plataforma

Se deben realizar pruebas y presentación de resultados con las personas encargadas de mayor rango dentro de la institución, ya que estas son responsables de lo que se produce en la institución. Cada responsable debe dar el visto bueno antes que una plataforma entre en funcionamiento.

Para cumplir con la aprobación de la plataforma por parte de la persona encargada de la institución, se debe contar con evidencia: video de la prueba, fotografías de la prueba y/o carta firmada.

La siguiente herramienta, contiene los criterios establecidos en los Estándares de Servicios Digitales, sirviendo de ayuda al gobierno para crear e implementar buenos servicios digitales.

Herramienta para verificar los criterios establecidos en los Estándares de Servicios Digitales			
Fecha de aplicación:			
Criterio	**¿Cumple?**		**Acción por realizar**
	Sí	**No**	
Entender las necesidades de las personas usuarias			
¿Se centra la atención en la persona usuaria en el momento de intentar resolver un problema?			
¿Se construyen prototipos para probar hipótesis y lograr comprender el problema central que se busca resolver?			
Hacer investigaciones de personas usuarias de manera constante			
¿Se realizan revisiones constantes a las plataformas digitales para corroborar si estas satisfacen las necesidades de la población?			
¿Se realizan pruebas de usabilidad durante la etapa de diseño e implementación?			
¿Se realizan planes de investigación al finalizar una etapa, para identificar como se realizó la investigación, mejoras, problemas, y demás elementos de importancia?			
Contar con un equipo multidisciplinario			
¿El equipo multidisciplinario está conformado por un product owner, project manager, manager de implementación, arquitecto técnico, líder de asistencia digital, diseñador de experiencia de usuario, investigador de usuario, diseñador de contenido, desarrollador back-end y desarrollador front-end.?			
Utilizar metodologías ágiles			
¿Se define en los equipos como se está utilizando las diferentes metodologías, herramientas y técnicas?			

¿Se muestra en cada etapa del proceso ágil metas claras y medibles, que permitan manejar cambios y tiempos?			
Iterar y mejorar frecuentemente			
¿Se cuentan con procesos de iteración y mejora anualmente?			
¿Se realizan explicaciones en los equipos de los procesos llevados en cada etapa, permitiendo identificar si satisface las necesidades de los usuarios?			
Evaluar herramientas y sistemas			
¿Se realizan evaluaciones de las herramientas que se utilizarán durante el proceso de diseño e implementación, para evitar contratos que limitan la mejora del sistema?			
Comprender los problemas de seguridad y privacidad			
¿Se identifican posibles amenazas y vulnerabilidades dentro del sistema, para garantizar confidencialidad y seguridad a las personas usuarias?			
¿Se tiene claridad dentro del equipo de la gestión de seguridad?			
¿Se presentan políticas de privacidad y cookies a las personas usuarias al ingresar al sistema?			
Realizar todo código nuevo, abierto			
¿Se tiene conocimiento de que todo código nuevo debe estar abierto para otras plataformas gubernamentales?			
Utilizar estándares abiertos y plataformas comunes			
¿Se utilizan plataformas comunes que permitan ahorrar tiempo y dinero en las instituciones públicas?			
Realizar pruebas con personas usuarias			
¿Se realizan pruebas en diferentes dispositivos utilizados por personas usuarias (con o sin discapacidades) para identificar problemas y errores de forma anticipada?			
Hacer un plan para cuando el servicio en línea no esté disponible			

¿Se cuenta con un plan en medios no digitales en caso de que alguna plataforma sea indispensable para las personas usuarias?			
¿Se cuenta con una estrategia de recuperación de datos?			
¿Se establecen las causas más probables por las que la plataforma falla y como evitarlo?			
¿Se cuenta con una estrategia para hacer frente a las interrupciones, incluyendo responsables y decisiones que se puedan tomar?			
Propiciar que las personas usuarias logren sus objetivos al primer intento			
¿Se cuentan con opciones de diseño que cumplan con accesibilidad web u buenas prácticas de usabilidad?			
Generar una experiencia consistente entre las diferentes plataformas gubernamentales			
¿Se utilizan patrones de diseño similares a través las demás páginas gubernamentales?			
Incentivar a todas las personas el uso de medios digitales			
¿Se ha generado un plan para aumentar el uso de las plataformas, donde se indiquen las acciones claras de cómo se va a utilizar?			
¿Se incluye en el plan métricas para los próximos 5 años de trabajo?			
¿Se involucra a los actores que apoyan a las personas usuarias, en los procesos de investigación para realizar mejoras continuas en las plataformas?			
Identificar, recolectar e informar datos e indicadores del rendimiento de las plataformas			
¿Se realiza la recolección de datos para identificar fortalezas y debilidades en las plataformas, y fortalecer la toma de decisiones?			
¿Se asigna dentro del equipo un encargado para realizar una ruta de análisis de los datos?			
¿Se realiza el plan que incluye los datos que se recolectarán, indicadores de rendimiento, métricas, y monitoreo de transición de personas usuarias de medios tradicionales a digitales?			
Realizar pruebas con el ministro/ministra o personas encargada de la plataforma			
¿Se realizan pruebas y presentaciones de resultados con las personas encargadas de mayor rango?			

Herramienta de Accesibilidad digital, usabilidad y experiencia de usuario, 4. Elaboración propia.

Accesibilidad Digital

Formatos de comunicación accesible

La producción de documentos accesibles es crucial para el intercambio de información. Un documento puede tener cualquier formato, aunque se suele hablar en este ámbito de formatos de uso ampliamente extendido. Se debe comprender que muchas plataformas de intercambio de información utilizan estos formatos tan variados, por lo cual no basta con generar interfaces accesibles si los documentos finales a que tendrán acceso las personas usuarias son en todo caso inaccesibles.

Las guías del Gobierno Británico están pensadas para el sector público, aunque igualmente se invita al sector privado a hacer uso de ellas. Las recomendaciones son conocidas como formatos alternativos y se explican a continuación:

1. Proveer formatos accesibles

Para producir formatos accesibles (también conocidos como formatos alternativos) se recomienda involucrar personas con discapacidades, a través de audiencias, en el desarrollo y revisión de la estrategia. Las organizaciones relacionadas con discapacidad también pueden brindar consejo en esta materia.

1.1. Mejores prácticas:

- Involucrar expertos relevantes, por ejemplo, en mercadeo y comunicaciones, desde las etapas tempranas de planificación.
- Considerar las necesidades de la audiencia con antelación, evaluar cuáles formatos accesibles pueden ser necesarios.
- Asegurarse de contar con proveedores que puedan producir materiales en formatos accesibles.
- Asegurarse de que las personas usuarias con alguna discapacidad no incumplan con fechas límite debido a que los documentos accesibles no están disponibles a tiempo.

1.2. Decidir cuál formato accesible usar:

- Tomar en cuenta el tipo de persona usuaria que usará la interfaz en particular, en otras palabras, se pueden requerir consideraciones más cuidadosas cuando la proporción de personas con discapacidad sea alta.
- Para discapacidades visuales se recomienda considerar audio, descripción de

audio, teléfono, braille y otros códigos impresos.

- Para problemas de aprendizaje y dificultades de alfabetización: audio, descripción de audio, lectura fácil, Makaton, subtítulos.
- Sordera o hipoacusia: LESCO, Makaton, subtitulación, SMS.
- Dificultades de coordinación: letra grande, audio, descripción de audio, teléfono.

1.3. Reducir la necesidad de formatos alternativos:

- Mantener los contenidos lo más simples posibles.
- Escribir en lenguaje sencillo.
- Ser conciso.
- Diseñar para que sea lo más legible posible, por ejemplo, utilizando un tamaño de texto de 14 puntos como mínimo en negrita o 18 en normal, sin perder de vista el peso de la tipografía usada.

1.4. Canales alternativos:

- Considerar el uso de canales alternativos cuando se necesita comunicar un mensaje.
- Un ejemplo de esto puede ser sustituir la impresión de material en braille por un mensaje radial.
- Tomar en cuenta a las instituciones encargadas de temas de discapacidad.

1.5. Versiones resumidas:

- Proveer resúmenes siempre que sea posible.
- Indica los puntos clave y brinda la información de contacto para obtener mayores detalles.

1.6. Análisis costo-beneficio:

- Investigar al público meta desde las etapas tempranas de sus proyectos.
- Hacer una segmentación de la audiencia en grupos.
- Considerar alcanzar la audiencia combinando canales y formatos, teniendo en cuenta sus costos.

1.7. Lenguas indígenas nacionales:

- En consonancia con las recomendaciones sobre audiencias generales y particulares, considerar la posibilidad de incluir versiones en lenguas indígenas nacionales.

1.8. Publicación web:

- Publicar información en un sitio web es una manera de que las personas usuarias ejerzan control sobre su acceso a la información, por ejemplo, cambiando el tamaño de la fuente, el color o el contraste.

2. Audio

2.1. Formatos de audio

Se pueden ofrecer formatos alternativos de audio, tales como:

- Cintas de audio
- Archivos en formato MP3
- CD-ROM
- CD

2.2. Canales de audio:

Los canales de audio incluyen:

- Radio
- Internet
- Periódicos para lector de pantalla
- Audio revistas
- Libros en formato DAISY (Sistema de Información Digital Accesible, por sus siglas en inglés)

Para periódicos para lector de pantalla, audio revistas o libros en formato DAISY, conviene contactar al Centro Nacional de Recursos para la Educación Inclusiva (CENAREC).

Si la institución produce el material en audio, se deben tener en cuenta las siguientes recomendaciones:

- Organizar la información en un orden lógico.
- Evitar el ruido de fondo y la música, salvo en los casos que específicamente se requiera
- Usar voces apropiadas para el tema y la audiencia.
- Brindar tiempo a las personas para entender las llamadas a la acción.

2.3. Descripción de audio:

La descripción de audio consiste en comentarios adicionales que describen acciones en pantalla o en un escenario, el lenguaje corporal y las expresiones faciales de los personajes. La descripción de audio está disponible en:

- televisión
- video y DVD
- cines
- museos y galerías
- teatros
- sedes deportivas.

3. Braille y otros códigos impresos

Estas recomendaciones son específicas para personas ciegas o con baja visión:

3.1. Braille:

- Se debe proporcionar braille a quienes lo soliciten. Sin embargo, es importante definir la cantidad por producir según la demanda real del público meta, ya que el material es costoso.

3.2. Otros códigos impresos:

- Como opción al Braille existe Moon, que es un sistema de lectura y escritura que utiliza símbolos táctiles basados en líneas y curvas para representar las letras, los números y los signos de puntuación.
- Es más fácil de aprender que el braille, pues las letras son más fáciles de distinguir al tacto. Sin embargo, Moon no puede escribirse a mano, ocupa más espacio que el braille y actualmente hay muy poca literatura disponible al respecto.

- En la actualidad, Moon es utilizado por pocas personas.
- Debido a su baja popularidad, no es necesario producir materiales en Moon de manera habitual. Si se recibe una solicitud de producir Moon, se debe consultar si otro formato podría ser una alternativa útil, como las cintas de audio.

4. Lengua de señas costarricense (LESCO)

Proporcionar alternativas de lenguaje de señas hará que las comunicaciones sean más accesibles para las personas que utilizan la Lengua de Señas Costarricense (LESCO) a la hora de comunicarse.

5. Lectura fácil y Makaton

Las personas con discapacidades de aprendizaje pueden utilizar la lectura fácil. Makaton puede ser útil para personas con discapacidades profundas de aprendizaje. El acceso fácil puede ser un formato útil para las personas que han tenido accidentes cerebrovasculares.

5.1. Lectura fácil:

- A menudo es preferida por lectores sin problemas de aprendizaje, ya que proporciona la información esencial sin profundizar en el contenido.
- Puede ser especialmente útil para las personas que no dominan el español.
- Se puede considerar la posibilidad de encargar versiones de fácil lectura de las publicaciones a una organización experta.
- La lectura fácil permite variaciones a lo interno del Sector Público de acuerdo con las preferencias de estilo del departamento.
- Debe ser desarrollada en consulta con la audiencia.
- Se ha de tomar en cuenta que la producción puede consumir mucho tiempo.

5.2. Imágenes de lectura fácil

Se pueden utilizar bancos de imágenes que muestran palabras comunes, así como fotografías. Se pueden elegir las imágenes de acuerdo con las preferencias de estilo de fácil lectura de la organización.

- Es importante elegir las imágenes cuidadosamente para apoyar el texto.
- La imagen puede ir por encima o por debajo de las palabras.

- Las fotografías o imágenes deben ser fáciles de entender.
- Cada una de las imágenes debe mostrar una única idea.
- Las bromas y el humor pueden ayudar a comprender el mensaje.

5.3. Cintas magnéticas y CD-ROMs

Una cinta o CD-ROM adicionales pueden hacer que la información escrita resulte más accesible para las personas con dificultades de aprendizaje.

- Articular las palabras de la publicación lentamente.
- Indicar cuándo se necesita pasar de página para que la persona pueda seguir el texto.
- Considerar incluir música para dar tiempo al pasar las páginas.

5.4. Makaton

Los símbolos de Makaton son compatibles con la escritura de la misma manera que las lenguas de señas son compatibles con el habla. Makaton fue desarrollado para quienes luchan por entender el habla, como las personas con discapacidades profundas de aprendizaje. La mayoría de las personas usuarias lo utilizan como su principal medio de comunicación. Otras personas usuarias incluyen familias, cuidadores, amigos, maestros y trabajadores sociales, que se comunican con personas con discapacidades profundas de aprendizaje.

- Para obtener guías más precisas sobre su producción se puede consultar Makaton (2017).

6. Publicaciones de impresión accesible

6.1. Impresión clara

- Si el sistema tiene opciones de impresión, este debe producir impresos claros, particularmente en cuanto al tamaño y tipo de letra utilizados.
- Usar como mínimo un tamaño de letra de 12 puntos en Arial.
- En caso de no tener disponible la fuente Arial, la fuente alternativa que se use debe ser clara en su diseño, sin demasiado adorno.
- Evitar las fuentes de "escritura a mano".
- El espacio entre líneas debe ser al menos de un espacio simple, preferiblemente más.

- El texto debe estar alineado a la izquierda. Si se alínea al centro o a la derecha se podría perder.
- No separar palabras al final de las líneas con guiones.
- Evitar usar texto sobre imágenes, pues resulta difícil de leer y se puede perder por completo.
- Se deben realizar pruebas de impresión reales, no dar por sentado que lo que se despliega adecuadamente en pantalla también producirá impresos claros.

6.2 Otras buenas prácticas de impresión clara:

- Evitar las cursivas, el subrayado, la escritura a mano simulada, letras con formas inusuales y tipografías decorativas.
- Considerar la longitud de las letras b, d, f, h, k, l, t, g, j, p, q, y en relación con la altura del tipo de letra. Los ascendentes y descendentes cortos hacen que las letras sean menos legibles.
- Considerar las características individuales de cada carácter a la hora de escoger una fuente. Un "3", por ejemplo, se puede confundir con un "8" en algunas fuentes.
- Investigar las preferencias de su audiencia: considerar la posibilidad de validar la eficacia de sus fuentes con una variedad de grupos de edad y discapacidad.
- Las letras más ligeras pueden afectar la legibilidad, ya que la legibilidad requiere un buen contraste. Se recomiendan negritas en material específico para personas con discapacidades visuales, pero se ha de verificar siempre que sea fácil de leer.
- Evitar bloques de letras mayúsculas en los títulos o en el texto del cuerpo.
- Procurar un diseño simple y ordenado.
- Establecer el texto horizontalmente, no inclinado.
- La alineación del texto debe ser a la izquierda, para máxima legibilidad. Evitar alinear a la derecha o justificar el texto.
- Mantener la longitud de la línea entre 60 y 70 caracteres, aproximadamente de 12 a 18 palabras por línea.
- Permitir suficiente espacio en los formularios. Si los detalles deben ser escritos a mano, hacer que las casillas, incluidas las de verificación, sean lo más grandes posible.

- Asegurarse de que las secciones y los capítulos estén claramente definidos con encabezados.
- Mantener los encabezados y números de página en el mismo lugar en cada página.
- Mantener los párrafos cortos y usar interlineado entre párrafos. Usar márgenes y encabezados amplios. Las cajas pueden ayudar a enfatizar o resaltar texto importante.
- Incluir un índice siempre que sea posible.
- Los colores pueden ser útiles para marcar divisiones en un documento y para hacerlo más fácil a la vista, especialmente en el caso de material estadístico, gráficos y tablas. Por lo tanto, se recomienda asegurarse de lograr un fuerte contraste entre el texto y los colores.
- Al configurar texto en columnas, asegurarse de que el espacio entre columnas marque una clara separación.
- Asegurarse de que los números se distingan cuando se imprimen. Los números 3, 5 y 8 se pueden confundir entre sí, al igual que 0 y 6 en algunas fuentes. Para información financiera use un tamaño de punto grande.
- Las imágenes pueden ayudar a comunicar mensajes, además de que proporcionan alivio a los ojos.
- Si se usa una imagen para transmitir información que es esencial para comprender un contenido, se debe incluir un texto alternativo que proporcione la misma información.
- Hacer ilustraciones y fotografías lo más grandes posibles sin que pierdan definición.
- Evitar fotos con muchos detalles o en las que el primer plano y el fondo no están bien contrastados.
- Evitar ajustar el texto alrededor de las imágenes si esto significa que las líneas de texto comienzan en un lugar diferente.
- Evitar gráficos de fondo que dificulten la lectura del texto.
- Mantener información esencial, por ejemplo, detalles de un evento agrupados de manera cercana.
- Buscar el contraste de tipo oscuro contra un fondo claro como regla general, por ejemplo, negro sobre papel blanco o amarillo.
- Evitar usar únicamente el color para transmitir información, ya que algunas personas no

distinguen entre colores.

- Tomar en consideración que algunas personas tienen dificultades para distinguir entre el rojo y el verde y a otras les resulta difícil leer el texto claro sobre un fondo oscuro.
- Cuando se imprime, a veces es muy difícil proporcionar una cobertura de tinta densa en superficies coloreadas.
- El texto en blanco sobre un fondo de color aparece más pequeño: es posible que deba aumentar el tamaño de la fuente y usar un tipo de letra en negrita.
- Cambiar entre negro sobre blanco y blanco sobre negro puede ser confuso y agotador para el ojo.
- Los documentos muy grandes o pequeños pueden ser difíciles de manejar. El tamaño A4 es generalmente el más fácil de usar.

6.3. Publicaciones en letra grande

Las publicaciones en letra grande son aquellas con letra de 16 puntos o más y son esenciales para algunas personas con discapacidad, por ejemplo, personas con discapacidades visuales, discapacidades de aprendizaje, dislexia y problemas de coordinación o destreza manual.

- Producir documentos impresos en letra grande desde un documento en un software procesador de texto.
- Enviar trabajos más elaborados a una impresora comercial para que la calidad de la imagen y la impresión sean consistentes en tamaños más grandes.
- No intentar crear versiones en letra grande al ampliar un documento de impresión estándar con una fotocopiadora.
- Considerar las solicitudes de tamaños de tipo por encima de 28 puntos cuidadosamente. Hoy en día existen tamaños de letra muy grandes, lo cual puede ser contraproducente porque hacen que las publicaciones se vuelvan voluminosas y difíciles de navegar.
- Ofrecer formatos alternativos puede evitar estos problemas, por ejemplo, proporcionar una versión de audio de la información o enviar un documento de texto a alguien para que pueda acceder a la información utilizando un lector de pantalla en su computadora.
- Si se tiene una cantidad limitada de espacio, considerar reducir la cantidad de texto antes de reducir el tamaño de la letra.

7. Subtitulado

- El subtitulado es un texto en pantalla que representa el habla y los efectos de sonido que pueden no ser audibles para las personas con discapacidades auditivas. Se debe sincronizar lo más cerca posible con el sonido.

- Las personas usuarias de subtítulos reflejan la gama completa de competencia en español. Algunas personas sordas consideran que la LESCO es su primera lengua y tienen menos fluidez en el español escrito.

8. Teléfono

8.1. Información disponible mediante teléfono

Las personas con discapacidad generalmente tienen menos acceso a internet que las personas sin discapacidad.

El teléfono es un canal importante para hacer que la información sea accesible a una audiencia. La información crucial, por ejemplo, sobre las pensiones, los beneficios, la salud y los impuestos deben ser fáciles de encontrar por todos los que la necesitan.

Muchas personas con discapacidad, especialmente las personas mayores, no tiene acceso a Internet o pueden tener dificultades para usarlo. El teléfono es un método de comunicación muy importante para estos grupos.

- Mantenga el ruido de fondo al mínimo.

- El orador debe ser claro y utilizar un ritmo que se adapte a la audiencia. Considerar la posibilidad de proporcionar una línea de ayuda o línea directa para respaldar sus comunicaciones. Los operadores telefónicos deben tener entrenamiento específico en comunicación con personas con discapacidad.

- Del mismo modo, las comunicaciones telefónicas no son accesibles para todas las personas con discapacidad, así que se debe de asegurar una combinación de canales de comunicación en su planificación de comunicaciones integrada.

- La información proporcionada únicamente en formato digital puede excluir sectores de su audiencia. Por ejemplo, el uso de preguntas frecuentes en un sitio web sin proporcionar un número de teléfono evitará que algunas personas utilicen el servicio.

La siguiente herramienta permite que las instituciones sigan una serie de pautas establecidas en el código, para identificar si cuentan con formatos de comunicación accesibles.

Herramienta para identificar la accesibilidad digital (formatos de comunicación accesibles)			
Fecha de aplicación:			
Formatos de comunicación accesibles	**¿Cumple?**		**Acción por realizar**
	Sí	**No**	
Proveer formatos accesibles			
Involucrar personas con discapacidades, a través de audiencias, para desarrollar y revisar la estrategia.			
Implementar mejores prácticas, tales como involucramiento de expertos relevantes, considerar las necesidades de la audiencia, contar con proveedores de formatos accesibles.			
Tener en cuenta los tipos de usuarios que usarán la interfaz, y las distintas capacidades con las que estos pueden contar.			
Utilizar cometidos simples, lenguaje sencillo, ser conciso y contar con un diseño legible.			
Considerar canales alternativos para comunicar mensaje.			
Contar con versiones resumidas, brindando puntos clave e información de contacto.			
Investigar al público meta desde la etapa inicial del proyecto, para lograr el alcance.			
Considerar la inclusión de versiones en lenguas indígenas nacionales.			
Publicar la información en sitio web al alcance de los usuarios.			
Audio			
Ofrecer formatos alternativos como cintas de audio, archivos MP3, CD-ROM y CD.			
Brindar canales de audio como radio, internet, periódicos para lector de pantalla, audio revistas y libros en formato DAISY.			
Implementar la descripción de audio.			
Braille y otros códigos impresos			

Proporcionar braille a quienes lo soliciten, definiendo la cantidad por producir según la demanda real del público meta.			
Lengua de señas costarricense (LESCO)			
Proporcionar alternativas de lenguaje que garanticen la comunicación accesible para las personas usuarias.			
Lectura fácil y Makaton			
Utilizar lectura fácil, como Makaton, que es útil para personas con discapacidades profundas de aprendizaje.			
Utilizar imágenes de lectura fácil, cintas magnéticas y CD-ROMs, para que la información escrita resulte más accesible para personas con dificultades de aprendizaje.			
Publicaciones de impresión accesible			
Brindar una impresión clara en cuanto a tamaño y tipo de letra, y las recomendaciones específicas d impresión clara.			
Utilizar buenas prácticas de impresión clara, como evitar cursivas, subrayado, y demás recomendaciones de buenas prácticas.			
Contar con publicaciones en letra grande, esenciales para personas con discapacidades visuales, de aprendizaje, dislexia y problemas de coordinación o destreza manual.			
Subtitulado			
Utilizar subtitulado de texto en la pantalla, para las personas con discapacidad auditivas.			
Teléfono			
Permitir que la información esté disponible mediante el teléfono, teniendo en cuenta la accesibilidad al internet de los usuarios con discapacidad o personas mayores.			

Herramienta de Accesibilidad digital, usabilidad y experiencia de usuario, 5. Elaboración propia.

MINISTERIO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES

GOBIERNO DE COSTA RICA

CAPÍTULO 2:

IDENTIFICACIÓN Y AUTENTICACIÓN CIUDADANA

EQUIPO DE TRABAJO

Integrante	Institución
Gabriel Alcázar	Registro Nacional
Miguel Carballo	BCCR
Patricia Chacón	TSE
Dayanna Mejía	MICITT
Óscar Solís	ICT

INTRODUCCIÓN AL TEMA

Uno de los pilares del CNTD tiene que ver con el tema de Identificación y Autenticación Ciudadana, que será abordado en el presente documento a través de una serie de estándares y lineamientos que permitirán cumplir con la eficaz identificación y autenticación de los ciudadanos a la hora de utilizar servicios y sistemas en línea, lo cual, en última instancia, brindará seguridad y confianza plena a la hora de suministrar sus datos personales a las distintas instituciones públicas.

PRINCIPIOS

Principio de "solo una vez": Asegura que los ciudadanos y las empresas solo han de suministrar cierta información estándar una vez.

Principio de "limitación de la finalidad": Los datos sólo se deben utilizar para la finalidad explícitamente indicada y no con cualquier otro motivo.

Las Instituciones Públicas deberán utilizar las identidades y los mecanismos oficiales de autenticación y compromiso jurídico en medios electrónicos.

Artículo 4º-

Las instituciones de la Administración Central y Descentralizada deberán implementar un sistema de identificación ciudadana seguro, utilizando fuentes de datos oficiales y mecanismos biométricos, que permitan identificar adecuadamente a los ciudadanos costarricenses en sus servicios de atención al público, de manera progresiva, debiendo cubrir al menos un 50% de todas sus ventanillas de atención ciudadana antes del 1ero de diciembre del 2020 (Directriz N°019-MP-MICITT, 2018).

Artículo 3º-Principios.

La Comisión se regirá por los siguientes principios: a) Centrado en las personas: el diseño de todos los servicios de gobierno digital será centrado en las personas e inclusivo, seguro, enfocado en la experiencia del usuario y la protección de sus datos.
b) Transparencia: las soluciones de gobierno digital apoyan la labor y el desarrollo del Gobierno Abierto, deben generar mayor transparencia en la gestión de trámites del Estado. c) Apoyo al sector productivo: se impulsará la competitividad de la empresa privada y del sector productivo en general mediante el uso de plataformas tecnológicas en la prestación de los servicios. d) Eficiencia: el desarrollo de la interoperabilidad, la neutralidad tecnológica y la digitalización y/o automatización de trámites potenciarán un aparato estatal que genera resultados de calidad a costos cada vez más bajos. e) Visión de liderazgomundial: se construirá una visión de liderazgo mundial en materia de gobierno digital ante los retos de la cuarta revolución industrial y el desarrollo y fortalecimiento de la economía del conocimiento en Costa Rica” (Decreto N°41248-MP-MICITT-PLAN- MEIC-MC, 2018).

“Artículo 95.- La ley regulará el ejercicio del sufragio de acuerdo con los siguientes principios: **… 2)** Obligación del Estado de inscribir, de oficio, a los ciudadanos en el Registro Civil y de proveerles de cédula de identidad para ejercer el sufragio; …” (Constitución Política de Costa Rica, 1949).

POLÍTICAS GENERALES

Política general del proceso de identificación

El proceso de identificación deberá efectuarse mediante el número de identificación personal en el formato oficial, de conformidad con la clasificación de la información de cada institución encargada de la identificación de las personas costarricenses y los extranjeros residentes en el país, a saber: TSE y la Dirección General de Migración y Extranjería (DGME), respectivamente.

Política general del proceso de autenticación

El proceso de autenticación deberá efectuarse con medidas que garanticen la protección de la información de las personas costarricenses y los extranjeros residentes en el país, para lo cual se utilizarán los medios disponibles de autenticación de las instituciones del Estado o una combinación de ellos: el uso de biométricos por parte del TSE y la DGME, y la firma digital certificada, de conformidad con la Constitución Política de Costa Rica, la Ley N°8454 de Certificados, Firmas Digitales y Documentos Electrónicos, y la Ley N°8968 de Protección de la Persona Frente al Tratamiento de sus Datos Personales.

POLÍTICAS ESPECÍFICAS

- Las instituciones del Estado deberán clasificar la información que pondrán a disposición de las instituciones del Estado y de la ciudadanía, con el fin de determinar si se requiere el uso de mecanismos de identificación y autenticación.
- Cuando se determine que la información por acceder es de dominio público, las instituciones del Estado podrán determinar los mecanismos pertinentes para permitir el acceso a esta, de forma ágil y sin ser excesivos.
- Cuando el nivel de sensibilidad de los datos amerite que alguna institución del Estado requiera validar el acceso a su plataforma, deberá realizar previamente un proceso de identificación inequívoca, utilizando para ello los mecanismos de identificación dispuestos por el TSE y la DGME.
- El proceso de autenticación en los sistemas de información deberá llevarse a cabo utilizando la tecnología de: algo que yo se mas algo que yo tengo como mínimo doble factor de autenticación, algo que yo se mas algo que soy como biometría cuando esta

sea factible, algo que yo sé, más algo que yo hago, biometría pasiva o de comportamiento, así poder garantizar la parte de identidad de forma inequívoca.

● El proceso de autenticación deberá efectuarse de conformidad con la clasificación de la información de cada institución, para ello deberán utilizarse los mecanismos de autenticación que se encuentran disponibles por el TSE y entidades autorizadas y registradas ante el MICITT según la Ley N°8454, acordes con el nivel de sensibilidad de la información.

ESTÁNDARES

A continuación, se detallan todos aquellos lineamientos que las instituciones del Estado deben seguir para que sus infraestructuras tecnológicas cumplan con los requerimientos exigidos para la validación de los diferentes factores de autenticación que se vayan a utilizar.

Estándar para clasificar la información

Se deben seguir los siguientes mecanismos para definir la clasificación de la información en dos niveles de sensibilidad: El primer nivel corresponde a la información No Sensible que involucra los datos irrestrictos (públicos) que no requiere autenticación y el segundo nivel es el Sensible que contiene la información de carácter privado, que requiere identificación y autenticación por medio de los mecanismos autorizados para acceder a esta.

Cuando alguna institución del Estado valida el acceso a su plataforma digital, en caso de que la categoría de la información requiera ser validada mediante el uso de firma digital certificada o algún sistema biométrico o una combinación de ambas, deberá ser verificada en línea; ya sea con la Autoridad Certificadora (CA) si se trata de firma digital certificada, o con el TSE en caso de requerir comparación biométrica, empleando componentes desarrollados por TSE y por la CA para este fin.

La autenticación podrá solicitar uno o más controles como firma digital certificada y uso de biométricos con prueba de vida, de forma tal que los mecanismos de autenticación permitan que este proceso sea universal y exponencial, es decir, que no sea excluyente para ninguna institución del Estado, por ningún motivo.

En caso de que la transacción que se intenta efectuar requiera de compromiso jurídico, se deberá utilizar firma digital certificada y una prueba de vida biométrica implementada por el TSE.

En caso de que la transacción no requiera compromiso jurídico, puede hacer uso de la biometría para autenticarse.

Estándares de conexión, dispositivos y parámetros para consumo

Autenticación con Firma Digital Certificada

La firma digital basada en el uso de Certificados Digitales debe respetar la Política de Certificados y la Política de Formatos Oficiales de los Documentos Electrónicos Firmados, publicados oficialmente por el MICITT.

Identificación y/o Autenticación Biométrica

La identificación y/o autenticación biométrica se basa en la toma de huella(s) y/o fotografía del ciudadano costarricense, que se deben de enviar al proveedor del servicio por medio de un enlace seguro con la información encriptada.

Estándares del proveedor de biometría para los ciudadanos costarricenses

El proveedor de biometría para los ciudadanos costarricenses es el Tribunal Supremo de Elecciones conforme a lo que se establece en el Convenio Marco entre el Poder Ejecutivo y el TSE, en su cláusula Segunda: Compromisos del Poder Ejecutivo incisos a y b.

Fotografía

La ICAO en su documento “Portrait Quality”, describe los requisitos y recomendaciones de mejores prácticas que deben aplicarse para la captura de retratos, estas capturas sirven como contenido de ISO/IEC 19794-5 y Estructuras de datos ISO/IEC 39794-5.

Formato de la foto

La fotografía debe ser a color, centrada y enfocada, para su formato se puede utilizar una de las siguientes codificaciones:

- Formato JPEG (ISO/IEC 10918-1)
- Formato JPEG-2000 (ISO/IEC 15444-1)
- Formato PNG (ISO/IEC 15948:2003)

Calidad de la fotografía

La fotografía tiene que ser neutral en cuanto al color y el reflejo natural del color de la piel, para lograr una foto de calidad no debe de haber saturación, todos los canales RGB deben tener al menos siete bits de variación en la intensidad, es decir que abarque un rango de al menos 128 valores únicos en la región de la imagen.

Todas las fotografías deben tener el enfoque y profundidad suficientes, la cámara debe ser capaz de representar con precisión los detalles faciales finos como arrugas y lunares.

Posición del rostro con respecto de la cámara

La foto tiene que mostrar a la persona mirando directamente al lente de la cámara, la fotografía tiene que guardar el aspecto natural del rostro.

Distancia del sujeto con respecto de la cámara

La distancia recomendada para una captura directa es de 1,0 m hasta 2,5 m según las mejores prácticas.

Posición y aspecto del rostro

La imagen en la fotografía debe reflejar la cabeza entera y la parte alta del cuello, los lados derecho e izquierdo del rostro deben estar completamente visibles. La persona fotografiada debe mirar directamente el lente de la cámara, la expresión del rostro debe ser natural y los labios deben estar cerrados. El rostro debe estar mirando fijo el lente de la cámara, la posición de la cabeza no puede estar torcida, no puede estar de perfil, no puede tener inclinaciones hacia arriba o abajo, debe estar en una posición horizontal con respecto del lente de la cámara.

La expresión del rostro

El rostro debe tener una expresión neutral, la persona no debe sonreír, la boca debe estar cerrada, los dientes no deben ser visibles y no se debe fruncir el ceño.

Dirección y visibilidad de los ojos

Los ojos deben mirar directamente hacia el lente de la cámara, ambos ojos deben de abrirse de forma natural, claramente visibles, no forzarse al abrirlos, no pueden estar cubiertos por cabello.

El fondo

El fondo de la fotografía debe ser liso sin sombras, no tener elementos decorativos. La foto tiene que mostrar solamente a la persona fotografiada, no puede verse ninguna otra persona u objeto.

Brillo y contraste

El rostro en todas las partes tiene que ser reflejado de manera nítida y con el contraste adecuado, en general el retrato debe tener brillo y buen contraste entre cara, cabello y fondo.

La iluminación (Luz)

El rostro debe estar bien iluminado, se tienen que evitar reflejos, sombras en el rostro y el efecto de ojos rojos. No se utilizarán filtros de polarización lineal delante de la lente de la cámara, ya que interfieren con las cámaras de enfoque automático y reducen o eliminan la piel, información de textura que podría ser utilizada por los algoritmos de comparación de imágenes faciales. El TSE utiliza una sola luz frontal con los ángulos recomendados.

Personas con anteojos

Los ojos tienen que estar bien visibles, el borde de los cristales y los marcos no pueden cubrir los ojos, los anteojos no pueden tener cristales de color u oscuros, los cristales no pueden reflejar la luz, no se pueden utilizar gafas de sol o gafas con filtros de polarización, se aplica una excepción cuando el sujeto afirma razón médica.

Cubiertas de la cabeza

La persona fotografiada no puede tener la cabeza cubierta salvo sea por razones religiosas, pero inclusive en esos casos debe ser visible sin distorsión ni sombras, desde la corona hasta la base de la barbilla, desde el punto de contacto superior entre la oreja izquierda y la cara, desde el punto de contacto superior entre la oreja derecha y cara, desde borde medio entre pelo y frente.

Accesorios faciales

La ornamentación facial que oscurece el rostro no es permitida, es permitida aquella que no interfiera en el rostro.

Dimensiones del retrato y ubicación de la cabeza

La cabeza debe estar centrada en el retrato, como se describe, la imagen debe estar entre el 74-80% de la foto, con respecto de la línea horizontal ocular. La distancia entre el borde

izquierdo y el punto medio de la cara debe estar entre 45-55% y la distancia vertical entre el borde superior y el centro de la cara debe estar entre el 30-50% del centro de la boca. Los puntos característicos referidos se describen en ISO/IEC 14496-2.

Huellas dactilares

En la revisión de la norma ANSI/NIST-CSL 1-1993, se aprobó un formato para el intercambio de huellas dactilares, este estándar define el contenido formato y unidades de medida para el intercambio de huellas dactilares. El TSE sigue las recomendaciones del estándar para realizar la captura de huellas, la captura estandarizada de la huella permite al motorbiométrico realizar una comparación eficiente y exitosa.

La huella dactilar o dermatoglifo es la impresión visible que produce el contacto de las crestas capilares de un dedo de la mano sobre una superficie o dispositivo biométrico. A la huella dactilar capturada, se le aplica un algoritmo matemático que toma en cuenta las características físicas de la huella, el algoritmo extrae los puntos específicos.

Puntos característicos de la huella

Cresta

La cresta es el relieve lineal que existe en la epidermis de ciertas zonas que, alternando con los surcos, forman el dibujo papilar. Son las rayas negras de una huella impresa en papel.

Bifurcación

Es una cresta que en algún momento de su trayectoria se divide en dos ramas, formando un ángulo más o menos agudo, adoptando una forma arqueada, estas pueden ser bifurcaciones hacia la izquierda o hacia la derecha.

Islote

Línea que es un poco más grande que el punto, formada por dos o más puntos.

Delta

Es un área de la huella digital donde hay una triangulación o división de las líneas.

Formato de la huella

- BMP: Se almacena un registro en formato BMP, este registro debe tener un tamaño específico y una profundidad de 8 bits. Esta información debería almacenarse cifrada y despersonalizada en cualquier institución pública o privada a nivel nacional para evitar que el robo o fuga de este tipo de información sirva para la materialización de riesgos al

darse violaciones de acceso a las cuentas digitales de ciudadanos. Además, esta información está catalogada como de acceso restringido por la ley 8968, ya que hacen a una persona identificable y deben ser tratados en consecuencia.

- Wavelet Scalar Quantization (WSQ): El algoritmo WSQ se usa para comprimir imágenes de huellas dactilares en escala de grises de 8 bits y de 500 dpi, el algoritmo fue desarrollado por el FBI y la NIST a principios de los años 90, bajo el estándar ANSI/NBS-CLS 1-1993.

El TSE comprime las huellas en formato estándar WSQ.

Minutiae

Son plantillas estandarizadas de una huella dactilar, que contiene una lista de características de fricción específicas de la huella. El primer estándar de minucias se estableció en 1986 por el FBI bajo el estándar ANSI/NBS-ICST 1-1986, la última versión de la norma aplicada es ANSI / NIST-ITIL 1-2007. Los puntos de minutia son características de la cresta local donde una cresta de piel de fricción comienza, termina o se divide en más crestas.

Calidad de la huella

La imagen de la huella en ocasiones presenta degradaciones, a causa de variaciones en la piel de la persona, existen diferentes razones que pueden afectar la calidad de la huella. El rendimiento de los algoritmos que extraen los puntos característicos de la huella o minucias, dependen de la calidad de la huella de entrada, es por eso que la calidad de captura es estrictamente vigilada. El TSE es muy riguroso en la aplicación de la calidad.

- NIST Fingerprint Image Quality: NFIQ (por sus SECIT en inglés) es un estándar creado por NIST, para medir la calidad de imagen de las huellas dactilares, en el documento NISTIR 7151, define los mecanismos de medición y clasificación. Una huella digital es un patrón de crestas de fricción en la superficie de la cresta de un dedo, una buena calidad permite la extracción de las características únicas de la huella. NFIQ utiliza la siguiente tabla para definir la calidad de una huella digital:

Q	QUALITY	RANGE
5	poor	$[0, W^{-1}(0.75)]$
4	fair	$(C^{-1}(0.75)], C^{-1}(0.05)]$
3	good	$(C^{-1}(0.05), C^{-1}(0.2)]$
2	very good	$(C^{-1}(0.2), C^{-1}(0.6)]$
1	excellent	$(C^{-1}(0.6), C^{-1}(1)]$

Fuente: NISTIR - 7151

El TSE, en su proceso de enrolamiento de las huellas de un ciudadano costarricense o naturalizado, solo acepta huellas cuando el valor de (NFIQ = 1 y 2), esto permite que sus algoritmos de extracción y comparación biométrica sean altamente precisos.

Dispositivos para captura de huellas

El TSE para realizar la captura o enrolamiento de las huellas de un ciudadano costarricense o naturalizado, utiliza lectores de huellas que cumplan con las siguientes características:

- Certificado por el FBI;
- Tecnología óptica con capacidad de soporte para 8 bits en escala de grises;
- Resolución mínima de 500 dpi;
- Debe cumplir con el estándar ANSI/INCITS 358-2002.

La siguiente herramienta permite identificar cuáles son los estándares de conexión, dispositivos y parámetros que las instituciones utilizan.

Herramienta para identificar los estándares de conexión, dispositivos y parámetros para Consumo			
Fecha de aplicación:			
Elementos	**¿Se utiliza?**		**Observaciones**
	Sí	**No**	
¿Se utiliza la firma digital certificada, respetando la normativa vigente de manera integral?			
¿Se utiliza la identificación y/o autenticación biométrica tales como huellas y/o fotografías o biometría comportamental?			
¿Se utilizan formatos para fotografías tales como JPEG, JPEG-2000 y PNG?			

¿La fotografía utilizada cuenta con calidad adecuada?			
¿La fotografía utilizada cuenta con la posición y distancia del rostro recomendada con respecto a la cámara?			
¿La fotografía utilizada cuenta con la dirección y visibilidad de los ojos, fondo, brillo, contraste e iluminación recomendado?			
¿La imagen se almacena de forma cifrada y despersonalizada en los sistemas de información?			
¿Se utilizan las huellas dactilares, con formatos como BMP y Wavelet Scalar Quantization?			
¿Se utiliza algún otro parámetro de conexión? (indicarlo en observaciones)			
¿Se utiliza algún otro medio de autenticación? (indicarlo en observaciones)			

Herramienta de Identificación y Autenticación Ciudadana, 1. Elaboración propia.

CAPÍTULO 3:

SEGURIDAD TECNOLÓGICA, SEGURIDAD DE LA INFORMACIÓN & CIBERSEGURIDAD

EQUIPO DE TRABAJO

Integrante	Institución
Ana María Castro	CCSS
Mario Robles	White Jaguars
Marvin Soto	Cybercom CR
Michell Cersosimo	Intel
Johnny Pan	MICITT
Comisión especial	CyberSec Clúster

INTRODUCCIÓN AL TEMA

De la mano de la evolución tecnológica, han surgido disciplinas a partir de la seguridad a ser aplicada en los distintos medios tecnológicos, dentro de ellas: seguridad informática, seguridad de la información y ciberseguridad.

El presente documento está orientado al establecimiento de los lineamientos en materia de Seguridad Tecnológica, Seguridad de la información y ciberseguridad, en adelante **STSI&C**, de forma tal que, cualquier nuevo proyecto que sea planteado haciendo uso de tecnologías digitales contemple la seguridad por diseño y con ello garantice el cumplimiento de los principios básicos transversales desarrollados, según el rol que como parte del proyecto se ejecute.

Los lineamientos se encuentran basados en estándares y mejores prácticas mundiales en las distintas disciplinas de la **STSI&C**, definiendo lo que se debe de cumplir; no así el cómo, lo cual queda circunscrito a la gestión local. Se han considerado dentro del desarrollo de estos lo normado por la Organización Internacional para la Estandarización ISO, en sus versiones 17799, 27001:2022, 27032:2017, así como la norma ANSI/TIA-942, el marco de ciberseguridad establecido por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos de América NIST y el Centro de Seguridad de Internet CIS, así como otros especializados según la materia.

Dichos lineamientos, evolucionarán acorde a la aparición de nuevas amenazas a nivel de hardware, software y otros recursos del ciberespacio; y garantizar la implementación de controles de seguridad con el propósito de disminuir los riesgos asociados al uso de los bienes y servicios que brindan las organizaciones.

Adicionalmente es de suma importancia considerar que, la industria usa y gestiona protocolos no solo atinentes a las Tecnologías de la Información (TI), sino también de Tecnologías Operativas (TO). Por lo que los estándares ISO/IEC 27400:2022 para la ciberseguridad y privacidad del IoT y el IEC 62443 – Ciberseguridad industrial, son considerados en este documento. Dado que la integración de las redes industriales modernas es incluyente tanto de las TI como de las TO.

Es imperativo para el país, contar con los lineamientos base en materia de **STSI&C**, de forma tal que toda iniciativa o proyecto a ser desarrollado cumpla con los mismos, como mecanismos que garanticen la aplicación de los controles de seguridad necesarios en la gestión de la información de la población y de los usuarios que intervienen en dichos proyectos o que son usuarios de los servicios donde se hace uso de su información, incluido el ciberespacio, así como de los mecanismos tecnológicos utilizados.

PRINCIPIOS

Se conocen como principios transversales a la **STSI&C**:

- **Confidencialidad:** Esto significa que la información es conocida, divulgada, accedida o utilizada únicamente por personas autorizadas. Por tanto, se deben establecer los controles necesarios para garantizar la confidencialidad y privacidad de la información que se procesa, almacena o distribuye a través de activos digitales.

- **Integridad:** Esto significa que la información es actualizada o modificada únicamente por personas autorizadas. Por tanto, se deben establecer los controles necesarios para garantizar la exactitud, completitud de la información que se procesa, almacena o distribuye a través de activos digitales.

- **Disponibilidad:** Esto significa que la información es accesible cuando los usuarios autorizados la requieran para operar con ella. Por tanto, se deben establecer los

controles necesarios para garantizar la disponibilidad de la información que se procesa, almacena o distribuye a través de activos digitales.

- **No repudio:** Prueba que el autor envió la comunicación (*no repudio en origen*) y que el destinatario la recibe (*no repudio en destino*). Por tanto, se deben establecer los controles necesarios para garantizar el evitar que un emisor o el receptor nieguen su participación en algún tipo de interacción que procesa, almacena o distribuye información a través de activos digitales.

Otros principios básicos que deben de considerarse como parte de la gestión de los nuevos proyectos que contemplen tecnologías digitales son:

- **Minimizar la superficie de ataque:** cada característica que se agrega a una solución tecnológica aumenta o disminuye riesgo de los sistemas de información en general, dependiendo de los niveles de control incorporados y su efectividad operativa. El objetivo del establecimiento de controles en general es reducir los niveles de exposición al riesgo, reduciendo el área o superficie de ataque.

- **Establecer valores predeterminados seguros:** hay muchas formas de ofrecer una experiencia predefinida para los usuarios. Esta debe considerar los aspectos de seguridad desde su conceptualización y los valores esenciales por ser configurados, mitigando la materialización de riesgos conocidos y por ende administrables.

- **Principio de privilegio mínimo:** recomienda que los perfiles de usuario posean la menor cantidad de privilegios necesarios para realizar sus procesos. Esto abarca derechos de usuario sobre las funcionalidades del sistema, permisos y accesos sobre los recursos tecnológicos, entre otros.

- **Principio de defensa en profundidad:** propone el uso de un conjunto de controles utilizados de forma complementaria, seguridad por capas, superpuesta o incremental para el diseño de una arquitectura de seguridad, utilizando niveles de control de acuerdo con su tipo (preventivo, correctivo, detectivo) o naturaleza (manual, automático, mixto), con el objetivo de aumentar la efectividad de la protección y disminuir los niveles de exposición e impacto ante la explotación exitosa se vulnerabilidades importantes.

- **Gestión de riesgos de terceros:** muchas instituciones utilizan las capacidades de procesamiento, almacenamiento o transferencia de datos mediante el uso de terceros

externos (cadena de suministro). Debido a esto las organizaciones deben gestionar el riesgo de terceras partes involucradas y cómo éstas puedan afectar su panorama de riesgos.

- **Segregación de funciones:** toda actividad de control a nivel operativo requiere de una adecuada separación o segregación de funciones para garantizar que una persona siempre valida y autoriza el trabajo de alguien más de manera formal. Es un principio fundamental de control interno que tiene como objetivo reducir el riesgo de errores o fraudes internos. Este principio se basa en la división de responsabilidades y tareas críticas entre diferentes personas o equipos, con el fin de asegurar que ninguna persona individual tenga el control total sobre un proceso o sistema crítico.
- **Confianza Cero:** enfoque arquitectónico para la seguridad de la red que asume que cada transacción, entidad e identidad no son de confianza hasta que se establece la confianza y la misma se mantenga a lo largo del tiempo. Es un modelo de seguridad que opera bajo el principio de "nunca confiar, siempre verificar" y asume que las amenazas pueden provenir tanto de dentro como de fuera de la red organizacional, y por lo tanto, todo acceso a recursos y datos debe ser restringido y verificado continuamente.
- **Seguridad por Diseño:** enfoque esencial en el ámbito de la ciberseguridad y la tecnología, que enfatiza la importancia de integrar medidas de seguridad desde las etapas iniciales de desarrollo y diseño, tanto en el software como en las arquitecturas tecnológicas. Este concepto se basa en la premisa de que la seguridad no debe ser un incluido posteriormente, sino como un componente fundamental en la creación y despliegue de cualquier sistema tecnológico

POLÍTICAS GENERALES

Se establece que, toda iniciativa o proyecto en el cual se considere el manejo de componentes tecnológicos, información, en entornos controlados o a nivel del ciberespacio debe contemplar la seguridad por diseño y cumplir con las medidas de seguridad requeridas de forma que se garantice la aplicación de los controles de seguridad para la protección de la confidencialidad, disponibilidad, integridad y no repudio sobre el producto y/o servicio que sea resultado de su consecución y acorde a la naturaleza del proyecto.

En cumplimiento de lo anteriormente definido, se han identificado lineamientos específicos

con base en las mejores prácticas, estándares mundiales y criterios expertos, esenciales para que, a nivel local se desarrolle el cómo implementar dichos lineamientos referenciado en dichas guías y en la realidad operativa de cada organización, favoreciendo la proyección en el tiempo, así como el mejoramiento continuo de las medidas en el entorno de la **STSI&C**.

POLÍTICAS ESPECÍFICAS

A continuación se enuncian los distintos lineamientos específicos, bajo el entendimiento que podrían requerirse algunos y no todos los lineamientos como producto de un análisis de aplicabilidad que se debe realizar en el momento de su evaluación preliminar cuando el proyecto sea presentado, considerando que la aplicación de los mismos no circunscriben exclusivamente al alcance del proyecto, sino deben de ser gestionados al nivel operativo del producto y/o servicio implementado, como parte de la sostenibilidad en el tiempo de forma segura.

A nivel seguridad de la información y seguridad informática:

- **Organización de la seguridad de la información:**
  Se entiende y se prioriza la misión, los objetivos, las partes interesadas y las actividades de la organización; esta información se utiliza para informar los roles, responsabilidades y decisiones de gestión de los riesgos de la seguridad de la información y la seguridad informática.

  El personal y los socios de la organización reciben educación de concienciación sobre la SECIT y son capacitados para cumplir con sus deberes y responsabilidades relacionados con la seguridad de la información y la seguridad informática, en conformidad con las políticas, los procedimientos y los acuerdos relacionados al campo.

  La información y los registros (datos) se gestionan en función de la estrategia de gestión de riesgos de la organización para proteger la confidencialidad, integridad y disponibilidad de la información, reforzando la seguridad y privacidad según los derechos de los ciudadanos, así como las leyes y regulaciones existentes.

- **Seguridad de los recursos humanos:**
  Se debe tener en cuenta la selección y contratación, la formación de empleados y los procesos

de terminación de la relación laboral y / o de un tercero.

- **Gestionar los activos:**
  Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización alcanzar los objetivos estratégicos se identifican y se administran de forma coherente con su importancia relativa para los objetivos organizacionales propuestos y la estrategia para la gestión de riesgos establecida por la organización.

- **Gestión de identidad, autenticacióny control de acceso:**
  El acceso a los activos físicos y lógicos y a las instalaciones asociadas está limitado a los usuarios, procesos y dispositivos autorizados, y se administra de forma coherente con el riesgo de acceso, actividades y / o transacciones evaluadas.

- **Criptografía:**
  El uso de criptografía es requerido para controlar el acceso y uso de datos de carácter restringido, los cuales deben ser accesibles únicamente por su titular como por ejemplo y no limitado a las contraseñas de las cuentas de usuario, pines, etc. Además, este tipo de datos deben utilizar mecanismos de almacenamiento con mecanismos de cifrado no reversible, conocidos como HASH. En caso de tratarse de datos de uso y almacenamiento compartido como por ejemplo registros de datos clasificados como confidenciales, deben utilizarse mecanismos de cifrado según sea requerido. Finalmente, en todos los casos los datos en tránsito mediante el uso de medios digitales, deben transitar utilizando mecanismos de cifrado que garanticen su integridad y confidencialidad.

- **Seguridad física de los sitios y equipos de la organización:**
  Se deben identificar y establecer medidas de control físicas para proteger adecuadamente el acceso a los activos digitales, con el propósito de evitar incidentes que afecten a la integridad física o interferencias no deseadas sobre estos.

- **Seguridad física y operacional:**
  Deben establecerse las medidas para asegurar la operación correcta y segura de las instalaciones de procesamiento de datos.

- **Comunicaciones seguras y transferencia de datos:**
  La protección de la información en redes y la protección de la infraestructura de soporte, debe garantizar controles para el aseguramiento de la red, servicios de red seguros, así como la segregación de redes, entre otros.

- **Adquisición de sistemas, desarrollo y soporte de sistemas de información:**

  Los proyectos de desarrollo o adquisición de aplicaciones, así como su mantenimiento considera las prácticas de seguridad vigentes de la industria, mediante procesos de desarrollo seguro de aplicaciones que promuevan la debida diligencia para la identificación y corrección de defectos en el código de programación.

  Arquitectura, diseño y modelado de amenazas

  Incluir procesos de seguridad dentro de metodologías de desarrollo de aplicaciones utilizadas tomando en cuenta la diversidad de procedimientos que abarcan desde la evaluación de arquitectura de aplicaciones, el modelado de amenazas, ciclo de vida de desarrollo seguro (Secure SDLC) y seguridad dentro de metodologías ágiles junto con procesos automatizados (DevSecOps).

  Autenticación

  Los mecanismos de autenticación, también conocidos como de identificación o de inicio de sesión que deben garantizar la verificación de la identidad del usuario siguiendo las mejores prácticas para prevenir el mal uso o el abuso por parte de usuarios o sistemas no autorizados. Sobre este tema se recomienda la aplicación de la guía de NIST 800-63.

  Gestión de sesiones

  La permanencia de un usuario autenticado en una plataforma debe implementarse de forma segura garantizando que el acceso concedido por un tiempo determinado y no susceptible a abusos o el secuestro por parte de usuarios maliciosos.

  Control de acceso

  Los usuarios autenticados deben poseer el acceso a los recursos informáticos sin que exista la posibilidad de abusar de las funcionalidades para obtener accesos no autorizados.

  Validación, filtrado y codificación

  La información recibida por las aplicaciones debe a) validar que los datos recibidos corresponden al tipo esperado para el correcto funcionamiento de la aplicación, b) cuando sea necesario filtrar aquella información que se considere como potencialmente insegura para el comportamiento de la aplicación y c) que la información enviada al usuario es presentada utilizando la codificación adecuada previniendo la posibilidad de envío de información maliciosa al usuario.

Manejo de errores y registro de eventos

Se entiende que toda aplicación es susceptible a poseer errores. Por ello, se debe ejecutar un proceso para el control de errores que evite que los usuarios reciban más información de la requerida. Todo error debe registrarse de forma segura y privada donde los responsables en la toma de decisiones los puedan recibir y analizar sin comprometer los sistemas de información.

Protección de datos

Los datos que se encuentren protegidos por leyes de protección ya sean locales o de otras legislaciones aplicables para asegurar su seguridad y / o privacidad, deben resguardarse de acuerdo con los lineamientos que dicte el cumplimiento legal o regulatorio vigente.

Comunicaciones

Las comunicaciones entre aplicaciones o entre las aplicaciones y los usuarios finales, se deben realizar utilizando canales seguros con mecanismos de cifrado considerados como vigentes para el momento de su evaluación. De igual forma las comunicaciones digitales deben ser accesibles sólo por los recursos o usuarios requeridos.

Protección ante código malicioso

Los procesos de desarrollo de aplicaciones y productos utilizados por la organización deben contener controles de integridad del código que garanticen que no han sido modificados por terceros maliciosos. Adicionalmente, deben existir medidas de protección que eviten el mal uso de la aplicación o la plataforma donde se encuentra instalada dicha aplicación, evitando la inclusión o difusión de código o aplicaciones que puedan causar efectos maliciosos.

Configuración

Tanto las aplicaciones, así como las librerías, componentes u otros artefactos utilizados para el desarrollo y la implementación de aplicaciones deben estar configuradas de forma segura siguiendo las prácticas de aseguramiento o recomendaciones brindadas por los fabricantes. Así mismo, todos los mencionados deben corresponder a las últimas versiones estables disponibles y deben estar libres de vulnerabilidades reportadas públicamente. Para el mantenimiento de plataformas se debe seguir un proceso de aplicación de parches de seguridad producto del descubrimiento de nuevas vulnerabilidades identificadas posteriormente a la implementación de las soluciones de aplicaciones.

Mantenimiento

El mantenimiento y la reparación de los componentes de aplicaciones y de control industrial

se deben realizar de acuerdo con las políticas y procedimientos establecidos.

- **Seguridad para proveedores y terceros:**

  En caso de que empresas o personal externo a la organización tengan acceso a los sistemas de información o a los recursos digitales que procesan, almacenan o distribuyen activos de información se deben establecer los controles requeridos para el uso seguro de dichos activos y supervisar el cumplimiento de dichos controles.

- **Gestión de eventos o incidentes de seguridad:**

  Detección de eventos o incidentes de seguridad:

  Se dispone de mecanismos de detección de actividad anómala y se comprende el impacto potencial de los eventos o incidentes que pueden afectar la seguridad de la información.

  Monitoreo de eventos o incidentes de seguridad:

  Los activos digitales y los activos de información son monitoreados con el propósito de identificar eventos de ciberseguridad y verificar la eficacia de los controles.

  Planificación de respuesta a eventos o incidentes de seguridad:

  Los procesos y procedimientos se registran, clasifican, analizan, documentan y envían con el propósito de garantizar una respuesta oportuna y eficaz a los eventos o incidentes de seguridad detectados.

  Análisis de incidentes de seguridad:

  Se lleva a cabo el análisis para garantizar una respuesta y recuperación eficaz de los servicios que habilitan los sistemas de información.

  Contención de eventos o incidentes de seguridad:

  Se realizan actividades para contener los eventos o incidentes de seguridad, mitigar sus efectos y la recuperación eficaz de los servicios que habilitan los sistemas de información.

  Mejora continua en la respuesta a eventos o incidentes de seguridad:

  Las actividades de respuesta de la organización deben mejorarse incorporando las lecciones aprendidas producto de la gestión de eventos o incidentes de seguridad.

  Comunicación de eventos o incidentes de seguridad:

  Las actividades de respuesta deben coordinarse con las partes interesadas, tanto internas como externas, incluyendo el apoyo de organismos encargados de hacer cumplir la ley.

Planificación de la recuperación de eventos o incidentes de seguridad:

Los procesos y procedimientos de recuperación deben ejecutarse y mantenerse para asegurar la restauración de los sistemas de información o activos de información afectados por eventos o incidentes de seguridad.

Gestión del proceso de recuperación ante eventos o incidentes de seguridad:

Las actividades de restauración deben coordinarse con partes internas y externas (por ejemplo, centros de coordinación, proveedores de servicios de Internet, propietarios de sistemas de ataque, victimas, otros CSIRT, vendedores o fabricantes).

Sobre la gestión de incidentes de seguridad se recomienda la aplicación de la guía de NIST 800-61 y la ISO 27035.

- **Aspectos de seguridad en la gestión de la continuidad del negocio:**
  Las soluciones técnicas de seguridad deben gestionarse para garantizar la seguridad y la capacidad de recuperación de los sistemas de información y activos de información, en consonancia con las políticas, procedimientos y acuerdos relacionados.

- **Conformidad:**
  Se establecen los mecanismos para certificar que, las partes están conformes con las medidas de control establecidas para garantizar la SECIT.

- **Generación de normativa para el gobierno y la gestión de la seguridad:**
  Se mantienen y se aprueban los procesos y procedimientos para la identificación, cuantificación, monitoreo, tratamiento y respuesta a eventos e incidentes de seguridad.

- **Gestión integral del riesgo:**
  La organización comprende el gobierno y la gestión de los riesgos de seguridad de la información y la ciberseguridad y su importancia para las operaciones de la organización (incluida la misión, las funciones, la imagen o la reputación), los activos de la organización y las personas. Se establecen las prioridades, restricciones, tolerancias de riesgo, tratamiento y suposiciones de la organización, que se usan para respaldar las decisiones de riesgos operacionales.

  A continuación, se brinda una herramienta que permite identificar los lineamientos relacionados con la gestión de la ciberseguridad y la seguridad de información, los cuales

deben ser analizados y evaluados de acuerdo con el panorama de riesgos de la institución y gestionados de acuerdo con las políticas y procedimiento de gestión de riesgos.

Herramienta para identificar los lineamientos de seguridad informática y seguridad de la información					
Fecha de aplicación:					
Nombre del proyecto:					
Lineamientos	**¿Cumple?**		**Acción por realizar**	**Unidad/persona responsable de la acción**	**Fecha para ejecutar las acciones.**
	Sí	**No**			
Organización de la seguridad de la información					
¿Se estableció la misión, objetivos, partes interesadas y actividades de la organización, para la gestión de riesgos de la seguridad de la información?					
¿El personal y socios de la organización reciben capacitación sobre la SECIT y el cumplimiento de deberes relacionados con la seguridad de la información?					
¿La información y registros se gestionan en función de la estrategia de riesgo existente en la organización?					
Seguridad de los recursos humanos					
¿Se tiene en cuenta la selección y contratación, formación de empleados y salida de los participantes del proyecto?					
Gestión de activos					

¿Se administran correctamente los datos, dispositivos, sistemas y las instalaciones que permiten el alcance de objetivos?					
¿Se cuenta con un inventario de los activos (Sistemas, aplicaciones, servicios, etc)?					
Gestión de la identidad, autenticación y control de acceso					
¿El uso de activos físicos, lógicos y las instalaciones asociadas está limitado a los usuarios, procesos y dispositivos autorizados?					
¿Se cuenta con doble factor de autenticación en servicios expuestos a internet (VPN, Correo, sistemas)?					
Criptografía					
¿Se utiliza la criptología para la información de acceso restringido?					
¿Se tiene conocimiento y se utilizan mecanismos de cifrado no reversibles (HASH) para información personal?					
Seguridad física de los sitios					
¿Se implementan medidas de control físicas para proteger los activos de información?					
Seguridad operacional					
¿Existen medidas para asegurar la correcta y segura operación de instalación de procedimientos de información?					

Comunicaciones seguras					
¿La protección de la información en redes e infraestructura de soporte está plasmada en los controles de aseguramiento de la Red?					
Adquisición de sistemas, desarrollo y soporte de sistemas de información					
¿Se siguen las prácticas de seguridad vigentes al desarrollar proyectos de software, tales como la arquitectura, diseño y modelado de amenazas?					
¿Se garantiza la veracidad de identidad del usuario por medio de mecanismos de autentificación?					
¿La gestión de sesiones del usuario se implementa de forma segura, evitando la susceptibilidad a abusos o secuestro por parte de usuarios maliciosos?					
¿Los usuarios identificados o no identificados poseen acceso a la plataforma sin que exista posibilidad de abusar de la funcionalidad para acceder a la información?					
¿Se realizan procesos de validación, filtrado y codificación de la información recibida?					
¿Se cuenta con un seguimiento de control de errores, registrados de forma segura y privada?					

¿Se resguarda la información protegida por leyes de protección de datos siguiendo los lineamientos que dicte el cumplimiento regulatorio?					
¿Se utilizan canales de comunicación seguros con mecanismos de cifrado?					
¿Se utilizan controles que garanticen la protección ante códigos maliciosos?					
¿Las plataformas utilizadas para el desarrollo de software están configuradas de forma segura y siguen las prácticas de aseguramiento brindadas por los fabricantes?					
Cifrado no reversibles (HASH) par información personal?					
Seguridad física de los sitios					
¿Se implementan medidas de control físicas para proteger los activos de información?					
Seguridad operacional					
¿Existen medidas para asegurar la correcta y segura operación de instalación de procedimientos de información?					
Comunicaciones seguras					

¿La protección de la información en redes e infraestructura de soporte está plasmada en los controles de aseguramiento de la Red?					
Adquisición de sistemas, desarrollo y soporte de sistemas de información					
¿Se siguen las prácticas de seguridad vigentes al desarrollar proyectos de software, tales como la arquitectura, diseño y modelado de amenazas?					
¿Se garantiza la veracidad de identidad del usuario por medio de mecanismos de autentificación?					
¿La gestión de sesiones del usuario se implementa de forma segura, evitando la susceptibilidad a abusos o secuestro por parte de usuarios maliciosos?					
¿Los usuarios identificados o no identificados poseen acceso a la plataforma sin que exista posibilidad de abusar de la funcionalidad para acceder a la información?					
¿Se realizan procesos de validación, filtrado y codificación de la información recibida?					
¿Se cuenta con un seguimiento de control de errores, registrados de forma segura y privada?					

¿Se resguarda la información protegida por leyes de protección de datos siguiendo los lineamientos que dicte el cumplimiento regulatorio?					
¿Se utilizan canales de comunicación seguros con mecanismos de cifrado?					
¿Se utilizan controles que garanticen la protección ante códigos maliciosos?					
¿Las plataformas utilizadas para el desarrollo de software están configuradas de forma segura y siguen las prácticas de aseguramiento brindadas por los fabricantes?					
¿Se realiza el mantenimiento y reparación de componentes del sistema de información y de control industrial siguiendo políticas y procedimientos establecidos?					
Seguridad para proveedores y terceros					
¿Se establecen condiciones formales para empresas o personal externo a la organización que tengan acceso a los sistemas de información?					
Gestión de incidentes de seguridad de la información					
¿Se dispone de mecanismos de detección de actividad anómala?					

¿Se monitorean los sistemas de sistemas de información y activos, para identificar eventos de seguridad cibernética y efectividad de medidas de protección?					
¿Se le da respuesta, se evita y se mejoran los incidentes de seguridad detectados?					
¿Se comunican las respuestas a incidentes detectados a las partes interesadas?					
¿Se ejecutan procesos y procedimientos para asegurar la restauración de los sistemas o activos afectados por incidentes de seguridad informática?					
¿Se coordina con partes internas y externas las actividades de restauración ante incidentes de seguridad informática?					
Aspectos de seguridad de la información en la gestión de la continuidad del negocio					
¿Se gestionan soluciones técnicas de seguridad para garantizar la seguridad y capacidad de recuperación de sistemas y activos?					
Conformidad					
¿Se establecen mecanismos para certificar que las partes están conformes con las medidas para garantizar la SECIT?					
Generación de normativa para la seguridad de la información					

¿Se mantienen y aprueban los procesos y procedimientos de detección para garantizar el conocimiento de los eventos anómalos?					
Gestión integral del riesgo					
¿Se establecen las prioridades, restricciones, tolerancias de riesgo, mitigación y suposiciones de la organización, que se usan para respaldar las decisiones de riesgos operacionales?					

Herramienta de Seguridad Tecnológica, 1. Elaboración propia.

A nivel de Ciberseguridad:

- **Controles a nivel de aplicación:**

  La arquitectura de ciberseguridad debe de contar con un inventario oficial de aplicaciones autorizadas, el cual debe actualizarse periódicamente, promoviendo la actualización de aplicaciones y el soporte por parte del fabricante. Para más detalles visite NIST SP 800-53.

  Como guía considere implementar las siguientes capacidades:

  - Limitar los permisos administrativos por parte de los usuarios en los equipos de usuario final y servidores, controlando la instalación de aplicaciones no autorizadas o potencialmente maliciosas.
  - Escanear y validar la integridad a nivel de archivos del sistema operativo cuando sea posible, como medida de protección contra programas maliciosos.

- **Controles para protección de equipos:**

  La arquitectura de ciberseguridad debe de contar con procedimientos para levantar y mantener un inventario de activos digitales necesarios para la operación de la organización.

Como guía considere implementar las siguientes capacidades:

- Limitar los permisos administrativos para autorizar la conexión de un nuevo dispositivo a la red que no cumpla con las políticas y requerimientos de seguridad establecidos.
- Garantizar que mantiene un inventario actualizado de todos los dispositivos que están conectados a la red y sus correspondientes responsables. Se sugiere, monitorear toda actividad DHCP dentro de la red utilizada para autorizar los servicios de red disponibles en aquellos dispositivos que se conectan de forma exitosa.
- Puede utilizar las herramientas para el monitoreo y correlación de eventos de seguridad y redes para optimizar las capacidades para la detección de nuevos dispositivos.

Por otra parte, se debe contar con procedimientos para la actualización periódica de firmware, controladores y parches del sistema operativo, aplicaciones y equipos, asegurando que se encuentran instaladas las últimas versiones que mitigan vulnerabilidades conocidas, acompañado de la documentación y control operativo de la ejecución de dichas actividades.

Como guía considere implementar las siguientes capacidades:

- Verificar y remediar la existencia de aplicaciones desactualizadas, mediante el uso de herramientas para el escaneo de vulnerabilidades tanto en aplicaciones, como equipos conectados a la red.

- **Listas de aplicaciones aprobadas para el uso dentro de la organización:**
  La arquitectura de ciberseguridad debe contar con listas de aplicaciones permitidas para su instalación y uso.

  Como guía considere implementar las siguientes capacidades:

  - Garantizar la existencia y mantenimiento de un inventario con todas las aplicaciones autorizadas por las políticas de la institución.
  - En la medida de lo posible crear listas de aplicaciones permitidas (whitelisting, para más detalles visite NIST SP 800-167) que puedan utilizarse para flexibilizar el control operativo y aplicaciones prohibidas (blacklisting) que puedan servir para la apoyar la creación de políticas automatizadas para la eliminación de aplicaciones no deseadas o no autorizadas.

- **Gestión continua de vulnerabilidades:**
  La arquitectura de ciberseguridad debe contar con procedimientos para la verificación periódica de vulnerabilidades, particularmente en las plataformas con exposición al Internet, buscando reducir el impacto que podría generarse ante la explotación de vulnerabilidades por

parte de un agente de amenaza.

Como guía considere implementar las siguientes capacidades:

- Garantizar la existencia de un proceso que identifique vulnerabilidades en equipos, aplicaciones y procesos operativos de forma continua y defina acciones de tratamiento para limitar los niveles de exposición.
- Utilizar aplicaciones especializadas para la identificación de vulnerabilidades en equipos y aplicaciones de forma automatizada.
- Complementar las fuentes de información de vulnerabilidades a través de boletines de amenazas, noticias de seguridad, actualizaciones de los fabricantes, bases de datos de vulnerabilidades, entre otros.

- **Desarrollo de planes de continuidad de las operaciones:**

La arquitectura de ciberseguridad debe contar con la planificación de la continuidad de las operaciones. Para ello, la institución debe identificar y definir un plan para la recuperación expedita de aquellos activos digitales que habilitan los procesos y servicios críticos de la institución, ante la ocurrencia de eventos o incidentes de ciberseguridad.

Adicionalmente es importante indicar que los planes de continuidad por desarrollar, deben estar acompañados de un documento de análisis de impacto de operaciones, insumo indispensable para la identificación, priorización y el desarrollo del plan de continuidad.

Como guía considere implementar las siguientes capacidades:

- Identificar los procesos o servicios críticos que la institución requiere para poder operar y cumplir sus objetivos.
- Identificar, clasificar y determinar el nivel de importancia de la información que se requiere para poder operar.
- Realizar un análisis sobre distintos escenarios de riesgo de ciberseguridad puedan provocar impactos relevantes de acuerdo con el panorama y contexto institucional.
- Documentar las actividades de respuesta a eventos o incidentes de ciberseguridad según los niveles de exposición, posible afectación a los procesos o servicios críticos asociados, la información que pueda verse afectada o comprometida, así como el impacto que puedan generar a la institución.
- Desarrollar pruebas periódicas para medir la efectividad de los controles y planes de respuesta a eventos o incidentes de ciberseguridad.
- Contar con un Plan de Recuperación de Desastres (DRP), el cual es un componente

crítico de la estrategia de continuidad de negocios y gestión de riesgos de una organización. Se centra en la recuperación y protección de una organización o infraestructura tecnológica en caso de desastres o incidentes graves que puedan causar interrupciones o daño.

- **Uso controlado de privilegios administrativos:**

  La arquitectura de ciberseguridad debe contar con políticas para la creación de contraseñas, uso responsable de los recursos tecnológicos, creación de cuentas de usuarios, perfiles de acceso y cualquier otro tipo control de acceso a los activos digitales de la institución.

  Como guía considere implementar las siguientes capacidades:

  - Crear y mantener un inventario de todas las cuentas de un usuario en los diferentes sistemas de la institución y en la medida de lo posible buscar hacerlo de forma centralizada.
  - Aplicar políticas para la creación de contraseñas únicas y robustas, de acuerdo con los estándares de la institución y mejores prácticas de la industria.
  - Deshabilitar toda cuenta que no haya sido utilizada durante un período mayor a 45 días de acuerdo con las mejores prácticas de la industria o los estándares establecidos por la institución.
  - Restringir el uso de cuentas privilegiadas y en la medida de lo posible administrarlas a través de un proceso operativo mancomunado o automatizado mediante el uso de soluciones PAM (privileged account management).
  - Considerar el uso de doble factor de autenticación para todas las cuentas privilegiadas y de usuario final en la medida de lo posible.
  - Crear y mantener un inventario de cuentas de servicio.
  - Ejecución de campañas de recertificación de funciones y cuentas de usuario, con una periodicidad de al menos dos veces al año.

- **Registro, monitoreo y análisis de registros de auditoría:**

  La arquitectura de ciberseguridad debe contar con la activación de las pistas de auditoría en los sistemas de información como lo son las bitácoras. Para poder realizar un manejo eficiente de estas bitácoras, se requiere el uso de herramientas automatizadas que faciliten el registro, monitoreo, detección y correlación centralizada de posibles amenazas para su respectivo análisis y tratamiento. Para más detalles visite NIST SP 800-61.

  Como guía considere implementar las siguientes capacidades:

  - Garantizar que todos los equipos estén utilizando la misma fuente de hora para facilitar

la correlación y el análisis de eventos o incidentes. Para más detalles visite NTP pools.

- Revisar y definir cuidadosamente qué información registrar y analizar utilizando soluciones SIEM.
- Definir qué alertas deben ser atendidas y con qué nivel de prioridad e importancia. Para más detalle visite White Paper- SANS Institute.

Considere cuestionarse:

  - ¿Qué considerar como una alerta crítica de seguridad?
  - ¿Quién y cómo deben recibir dichas alertas?

- Considerar almacenar en la medida de lo posible las siguientes bitácoras. Para más detalle visite NIST SP 800-92:
  - Equipos de red: switches, enrutadores, firewalls, puntos de acceso, controladores inalámbricos y dispositivos IoT.
  - Servidores: Controladores de dominio, servidores de aplicaciones, servidores de bases de datos, servidores web, servidores de archivos.
  - Estaciones de trabajo: bitácoras de seguridad.
  - Plataformas de seguridad de terceros: Proxy y filtrado web, soluciones anti malware, seguridad de dispositivos de usuario final, gestión de identidad, IDS/IPS.

- **Protecciones de correo electrónico y navegadores Web:**

  La arquitectura de ciberseguridad debe contar con herramientas de filtrado de contenidos, filtrado de nombres por dirección IP, DNS, palabras clave, entre otros; que permitan regular el acceso a sitios de acuerdo con las políticas de uso aceptable y responsable de los recursos digitales.

  Como guía considere implementar las siguientes capacidades:

  - Gestionar la validación de archivos adjuntos del correo antes de entregárselo a los buzones de los clientes.
  - Implementar el filtrado de sitios permitidos y no permitidos en la navegación web de todos los usuarios.
  - Utilizar mecanismos de autenticación de correos entrantes combinando tecnologías SPF con DMARC o DKIM.

- **Protección contra programas maliciosos:**

  La arquitectura de ciberseguridad debe contar con sistemas de aplicaciones o equipos

especializados en la protección contra programas maliciosos. Todos los equipos (servidores, equipos de usuarios final, equipos móviles, etc), sistemas y/o redes deberán estar protegidos por este tipo de soluciones, para minimizar los riesgos de infección por programas maliciosos como virus, botnets, gusanos, troyanos, keyloggers, spywares, adwares, entre otros.

Como guía considere implementar las siguientes capacidades:

- Considerar la implementación de anti virus, anti programa malicioso (anti malware), aplicaciones de detección y respuesta (EDR), entre otros; con el propósito de identificar la presencia y acciones no deseadas de programas maliciosos.
- Registrar, monitorear, analizar y controlar acciones anómalas identificadas.
- Detectar toda actividad maliciosa (HIDS) a nivel del sistema operativo, medios removibles, instalación de programas maliciosos, manipulación del sistema operativo o aplicaciones de seguridad, elevación de privilegios, entre otros; así como a nivel de la red (NIDS) como la identificación de actividades de comando y control (C2), DNS o solicitudes URL maliciosas.

- **Control y limitación de puertos de red, protocolos y servicios:**

  La arquitectura de ciberseguridad debe configurar la protección de todos los dispositivos de la red a nivel de diseño.

  - Segregar a nivel del diseño de la arquitectura de red, los activos digitales que soportan los servicios críticos o esenciales de la institución, de los equipos de usuario final.
  - Cerrar o inactivar puertos, protocolos o servicios no utilizados, entre otros;
  - Escanear los activos digitales con el propósito de identificar las vulnerabilidades y compararlas contra una línea base o estándar permitido.
  - Complementar el uso de cortafuegos a nivel de la red con cortafuegos a nivel de los equipos y/o aplicaciones.

- **Recuperación de datos:**

  La arquitectura de ciberseguridad debe contar con los mecanismos de respaldo de información relevante que aseguren la recuperación de los servicios críticos o esenciales en caso de materializarse escenarios de riesgo de ciberseguridad. Unido a lo anterior, deben de establecerse las políticas y procedimientos para la identificación y selección de los datos por respaldar, tipos de respaldo, control de acceso físico y lógico, mecanismos de cifrado eficientes y efectivos según naturaleza y criticidad de los datos, pruebas de restauración y el traslado a sitios alternos y seguros de almacenamiento.

Como guía considere implementar las siguientes capacidades:

- Establecer políticas y procedimientos para definir y priorizar los datos deben respaldarse.
- Definir las estrategias y tipos de respaldos de datos por utilizar.
- Definir los períodos de retención de los respaldos de datos.
- Establecer mecanismos de protección físicos para los respaldos de datos.
- Evaluar la necesidad de mecanismos de protección lógica (cifrado) para los respaldos de datos, especialmente cuando se trate de datos protegidos por leyes o regulaciones, que se almacenan en infraestructuras tecnológicas en control de terceros (ejemplo: nube).
- Realizar pruebas de restauración e integridad de los respaldos de datos.
- Asegurar que los sistemas de respaldos de datos no sean direccionables a través de llamadas del sistema operativo o direcciones compartidas, para evitar el cifrado automatizado de respaldos de datos por ataques tipo ransomware.

- **Configuración segura de dispositivos de red:**

  La arquitectura de ciberseguridad debe contar con una estandarización de la línea base de configuración de todos los dispositivos de red.

  - Estandarizar la configuración segura (hardening) a todos los equipos de red como cortafuegos (firewalls), enrutadores (routers), conmutadores (switches), sistemas de detección de intrusos (IDS), sistemas de prevención de intrusos (IPS), equipos DHCP/DNS o de control de acceso a la red (NAC), entre otros.
  - Comparar de forma periódica y en la medida de lo posible de forma automatizada, la configuración segura de los equipos de red contra los estándares establecidos para identificar desviaciones.
  - Complementar los controles de acceso a cuentas administrativas de los equipos de red con el uso de doble factor de autenticación en la medida de lo posible.

- **Defensa perimetral:**

  La arquitectura de ciberseguridad debe contar con sistemas para el control del flujo del tráfico a través de la zona desmilitarizada (DMZ), cortafuegos (firewalls), proxies, IDS/IPS, accesos remotos, entre otros.

  Como guía considere implementar las siguientes capacidades:

  - Crear zonas desmilitarizadas entre las redes internas y el internet.

- Segmentar las redes y utilizar proxies para controlar de forma más efectiva el flujo de los datos y sitios maliciosos visitados por los usuarios finales.
- Considerar la aplicación de listar negras para bloquear tráfico malicioso de direcciones IP conocidas.
- Implementar estratégicamente el uso de sistemas de detección de intrusos de red (IDS) para alertar sobre tráfico malicioso o patrones conocidos de ataque y sistemas prevención de intrusos (IPS) de red para bloquear cualquier tráfico malicioso o patrones conocidos de ataque.
- Recolectar, correlacionar, monitorear y analizar toda la información posible de la red con el objetivo de identificar conexiones no autorizadas, conexiones TCP o UDP por períodos extendidos de tiempo, actividad SSH o RDP inusual, conexiones a puertos indefinidos, conexiones VPN no autorizadas, barridos de red, sistemas interactuando con IPs maliciosas o asociadas a indicadores de compromiso (IOCs), entre otras anomalías de red.
- Monitorear y dar trazabilidad a toda conexión de acceso remoto.

- **Protección de datos:**

  La información se categoriza por niveles, se basa en el grado de sensibilidad ante el mal uso y su divulgación, se encuentra en cumplimiento con regulaciones de protección de datos vigentes y aplicables tanto local como internacional, que protegen a las personas ante el tratamiento de sus datos. Utilizar mecanismos de cifrado en los medios de almacenamiento donde reside información catalogada como sensible.

  Como guía considere implementar las siguientes capacidades:

  - Identificar información como contraseñas y otros datos confidenciales, sensibles disponibles en texto sin formato.
  - Monitorear los intentos de vulneración de los sistemas.
  - Identificar el uso de servicios de transferencia de archivos y datos basados en la nube.
  - Identifica los datos confidenciales, los sistemas que los albergan y los mejores esquemas de protección posibles para reducir las posibilidades de fuga y exfiltración.

- **Controles de acceso para redes inalámbricas:**

  Con respecto a los puntos de acceso de redes inalámbricas, debe de existir un inventario de dispositivos autorizados para ser utilizados, ejecutar tareas de forma periódica para la detección de dispositivos de redes no autorizadas. Las redes inalámbricas deben estar

configuradas utilizando los protocolos de cifrado vigentes y recomendados como seguros para el momento de su evaluación.

Las redes inalámbricas, si requieren acceso de forma pública, debe de contar con mecanismos para la identificación de los usuarios, restricción de acceso a servicios definidos como restringidos, detectar el mal uso y el abuso de la plataforma, adicionalmente estas redes de acceso público deben estar aisladas de las redes internas de la organización y existir mecanismos que controlan el acceso solo a los recursos estrictamente requeridos para el funcionamiento operacional.

Las comunicaciones para los dispositivos que no lo requieren para su funcionamiento fundamental serán deshabilitadas, se utilizan tecnologías de comunicación Bluetooth solo cuando es estrictamente requerido para en funcionamiento mínimo siempre que el dispositivo no contenga información o tenga acceso directo a información considerada como sensible.

Como guía considere implementar las siguientes capacidades:

> Identificar puntos de acceso inalámbricos no autorizados y detectar dispositivos desconocidos que se conectan a la red inalámbrica para reducir las amenazas.
>
> Revisa los puntos de acceso inalámbrico existentes, los controles de acceso a la red y el uso de LAN virtuales dentro de la organización para identificar cualquier brecha y determinar mejoras en la seguridad.

- **Monitoreo y control de credenciales:**

  Utilizar múltiples factores de autenticación para sistemas con acceso a información clasificada como sensible o que requiera de acceso privilegiado, contar con mecanismos centralizados para la gestión de usuarios y niveles de acceso, procedimientos para la solicitud, aprobación y revocación tanto para cuentas de usuario como para los distintos niveles de acceso que se encuentren disponibles y un registro de eventos para recolectar evidencia sobre inicios de sesión fallidos.

  Las contraseñas no deben ser almacenadas utilizando mecanismos de cifrado que sean reversibles y en su lugar deben ser almacenadas con valores no reversibles llamados Hash generados a partir de los protocolos y algoritmos considerados como seguros para el momento de la evaluación.

  Deben de existir y estar implementados mecanismos para la inhabilitación de cuentas de

usuario no utilizadas dentro de un periodo determinado de tiempo, mecanismos de bloqueo y/o de expiración de sesiones inactivas y mecanismos de alerta para la notificación de intentos de ingreso no autorizados.

Como guía considere implementar las siguientes capacidades:

Auditar y monitorear los controles de autenticación del sistema.
Revisión de contraseñas débiles y compartidas y alertan sobre posibles ataques basados en autenticación o uso indebido de privilegios.

Examinar los procesos de revisión de registros de autenticación existentes y garantizar que las políticas de control de autenticación se sigan adecuadamente por los funcionarios.

- **Programas de entrenamiento y cultura de seguridad:**

Contar con mecanismos de evaluación implementados con los que se califique el estado actual del conocimiento de los funcionarios en materia de buenas prácticas de seguridad de la información, con evidencia proporcionada por un ente imparcial. Tener programas de capacitación en materia de seguridad de la información, que se realicen al menos una vez al año, asegurarse que dentro del paquete de inducción de todos los funcionarios se den las capacitaciones de cultura de seguridad.

Como guía considere implementar las siguientes capacidades:

Evaluar y mejorar el conocimiento de todos los funcionarios a través de campañas de capacitación sobre temas tales como phishing, ingeniería social y la identificación del uso indebido y abuso de activos.
Determina si las directivas de control de autenticación se siguen adecuadamente.

- **Respuesta y gestión de incidentes:**

Implementación de procesos para la gestión y respuesta de incidentes en seguridad de la información, establecer los responsables de la gestión, sus roles, y contar con la información de contacto del personal a cargo de atender el incidente.

Contar con mecanismos de asignación de puntajes y de priorización de incidentes basados en criterios de impacto definidos con base en las necesidades específicas de la organización.

Como guía considere implementar las siguientes capacidades:

Realizar pruebas de las capacidades existentes de respuesta a incidentes, con el fin de poder establecer los procesos de detección y respuesta, opcionalmente a través de tecnología o un servicio gestionado.

Optimizar los procesos de monitoreo y respuesta a incidentes.

Esta herramienta permite identificar los lineamientos relacionados con ciberseguridad.

Herramienta para identificar lineamientos de Ciberseguridad					
Fecha de aplicación:					
Nombre del proyecto:					
Lineamientos	**¿Cumple?**		**Acción por realizar**	**Unidad/ persona responsable**	**Fecha para implementación de las acciones**
	Sí	**No**			
Controles a nivel de aplicación					
¿Se cuenta con un inventario de aplicaciones oficial y actualizado?					
Controles para protección de servidores y estaciones de trabajo					
¿Se cuenta con procedimientos para el inventario y descubrimiento de activos tecnológicos necesarios para la operación de la organización?					
¿Se cuenta con un proceso de gestión de vulnerabilidades y actualización de forma periódica?					
Listas de software aprobado para el uso dentro de la organización					
¿Se cuenta con listas de aplicaciones permitidas para la instalación y uso, que promuevan la seguridad de la información?					
Gestión continua de riesgos de ciberseguridad					

¿Se cuentan con procedimientos para la verificación periódica de vulnerabilidad en plataformas web?					
Desarrollo de planes de continuidad para las infraestructuras					
¿Se cuenta con planeación de la continuidad del negocio para determinar los dispositivos y servicios críticos que deben ser controlados y recuperados?					
¿Se cuenta con respaldos dentro y fuera del sitio para asegurar redundancia y protección contra pérdida de datos?					
¿Se realizan pruebas y validan la integridad y buen funcionamiento de los respaldos?					
¿Se cuenta con planes de recuperación ante desastre (DRP) en los servicios tecnológicos?					
Uso controlado de privilegios administrativos					
¿Se cuenta con desarrolladores de políticas de creación de contraseñas, uso adecuado de los recursos tecnológicos, creación de cuentas de usuarios y demás obras técnicas para el control de acceso a los recursos?					
¿La asignación de permisos, roles y accesos, se otorga bajo el mínimo privilegio necesario?					
Mantenimiento, monitoreo y análisis de registros de auditoría					

¿Se cuenta con la activación, monitoreo y análisis de las opciones de auditoría de sistemas, tales como bitácoras?					
Protecciones de correo electrónico y navegadores web					
¿Se cuenta con herramientas de filtrado de contenidos, de nombres por dirección ip, dns, palabras claves, y demás, que permitan regular el acceso a sitios para apegarse a las políticas de uso adecuado y racional de los recursos?					
Protección contra software malicioso					
¿Se cuentan con sistemas de software o hardware especializado en protección contra amenazas?					
Control y limitación de puertos de red, protocolos y servicios					
¿Se cuenta con una protección perimetral en todos los dispositivos y la red de datos institucional?					
Recuperación de datos					
¿Se cuenta con mecanismos de respaldo de información que aseguren la recuperación de información en caso de daños o desastres sobre la infraestructura?					
Configuración segura de dispositivo de red					
¿Se mantienen documentadas las reglas de enrutamiento y configuraciones de los principales equipos servidores y dispositivos de red?					
Defensa perimetral					

¿Se cuenta con sistemas para la detección y prevención de intrusos, para garantizar el monitoreo constante del tráfico y detectar condiciones irregulares en la red institucional?					
Protección de datos					
¿Se categoriza la información por niveles, está basada en el grado de sensibilidad ante el mal uso y su divulgación?					
¿Se encuentra la información en cumplimiento con las regulaciones de protección de datos vigentes y aplicables?					
Controles de acceso para redes inalámbricas					
¿Se cuenta con un inventario de dispositivos autorizados para ser utilizados y se ejecutan tareas periódicas para detectar dispositivos de redes no autorizadas?					
¿Se utilizan protocolos de cifrado vigentes y recomendados para la configuración de redes inalámbricas?					
¿Se utilizan mecanismos de identificación de usuarios, restricción de acceso a servicios definidos, y detección de mal uso y/o abuso de la plataforma, con redes inalámbricas de acceso público?					
¿Se encuentran aisladas las redes inalámbricas de acceso público de las redes internas de la organización?					

¿Se cuentan con mecanismos de control para el acceso a los recursos estrictamente requeridos para el funcionamiento operacional?					
¿Se utilizan tecnologías de comunicación Bluetooth solo cuando es estrictamente requerido para el funcionamiento mínimo, siempre que el dispositivo no contenga información o acceso directo a información sensible?					
Monitoreo y control de credenciales					
¿Se utilizan múltiples factores de autenticación para sistemas con acceso a información clasificada como sensible o de acceso privilegiado?					
¿Se utilizan mecanismos de cifrado por medio de valores no reversibles llamados Hash para el almacenamiento de contraseñas, generados a partir de los protocolos y algoritmos considerados como seguros?					
¿Se implementan mecanismos para la inhabilitación de cuentas de usuario no utilizadas dentro de un periodo de tiempo determinado, tales como mecanismos de bloqueo y/o expiración de sesiones inactivas?					
¿Se cuentan con y mecanismos de alerta para notificaciones de intento de ingreso no autorizados?					
Programas de entretenimiento y cultura de seguridad					

¿Se implementan mecanismos de evaluación para el control del conocimiento de los funcionarios en materia de buenas prácticas de seguridad de la información?					
¿Se implementan al menos una vez al año programas de capacitación en materia de seguridad de la información?					
¿Se brindan capacitaciones de cultura de seguridad de la información a nuevos funcionarios?					
Respuesta y gestión de incidentes					
¿Se implementan procesos documentados para la gestión y respuesta de incidentes en seguridad de la información?					
¿Se establecen los responsables para la gestión de incidentes, sus roles y se posee la información de contacto del personal que se encarga de atender el incidente?					
¿Se implementan mecanismos de asignación de puntajes y priorización de incidentes basados en criterios de impacto definidos con base en las necesidades específicas de la organización?					

Herramienta de Seguridad Tecnológica, 2. Elaboración propia.

ESTÁNDARES

Dentro de las mejores prácticas de TIC existen estándares y marcos de referencia que soportan no solo a nivel técnico, sino también administrativamente los aspectos inherentes al ST, de forma tal que se cuente con los mecanismos para la gestión segura de los componentes TIC y de la información. El apego a los estándares promovidos en el sector público costarricense forma parte de los requisitos necesarios para el desarrollo de productos y servicios digitales en el país.

Acrónimo de Information Technology Infrastructure Library, es un conjunto de prácticas detalladas para la gestión de servicios de TI (ITSM) que se centra en alinear los servicios de TI con las necesidades de las empresas.

COBIT. Desarrollado por la Asociación de Auditoría y Control de Sistemas de Información (ISACA) y el Instituto de Gobernanza de TI (ITGI), consta de varios componentes, incluidos:

1. Marco de referencia: Organiza los objetivos de gobierno de TI y las mejores prácticas.
2. Descripciones de procesos: Proporciona un modelo de referencia y un lenguaje común.
3. Objetivos de control: Documenta los requisitos de gestión de alto nivel para el control de los procesos de TI individuales.
4. Directrices de gestión: Herramientas para asignar responsabilidades, medir el rendimiento e ilustrar relaciones entre procesos.
5. Modelos de madurez: Evaluar la madurez / capacidad organizacional y abordar las brechas.

Es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

El estándar ISO 27001 para los Sistemas Gestión de la Seguridad de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

La Gestión de la Seguridad de la Información se complementa con las buenas prácticas o controles establecidos en la norma ISO 27002.

ISO / IEC 27002 (Organización Internacional de Normalización / Comisión Electrotécnica Internacional). Formalmente titulado "Tecnología de la información - Técnicas de seguridad - Código de práctica para la gestión de la seguridad de la información" documenta las mejores prácticas de seguridad en 14 dominios, de la siguiente manera:

- Políticas de seguridad de la información.
- Organización de la seguridad de la información.
- Seguridad de los recursos humanos.
- Gestión de activos.
- Control de acceso y gestión de acceso de usuarios.
- Criptografía.
- Seguridad física de los sitios y equipos de la organización.
- Seguridad operacional.
- Comunicaciones seguras y transferencia de datos.
- Adquisición de sistemas, desarrollo y soporte de sistemas de información.
- Seguridad para proveedores y terceros.
- Gestión de incidentes de seguridad de la información.
- Aspectos de seguridad de la información en la gestión de la continuidad del negocio.
- Conformidad.

Más específicamente el ISO / IEC 27032: 2017 titulado “Tecnología de la información - Técnicas de seguridad - Guías para ciberseguridad” proporciona una guía para mejorar el estado de la seguridad cibernética, explicando los aspectos únicos de esa actividad y sus dependencias en otros dominios de seguridad, en particular:

- Generalidades del ciberespacio y ciberseguridad.
- Modelo
- Partes interesadas en el ciberespacio.
- Amenazas contra la seguridad en el ciberespacio.
- Activos en el ciberespacio.
- Amenazas contra la seguridad en el ciberespacio.
- Robles de las partes interesadas en la ciberseguridad.
- Directrices para las partes interesadas.
- Controles de ciberseguridad.
- Marco de referencia de intercambio de información y coordinación.

La norma ISO 22301 establece todos los requisitos de planificar, establecer, implantar, operar, monitorear, revisar, mantener y realizar la mejora continua del sistema en cuanto a la respuesta y recuperación de los incidentes, cuando suceden.

Algunos beneficios de la gestión de continuidad del negocio son:

- Identificar y gestionar las amenazas actuales y futuras de la empresa.
- Método proactivo para minimizar el impacto de los incidentes.
- Operar funciones críticas durante los momentos del incidente.
- Mejorar el tiempo de reacción.

La norma ISO 22301 establece la metodología general para la continuidad de negocio. Dentro de la información documentada que se debe desarrollar:

- El alcance.
- La lista de requisitos legales, normativos y de otra índole.
- Política de la continuidad de negocio.
- Objetivos de la continuidad del negocio.
- Competencias del personal.
- Comunicación con las partes interesadas.
- Análisis del impacto en el negocio.
- Evaluar el riesgo.
- Estructura de la respuesta ante incidentes.
- Planes de continuidad del negocio.
- Procedimientos de recuperación.
- Resultados de acciones preventivas.
- Auditoría interna.
- Revisión de la dirección.
- Acciones correctivas.
- Mejora continua.

Tiene por objetivo que organizaciones de todos los tipos y tamaños puedan gestionar los riesgos en la empresa de forma efectiva, por lo que recomienda que las organizaciones desarrollen, implanten y mejoren continuamente un marco de trabajo cuyo objetivo es integrar el proceso de gestión de riesgos en cada una de sus actividades.

Como complemento a esta norma se ha desarrollado otro estándar: la ISO 31010 “Gestión del riesgo. Técnicas de evaluación de riesgos”. Esta norma provee de una serie de técnicas para la identificación y evaluación de riesgos, tanto positivos como negativos.

OWASP es una organización sin fines de lucro líder en materia de desarrollo seguro de software, sus diversos proyectos han sido adoptados como estándares de la industria y se han convertido en lineamientos base para garantizar la seguridad del software. Específicamente para el desarrollo de software se debe garantizar que los procesos de desarrollo de software implementado deben incluir prácticas de seguridad utilizando como línea base el **OWASP ASVS** (Application Security Verification Standard) y que garantizan que los productos entregados son libres de los diez riesgos identificados por el proyecto **OWASP Top 10** que sea vigente para el momento dado.

NIST (Instituto Nacional de Estándares y Tecnología) Publicación especial 800-53: Controles de seguridad y privacidad para sistemas y organizaciones de información federales. Conocido como NIST SP800-53, este es un marco de controles muy popular e integral requerido por todas las agencias gubernamentales de los EE. UU. También es ampliamente utilizado en la industria privada. Otras publicaciones especiales de la NIST importantes como material de referencia:

- NIST 800-61: Guía sobre la gestión de incidentes de seguridad.
- NIST 800-63: Lineamientos para la gestión de identidades digitales y la autenticación.
- NIST 800-92: Guía de gestión de registro y auditorías de seguridad informática.
- NIST 800-167: Guía de gestión de control de aplicaciones.

El Centro para la seguridad de internet (CIS por sus siglas en inglés) es un organización independiente sin fines de lucro con la misión es hacer del mundo conectado un lugar más seguro, desarrollando, validando y promoviendo soluciones oportunas de mejores prácticas que ayuden a las personas, las empresas y los gobiernos a protegerse contra las amenazas cibernéticas generalizadas, por lo que han desarrollado los Controles de Seguridad Critica que dan los recursos y las herramientas para implementarlos, al igual que tienen una comunidad de apoyo y trabajo.

CAPÍTULO 4:

INFRAESTRUCTURA Y TECNOLOGÍA EN LA NUBE

EQUIPO DE TRABAJO

Integrante	Institución
Job Céspedes	UCR
Ricardo Villalón	UCR
Roberto Lemaitre	MICITT
Edgar Mora	MICITT

INTRODUCCIÓN AL TEMA

El presente capítulo contiene los insumos para construir políticas que puedan ser utilizadas por las entidades del sector público en los temas de Infraestructura, Datos y Nube.

PRINCIPIOS

Interoperabilidad

Se deben tomar en cuenta las mejores prácticas de interoperabilidad y los estándares internacionales para garantizar que los diferentes desarrollos de infraestructura puedan interactuar, conectarse y funcionar con otros sistemas del Estado sin ningún problema.

Escalabilidad

Cualquier desarrollo de infraestructura debe tener los mecanismos para garantizar la escalabilidad a largo plazo sin depender de ningún proveedor o tecnología en particular.

Continuidad de los servicios

Se debe asegurar que el sistema opere 24/7/365 con una disponibilidad de los servicios de 99,99%.

Aprovechamiento de las infraestructuras tecnológicas existentes

En todo desarrollo de infraestructura se debe buscar, de antemano, el aprovechamiento de los servicios tecnológicos existentes en el Estado, todo con el propósito de hacer un uso eficiente de los recursos económicos de acuerdo con la realidad nacional, según se establece en la Directriz N°031-MICITT-H Mejoras en la eficiencia del gasto público mediante el uso adecuado de tecnologías digitales en el sector público costarricense y la Directriz N°053-H-MICITT Regulación y normalización de adquisiciones de tecnología y/o desarrollo de sistemas informáticos de apoyo a la gestión.

Cumplimiento normativo

Todo desarrollo de infraestructuras tecnológicas debe cumplir con el marco legal vigente y aplicable para el uso y desarrollo de los servicios tecnológicos.

POLÍTICAS GENERALES

Infraestructura

- Estar diseñada y gestionada siempre en función del propósito de la misma, para ser eficiente en la generación de productos, servicios y el uso de los recursos.
- Contemplar en su diseño y gestión la cantidad apropiada de personal para soportar la generación de productos y servicios.
- Diseñar y categorizar en su criticidad y privacidad las estructuras de información que administra.
- Implementar un esquema de seguridad de las estructuras de datos, para asegurar su confidencialidad, integridad y disponibilidad para la misma organización o para los usuarios internos y externos cuando corresponda.
- Controlar adecuadamente el uso de sus propios recursos y gestionar la administración de los recursos y servicios provistos por terceros.
- Realizar la planeación correspondiente para implementar una adecuada gestión de la continuidad de las operaciones de la organización y permitir enfrentar incidentes con el menor impacto posible.
- Tomar en cuenta las necesidades de procesamiento y almacenamiento de información para los proyectos de adquisición de infraestructura tecnológica, de acuerdo con sus capacidades y objetivos.
- Alinearse con todas las normativas emitidas por el Gobierno en relación con el uso, administración y adquisición de equipos para la infraestructura tecnológica.

- Promover la mejora de las capacidades técnicas del personal para el máximo provecho de las tecnologías adquiridas e implementadas en la organización.
- Asegurar la plataforma tecnológica frente a las amenazas de ciberseguridad adquiriendo equipo para la protección perimetral, detección y prevención de intrusos, control de acceso externo o interno a la organización y protección de aplicaciones en línea, entre otros aspectos.
- Diseñar las políticas de uso y procedimientos para la implementación de la tecnología de virtualización de servidores de datos en la organización, para asegurar el acceso y disponibilidad de los servicios virtualizados.
- Realizar una valoración de las condiciones ofrecidas por los servicios de manejo de datos en la Nube disponibles en el mercado, para velar por la seguridad, confidencialidad, disponibilidad y otras características relacionadas con el traslado o descarte de la información por parte de los encargados de la información de la organización.
- Contemplar, en caso de adquisición de tecnología de computación en la Nube, el modelo de servicio que requiera para la organización, tomando en cuenta la plataforma existente en su organización y su capacidad.
- Asegurar la interoperabilidad entre los servicios de computación locales y los servicios adquiridos de computación en la Nube.
- Alinearse con la normativa nacional concerniente al diseño y construcción de instalaciones que cumplen con requisitos eléctricos, mecánicos y de seguridad física.
- Establecer los mecanismos para implementar la seguridad física y el control del acceso en las infraestructuras tecnológicas existentes o planeadas.
- Establecer los mecanismos para la detección y prevención de incendios dentro de las infraestructuras tecnológicas, en apego con la normativa existente para tal efecto.

Según las políticas generales, relacionadas con infraestructura, se elabora la siguiente herramienta para identificar los elementos que debe de contener la infraestructura tecnológica:

Herramienta para identificar los elementos de la infraestructura tecnológica			
Fecha de aplicación:			
Requisito	**¿Cumple?**		**Acción por realizar**
	Si	**No**	
¿La infraestructura está diseñada y gestionada siempre en función del propósito de esta, para ser eficiente en la generación de productos, servicios y el uso de los recursos?			

¿La infraestructura contempla en su diseño y gestión la cantidad apropiada de personal para soportar la generación de productos y servicios?			
¿Se diseña y categoriza en su criticidad y privacidad las estructuras de información que administra?			
¿La infraestructura implementa un esquema de seguridad de las estructuras de datos, para asegurar su confidencialidad y disponibilidad para la organización o para los usuarios internos y externos?			
¿La infraestructura controla adecuadamente el uso de sus propios recursos y gestionar la administración de los recursos y servicios provistos por terceros?			
¿Se realiza la planeación correspondiente para implementar una adecuada gestión de la continuidad de las operaciones de la organización y permitir enfrentar incidentes con el menor impacto posible?			
¿Se toma en cuenta las necesidades de procesamiento y almacenamiento de información para los proyectos de adquisición de infraestructura tecnológica, de acuerdo con sus capacidades y objetivos?			
¿Se alinea con todas las normativas emitidas por el Gobierno en relación con el uso, administración y adquisición de equipos para la infraestructura tecnológica?			
¿Se promueve la mejora de las capacidades técnicas del personal para el máximo provecho de las tecnologías adquiridas e implementadas en la organización?			
¿Se asegura la plataforma tecnológica frente a las amenazas de ciberseguridad adquiriendo equipo para la protección perimetral, detección y prevención de intrusos, control de acceso externo o interno a la organización y protección de aplicaciones en línea, entre otros aspectos?			

¿Se diseñan las políticas de uso y procedimientos para la implementación de la tecnología de virtualización de servidores de datos en la organización, para asegurar el acceso y disponibilidad de los servicios virtualizados?			

Herramienta de Infraestructura en la Nube, 1. Elaboración propia.

Tecnología de Nube

Cumplimiento legal

Cumplir con el marco legal vigente y aplicable para el uso de los servicios de la Nube, para lo cual se tomará en consideración tanto la legislación costarricense como la normativa local, nacional e internacional.

Marco de referencia común

Utilizar un marco de referencia común estandarizado que permita consultar términos, conceptos y terminología definidos y conocidos a nivel de la industria.

Cumplimiento del servicio

Asegurar el cumplimiento de los servicios contratados por medio de los instrumentos y controles pertinentes.

Interoperabilidad y portabilidad

Posibilitar la interoperabilidad y portabilidad entre servicios nativos de la Nube o no, y entre diferentes proveedores de Nube.

Uso de datos

Comprender cómo los datos son utilizados en la Nube.

Políticas de uso

Asegurar los intereses de la institución por medio del establecimiento de políticas concernientes a la implementación y uso de sistemas y servicios en la Nube.

Seguridad y privacidad

Proteger la seguridad y privacidad de los datos de la organización y sus usuarios.

POLÍTICAS ESPECÍFICAS

Infraestructura

- Seguir y cumplir con las normativas o directrices sobre tecnologías indicadas en el presente CNTD.
- Tener claramente identificados, ubicados e inventariados sus activos.
- Contar con un plan de continuidad de servicios en el cual se identifiquen los activos y servicios críticos, y se definan los procedimientos a seguir. Dichos planes de continuidad se encuentran definidos en la Administración Pública para su aplicación.
- Cumplir con los códigos de construcción y eléctricos nacionales, además de las normativas internacionales para dichas instalaciones según corresponda.
- Contar con la documentación sobre las políticas de uso adecuado de los recursos, de acceso físico y respaldo de la información, entre otros.
- Contar con procedimientos para la recuperación ante desastres, con miras a buscar la más alta disponibilidad posible de los servicios y los datos.
- Contar con el registro completo de las licencias de software de aplicaciones de usuario y sistemas operativos de los sistemas utilizados para sus funciones y servicios.

Tecnología de Nube

Las políticas específicas sobre la tecnología de Nube, agrupadas según al objetivo general al que pertenecen, son las siguientes:

Cumplimiento legal

Privilegiar, cuando sea posible y conveniente, la adquisición de soluciones de cómputo en la Nube sobre otro tipo de infraestructura.

Establecer acuerdos de niveles de servicios.

Incluir penalidades por incumplimiento en cada uno de los acuerdos de nivel de servicio.

Realizar una evaluación de los servicios en la Nube que incluya aspectos técnicos, legales y financieros.

Realizar la evaluación financiera sobre el valor presente de todos los costos asociados a las alternativas, proyectado a un plazo de tres años.

No incluir en la evaluación detalles que puedan comprometer la seguridad de la información y de la infraestructura tecnológica de las instituciones relacionadas.

No arriesgar o comprometer información confidencial de los particulares a la que tuviera acceso la institución.

Garantizar, de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizados, daño o pérdida u otros factores disfuncionales.

Documentar e implementar una política de seguridad de la información junto con los procedimientos correspondientes.

Asignar los recursos necesarios para lograr los niveles de seguridad requeridos.

Considerar aquello que establece la normativa vigente con relación en los siguientes aspectos:

- La implementación de un marco de seguridad de la información.
- El compromiso del personal con la seguridad de la información.
- La seguridad física y ambiental.
- La seguridad en las operaciones y comunicaciones.
- El control de acceso.
- La seguridad en la implementación y mantenimiento de software e infraestructura tecnológica.
- La continuidad de los servicios de TI.

Generar los productos y servicios de TI de conformidad con los requerimientos de sus usuarios con base en un enfoque de eficiencia y mejoramiento continuo.

Responder adecuadamente a las amenazas que puedan afectar la gestión de las TI, mediante una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional, y que considere el marco normativo que le resulta aplicable.

Contar con una definición clara, completa y oportuna de los requerimientos, como parte de los cuales debe incorporar aspectos de control, seguridad y auditoría bajo un contexto de costo – beneficio.

Asegurar la obtención satisfactoria del objeto contratando a terceros en procesos de implementación o mantenimiento de software e infraestructura:

- Establecer una política relativa a la contratación de productos de software e

infraestructura.

- Justificar debidamente la contratación de terceros para la implementación y mantenimiento de software e infraestructura tecnológica.
- Establecer un procedimiento o guía para la definición de los “términos de referencia” que incluyan las especificaciones y requisitos o condiciones requeridos o aplicables, así como para la evaluación de ofertas.

Tener claridad respecto de los servicios que se requiere y sus atributos, y los prestados por la Función de TI según sus capacidades.

Establecer cuáles son los servicios requeridos, los ofrecidos y sus atributos. Documentar y considerar el resultado como un criterio de evaluación del desempeño:

- Tener una comprensión común sobre exactitud, oportunidad, confidencialidad, autenticidad, integridad y disponibilidad.
- Contar con una determinación clara y completa de los servicios y sus atributos, y analizar su costo y beneficio.
- Definir con claridad las responsabilidades de las partes y su sujeción a las condiciones establecidas.
- Establecer los procedimientos para la formalización de los acuerdos y la incorporación de cambios en ellos.
- Defender los criterios de evaluación sobre el cumplimiento de los acuerdos.
- Revisar periódicamente los acuerdos de servicio, incluidos los contratos con terceros.

Cumplir íntegramente con la Ley:

- Establecer las pautas por seguir para la contratación de proveedores de servicios.
- Evitar contingencias legales por la contratación de servicios personales, a personas físicas y/o jurídicas, para dar pleno cumplimiento con la legislación laboral en materia de obligaciones sociales.
- No contratar servicios que forman parte de las actividades habituales de la empresa.
- Establecer un contrato de servicios para amparar el servicio brindado a través de proveedores externos.
- Establecer la naturaleza jurídica del contrato como de carácter civil o comercial.
- Incluir en el contrato la descripción del bien o servicio por contratar, las obligaciones de ambas partes, y la forma de retribución económica.
- Asegurarse de que la contratación se rija con base en los principios de eficiencia, eficacia, publicidad, libre competencia, igualdad, buena fe e intangibilidad patrimonial.
- Establecer un acuerdo a nivel de servicios.

- Establecer la relación entre el proveedor y el cliente.

Asegurarse de que los servicios contratados a terceros satisfagan los requerimientos en forma eficiente:

- Establecer los roles y responsabilidades de terceros que brindan servicios de TI a la institución.
- Establecer y documentar los procedimientos asociados con los servicios e instalaciones contratados a terceros.
- Vigilar que los servicios contratados sean congruentes con las políticas relativas a calidad, seguridad y seguimiento establecidas por la organización.
- Minimizar la dependencia de la organización respecto de los servicios contratados a terceros.
- Asignar a un responsable con las competencias necesarias para evaluar periódicamente la calidad y cumplimiento oportuno de los servicios contratados.

Marco de referencia común

Emplear términos y definiciones estandarizadas para la computación en la Nube. Se pueden consultar las definiciones estándar sobre las características clave, roles, actividades, tipos de capacidades, categoría de los servicios, modelos de despliegue y aspectos transversales de este paradigma.

Apoyarse en un marco de referencia común al diseñar y desarrollar una arquitectura específica del sistema. Es efectivo para describir los roles, las actividades, los aspectos transversales, la arquitectura y los componentes funcionales de la computación en la Nube. Su uso también es útil para categorizar y comparar servicios de Nube.

Cumplimiento del servicio

Utilizar un conjunto común de elementos (conceptos, términos, definiciones, contextos) para crear acuerdos de niveles de servicio e identificar la relación entre sus componentes.

Tener en cuenta las características clave de la computación en la Nube en los acuerdos de niveles de servicio.

Asegurarse de que los acuerdos de niveles de servicio y otros documentos rectores estén alineados con los casos de negocios y estrategia global de la institución.

Para el diseño

Establezca acuerdos de niveles de servicio que satisfagan sus necesidades, alineados con

las capacidades de los servicios cubiertos.

Tome en cuenta los roles apropiados en el proceso de diseño de los acuerdos de niveles de servicio.

Incluya dentro del acuerdo de nivel de servicio u otro documento de gobernanza, el proceso para cambiar el acuerdo y para notificar a las partes sobre los cambios.

Considere los mecanismos que se pueden usar para monitorear cada característica del servicio e informar fallas, con el fin de cumplir con los compromisos acordados.

Para la evaluación y aceptación

Asegúrese que esté listo para implementar y ejecutar cada acuerdo de nivel de servicio, independientemente de los medios de aceptación.

Asegúrese estar preparado para respaldar la implementación y la ejecución de términos únicos, cuando el acuerdo los incluya.

Para la implementación y ejecución

Incluya el acuerdo de nivel de servicio como parte de la gobernanza interna.

Monitoree el servicio de nube para asegurarse que los acuerdos de nivel de servicio y sus componentes se cumplan.

Solicite una notificación cuando se complete el proceso de finalización del acuerdo de nivel de servicio.

Entienda y prepárese para cualquier cambio anunciado al servicio y sus respectivas condiciones.

Determine si necesita incluir condiciones adicionales respecto a la fiabilidad y disponibilidad del servicio, respaldo de datos y recuperación de desastres, más allá de las ofrecidas por defecto.

Implemente sus propios procesos de limpieza y eliminación de datos.

Utilice un modelo métrico estandarizado que defina las condiciones y reglas para realizar una medición y comprender el resultado, con el objetivo de que cada métrica sea clara, comparable e implementable.

Interoperabilidad y portabilidad

Asegurarse de tener un entendimiento en común sobre los tipos de interoperabilidad y de portabilidad, sus relaciones e interacciones, así como los conceptos y terminología asociados

a ellos.

Uso de datos

Entender y proteger la privacidad y confidencialidad de los datos de la institución y los datos de los usuarios a través de una mayor transparencia de las políticas y prácticas, utilizando un esquema estandarizado para la estructura de las declaraciones de uso de datos.

Políticas de uso

Regular los sistemas y servicios en la Nube formulando políticas y prácticas pertinentes que tomen en cuenta los intereses de la institución u organización.

Utilizar códigos de prácticas definidos por la industria para guiar la operación y el uso de la Nube.

Seguir buenas prácticas al manejar contraseñas u otras credenciales, al otorgar los permisos apropiados a usuarios específicos, en el tipo de datos que ingresan en el servicio en la Nube, y al etiquetar el contenido.

Proteger los datos confidenciales de la institución u organización.

Controlar la autorización y la autenticación de los servicios que la institución brinda en la Nube para garantizar que los usuarios no abusen de dichos servicios.

Seguridad y privacidad

Proteger la privacidad y la seguridad de la información de los usuarios utilizando los controles adecuados.

No utilizar los datos con fines comerciales u otro tipo de uso diferente de la naturaleza del contrato.

Definir y seguir las pautas que respaldan la implementación de la gestión de seguridad de la información para el uso de servicios en la Nube, identificando y controlando los riesgos asociados.

Con base en las políticas específicas, relacionadas con tecnología de nube, se elabora la siguiente herramienta.

Herramienta de validación de Tecnología de Nube		
Fecha de aplicación:		
	¿Cumple?	

Requisito	Si	No	Acción por realizar
Cumplimiento Legal			
¿Se cumple con el marco legal vigente y aplicable para el uso de los servicios de la Nube, tomando en cuenta la legislación costarricense, normativa local, nacional e internacional?			
Marco de referencia común			
¿Se utiliza un marco de referencia común estandarizado que permite consultar término, conceptos y terminología definidos y conocidos a nivel de la industria?			
Cumplimiento del servicio			
¿Se asegura el cumplimiento de los servicios contratados por medio de los instrumentos y controles pertinentes?			
Interoperabilidad y portabilidad			
¿Se posibilita la interoperabilidad y portabilidad entre servicios nativos de la Nube o no, y entre diferentes proveedores de Nube?			
Uso de datos			
¿Se comprende como los datos son utilizados en la Nube?			
Políticas de uso			
¿Se aseguran los intereses de la institución por medio de políticas concernientes a la implementación y uso de sistemas y servicios en la Nube?			
Seguridad y privacidad			
¿Se protege la seguridad y privacidad de los datos de la organización y de sus usuarios?			

Herramienta de Infraestructura en la Nube, 2. Elaboración propia.

ESTÁNDARES

Algunos estándares que se pueden considerar como referencia son los siguientes:

ISO/IEC 17788:2014
Information technology -- Cloud computing -- Overview and vocabulary

ISO/IEC 17789:2014 Information technology -- Cloud computing -- Reference architecture
ISO/IEC 19086-1:2016 Information technology -- Cloud computing -- Service level agreement (SLA) framework -- Part 1: Overview and concepts
ISO/IEC 19086-2:2018 Cloud computing -- Service level agreement (SLA) framework -- Part 2: Metric model
ISO/IEC 19941:2017 Information technology -- Cloud computing -- Interoperability and portability
ISO/IEC 27036-4:2016 Information technology -- Security techniques -- Information security for supplier relationships -- Part 4: Guidelines for security of cloud services
ISO/IEC TR 22678:2019 Information technology -- Cloud computing -- Guidance for policy development

CAPÍTULO 5:

INTEROPERABILIDAD

EQUIPO DE TRABAJO

Integrante	Institución
Marco Jiménez	UCR
Edgar Mora	MICITT
Erick Mora	MICITT
Jorge Mora	MICITT
Aldo González	MICITT

INTRODUCCIÓN AL TEMA

En el marco de la ETD, el MICITT ha planteado el desarrollo de un marco nacional de referencia de interoperabilidad de sistemas de información orientado a la presentación de servicios digitales.

Este marco pretende ser un punto de inicio para el desarrollo de nuevos proyectos de sistemas de información por desarrollarse, en instituciones de gobierno que participen en el desarrollo de un gobierno digitalmente inteligente.

La interoperabilidad no es un fin en sí mismo, es un medio a través del cual alcanzar un objetivo orientado a la prestación de un conjunto de servicios, apoyado por un conjunto de procesos internos de las organizaciones para facilitar los servicios a ciudadanos, instituciones y negocios.

Los planes de acción que toman en cuenta las dimensiones de la interoperabilidad se plasman en la Estrategia de Transformación Digital 2023-2027, la cual promueve la buena gobernanza mediante la mejora de la institucionalidad y la coordinación interinstitucional, los servicios transversales, la participación ciudadana y la transparencia de la gestión pública impulsando la rendición de cuentas. (ETD,2023, pag.74)

La interoperabilidad involucra una gran cantidad de componentes y de actores que deben de trabajar de manera conjunta, coordinada y eficiente para proveer servicios integrados a nivel nacional y en el caso de este Código en particular, para un conjunto de usuarios que pueden ser tanto, los propios habitantes como otras instituciones del país.

A partir del valor estratégico que tiene la interoperabilidad de servicios para la función pública y el país en general se ha contado para la siguiente guía de implementación de servicios con el valioso apoyo y experiencia que ILPES/CEPAL llevan en esta materia.

Para introducir este apartado, será conveniente conocer lo que la CEPAL tiene claro acerca de la interoperabilidad:

"*La interoperabilidad es un eje central dentro de las iniciativas de Gobierno Digital, contribuye en la eficiencia de los servicios que el Estado brinda a los Ciudadanos y contribuye en los aspectos Organizacionales, Normativo/Legales, Semánticos y Técnicos, entre las distintas instituciones públicas, privadas y la ciudadanía.*", CEPAL, 2020.

La Gobernanza estratégica para la interoperabilidad, corresponde a la capa más externa y se refiere a la instancia de planificar a largo plazo la integración de servicios al ciudadano desde una mirada Estado y no de trámites de cada institución. Incluye la colaboración, interacción o asociación entre diferentes sectores de la administración pública, entre el sector público y privado, el gobierno y la sociedad (CEPAL, 2021).

Teniendo en cuenta esta visión integradora del país y de los servicios del Estado, se ejecuta todo un trabajo liderado por el MICITT como ente rector con la colaboración y aporte de la CEPAL si no, de un grupo de instituciones del país para iniciar este necesario proyecto de interoperabilidad para el país.

Este grupo de instituciones forman una referencia que compone un volumen importante de actividades dirigidas a las personas y que a su vez cuentan con un gran potencial de integración de sus actividades y definió la propuesta de valor de la interoperabilidad para Costa Rica.

De esta manera, se plantean cinco elementos base: modelo de madurez y capacidad de implementación, datos abiertos, arquitectura orientada a servicios, sistemas de autenticación y autorización, y plataformas para el intercambio documental.

PROPUESTA DE VALOR

"***Proveer a la ciudadanía un acceso simple, ágil, seguro y transparente que responda a las necesidades de las personas físicas y jurídicas, mediante un modelo que incorpore componentes normativos, organizacionales, semánticos y técnicos, a través de una institucionalidad comprometida, competente y sostenible que vele por la confidencialidad y seguridad de la información. Que, a través de esto, se mejore la calidad de vida de las personas y propicie unclima de negocios favorable y competitivo al país***".

PRINCIPIOS

- Transparencia organizacional.
- Mejora en la competitividad.
- Integración intra-organizacional y extra-organizacional.
- Servicio al ciudadano.
- Servicio a empresas.
- Servicio a otras entidades del Gobierno.
- Servicio a entidades internacionales.
- Disponibilidad de información.
- Confiabilidad en las comunicaciones.
- Acceso seguro a la información.
- Transparencia en la información brindada.
- Mejoras en los procesos administrativos.
- Eficiencia para las organizaciones, empresas y ciudadanos.

POLÍTICAS GENERALES

Políticas generales de Interoperabilidad Organizativa

- Determinar su capacidad organizativa y técnica para desarrollar el proceso de interoperabilidad.
- Crear un equipo de trabajo interdisciplinario a cargo de la validación y coordinación de los servicios que se van a interoperar. Este equipo de trabajo se denominará El equipo Ad Hoc Interno de Interoperabilidad.
- Definir las organizaciones con las que busca realizar el intercambio de información que quiere interoperar y contar con los convenios respectivos.
- Definir claramente el producto y/o servicio derivado que será interoperado.
- Tener claramente documentados los procesos que se requieren para proveer el producto o servicio.
- Asignar un líder responsable del producto y/o servicio.
- Asignar un líder encargado de la gestión del convenio firmado con la organización u organizaciones con las que interoperan.
- Asignar un líder encargado de la gestión técnica del producto y/o servicio que se desea interoperar. El líder técnico se encarga de servir como enlace entre el proceso administrativo y el proceso técnico para que se lleve a cabo el proyecto.
- Valorar la factibilidad de la generación de ingresos económicos por parte del producto y/o servicio implementado, para apoyar el coste del proyecto.
- Determinar los costes estimados para brindar el producto y/o servicio.
- Determinar la factibilidad legal del producto y/o servicio que va a interoperar y sus datos.

Políticas generales de Interoperabilidad Normativa / Legal

- Garantizar el cumplimiento de la normativa de protección de datos de los habitantes vigente en el país.
- Garantizar que las organizaciones que trabajan sobre marcos jurídicos, políticas y estrategias diferentes, puedan trabajar juntas.
- Definir acuerdos claros sobre cómo abordar las diferencias jurídicas para poder trabajar en conjunto.
- Tomar en cuenta e identificar leyes y normativas que regulan, restringen o posibilitan el ofrecimiento de un servicio interoperado a las personas.
- Cooperar con las contrapartes que tienen a cargo las funciones normativas para poder desarrollar el trabajo de la interoperabilidad.
- Realizar revisiones integrales de la normativa vigente para garantizar que no existan

limitaciones en los servicios que se van a interoperar.

- Garantizar en todo momento el cumplimiento de la normativa vigente en nuestro país.

Políticas generales de Interoperabilidad Semántica

- Tener claramente definidas las fuentes de los datos por interoperar, ya sean correspondientes a sistemas internos o sistemas externos.
- Documentar claramente cada uno de los metadatos y agrupaciones de metadatos, dando así un significado claro y adecuado para que pueda ser interpretado de manera correcta.
- Desarrollar un diccionario de metadatos, con el fin de identificar los datos que van a ser utilizados en el proyecto, claramente descritos en su significado, incluyendo además alias, tipo, formato y cualquier otro detalle que facilite el intercambio consistente de información.
- Contribuir para la formación, la comprensión y el tratamiento de los datos y la información, para impulsar los servicios digitales y la implementación del Gobierno Digital.
- Garantizar que el formato y el significado de la información intercambiada sean exactos, se comprendan y conserven en todos los intercambios entre las partes.
- Emplear la norma de clasificación de metadatos para documentos indicada por el Archivo Nacional.
- Determinar la arquitectura tecnológica necesaria y los estándares a utilizar entre los servicios interoperables

Políticas generales de Interoperabilidad Técnica

- Desarrollar un marco general de interoperabilidad técnica en el que se definan las especificaciones técnicas, estándares de intercambio de datos, lineamientos para la interoperabilidad de los sistemas, que sirva como referencia durante cualquier otro proyecto que establezcan.
- Acordar el uso de protocolos o estándares de intercambio de datos de tipo abierto o no propietarios, para garantizar la interoperabilidad entre los sistemas interconectados u otros sistemas a futuro.
- Acordar los canales de interconexión con que cuentan de manera común para el intercambio de información y que permitan a su vez el cumplimiento de la interoperabilidad organizacional, semántica y técnica.
- Acordar los mecanismos de seguridad tanto en procedimientos como en herramientas técnicas para establecer la seguridad de la información de los canales de interconexión acordados con el fin de evitar comprometer la confidencialidad de los datos.
- Acordar en común, de ser necesario, aplicaciones intermedias que puedan requerirse en el proceso de interconexión, siendo estas últimas de tipo abierto o no propietarias.

- Diseñar, crear y gestionar un catálogo de servicios de interoperabilidad que la institución ofrece.
- Diseñar, crear, y gestionar un catálogo de esquemas y metadatos que la institución utiliza para los datos y la información de los servicios que interopera.
- Utilizar estándares abiertos y cumplir con los requisitos del capítulo de Accesibilidad Digital, Usabilidad y Experiencia de Usuario.
- Seguir lo establecido en el capítulo de Neutralidad Tecnológica.

POLÍTICAS ESPECÍFICAS

Seguir y cumplir con los mínimos sobre tecnologías indicadas en el presente CNTD.

Documentar todo producto y/o servicio tomando en cuenta los tipos de interoperabilidad dictados en la sección de políticas generales.

Catalogar el producto y/o servicio claramente, sea G2G, G2B o G2C.

Responder a una necesidad o requerimiento de intercambio de información, enfocándose en buscar la mejora de la ciudadanía en general.

Someter el producto y/o servicio al proceso de sello digital brindado por el MICITT.

Documentar el producto y/o servicio con el fin de definir la cadena de interoperabilidad, creando un documento de términos de referencia, el cual, como mínimo, debe contener:

- Nombre del producto o servicio.
- Descripción del producto o servicio.
- Beneficios que se obtendrán.
- Catalogarlo según el público meta (G2C, G2B, G2B).
- Líder de la interoperabilidad organizacional.

- Indicar con qué organizaciones se va a realizar la interoperabilidad.
- Líder de interoperabilidad semántica.
- Líder interoperabilidad técnica.
- Estimación del tiempo para invertir.
- Costo presupuestado.
- Costo aproximado del servicio (en caso de existir).
- Estimación de la reducción de tiempo y costos del proceso por ser interoperado.
- Tipo de sistema (data céntrico o docu céntrico).
- Listado de tecnologías por emplear (Hardware, Software).
- Listado de protocolos de comunicación por utilizar, lenguaje(s) de programación.
- Listado de tecnologías de seguridad de la información.
- Listado de tecnología de accesibilidad (en caso de ser necesarias).

Los productos o servicios de interoperabilidad deben exponer los métodos o funciones de llamados remotos para ser empleados en la interoperabilidad.

Los productos o servicios relacionados con sistemas de tipo docu céntrico deben contar con un repositorio de documentos digitales de acuerdo con la política de gestión de documentos del Archivo Nacional.

Los sistemas de tipo data céntrico son recomendables, pero no es necesaria la utilización de una arquitectura orientada a servicios.

ESTÁNDARES

Gestión de documentos electrónicos

Requisitos de recuperación y conservación

1. Definir una política de gestión de documentos.
2. Inclusión de un índice electrónico en los expedientes.
3. Dotar a los documentos de una identificación única e inequívoca dentro del sistema

de gestión, que permita clasificarlos, recuperarlos y referirse a los mismos con facilidad.

4. Asociar los metadatos mínimos obligatorios al documento electrónico y, en su caso, los complementarios o necesarios para asegurar su gestión y conservación a lo largo del ciclo de vida.

5. Clasificación, de acuerdo con un cuadro adaptado a las funciones, tanto generales como específicas, de cada una de las organizaciones.

   Conservación de los documentos durante el periodo establecido por las comisiones calificadoras que corresponden, de acuerdo con la legislación en vigor, a las normas administrativas y obligaciones jurídicas que resultan de aplicación en cada caso, especificando las medidas que aseguran dicha conservación.

6. Acceso completo e inmediato a los documentos, en función del esquema de tipos de acceso a los mismos, a través de métodos de consulta en línea que permitan la visualización de los documentos con todo el detalle de su contenido, la recuperación exhaustiva y pertinente de los documentos, la copia o descarga en línea en los formatos originales y la impresión en papel de aquellos documentos que sean necesarios. El sistema permitirá, al menos, la consulta durante todo el periodo de conservación de la firma electrónica, incluido, en su caso, el sello de tiempo y de los metadatos asociados al documento.

7. Adopción de medidas para asegurar la conservación del documento electrónico a lo largo de su ciclo de vida.

8. Coordinación horizontal entre los responsables de la gestión de documentos y los restantes servicios interesados en materia de archivo.

9. Transferencia, en su caso, de los expedientes entre los diferentes repositorios electrónicos para efectos de conservación de acuerdo con lo establecido en la legislación en materia de archivos, de manera que se pueda asegurar su conservación y recuperación a mediano y largo plazo.

10. Si el procedimiento de calificación documental así lo establece, se ha de borrar la información o, en su caso, proceder con la destrucción física de los soportes, dejando registro de su eliminación de acuerdo con la legislación que resulta de aplicación.

11. Formación tecnológica del personal involucrado en la ejecución y gestión documental.

12. Documentación de los procedimientos que garantizan la interoperabilidad a mediano

y largo plazo, así como las medidas de identificación, recuperación, control, tratamiento y conservación de los documentos electrónicos.

Propiedades del documento electrónico

1. **Autenticidad**: Propiedad que puede atribuirse al documento al probarse que es lo que afirma ser, que ha sido creado o enviado por la persona de la cual se afirma que lo ha creado o enviado y en el momento en que se afirma, sin que haya sufrido ningún tipo de modificación.
2. **Fiabilidad**: Propiedad o característica que indica que su contenido puede ser considerado una representación completa y precisa de las actuaciones, las actividades o los hechos de los que da testimonio y al que se puede recurrir en el curso de posteriores actuaciones o actividades.
3. **Integridad**: Propiedad o característica que indica su carácter de completo, sin alteración de ningún aspecto esencial.
4. **Disponibilidad**: Propiedad o característica que permite que el documento pueda ser localizado, recuperado, presentado o interpretado. El mismo debe señalar la actividad o actuación donde se generó, proporcionar la información necesaria para la comprensión de las actuaciones que motivaron su creación y utilización, identificar el contexto marco de las actividades y las funciones de la organización y mantener los vínculos existentes con otros documentos como reflejo de una secuencia de actuaciones.

Ciclo de vida del documento electrónico

El ciclo de vida del documento electrónico consta de tres fases:

1. **Fase de captura**. Posterior a la propia creación o producción del documento, bien por parte de un ciudadano o internamente en una organización, la captura supone su incorporación al sistema de gestión de documentos de una organización.
2. **Fase de mantenimiento y uso**. Una vez finalizada la tramitación administrativa, los documentos mantienen su validez administrativa y están disponibles.
3. **Fase de conservación y selección**. Los documentos de valor efímero se eliminan reglamentariamente, en tanto aquellos que tienen valor a largo plazo se conservan permanentemente en atención a su utilidad administrativa, jurídica, archivística, histórica o de investigación y social, según establezcan las autoridades competentes.

Los principales procesos y acciones por tener en cuenta

1. La **creación del documento**. Se puede dar por iniciativa del ciudadano bien de la organización, por vía de entrada del registro (papel o electrónico) u otras posibles vías de entrada según actividades propias de cada organización, como pueden ser, por ejemplo, los procesos de incautación de documentos derivados de inspecciones o revisiones. Los documentos pueden presentarse en soporte papel o en soporte electrónico. Además, los documentos electrónicos presentados por los ciudadanos pueden ir acompañados de una firma electrónica que, estando sujeta a las condiciones establecidas en la Ley Nº8454 de certificados, firmas digitales y documentos electrónicos y en su normativa aplicable, será conservada, al igual que el resto de los componentes del documento, por la organización ante la cual haya sido presentada.

2. La **captura del documento** en el sistema de gestión de documentos de la organización. Incluirá los procesos de registro e incorporación de los documentos en el sistema de gestión de documentos de la organización, y, como acción de especial relevancia, incluirá la asignación de los metadatos y, si procede, la firma del documento por parte de la organización (por ejemplo, un sello electrónico por parte de una organización en un Registro de Entrada). En caso necesario, esta captura del documento puede venir precedida por una digitalización o por un proceso de conversión de formato del documento.

3. La **gestión del documento** en el contexto de la tramitación administrativa. Durante este proceso pueden generarse copias auténticas de los documentos para su puesta a disposición del ciudadano, producirse cambios de estado, así como conversiones de formato, y es el momento en el que tiene lugar la generación de expedientes electrónicos.

4. La **gestión del documento en un sistema de repositorio electrónico.** Una vez finalizada la tramitación administrativa, se llevará a cabo este paso con la intención de conservar de forma segura los documentos electrónicos y su integración en el sistema para la gestión del archivo de la organización, con el fin de garantizar el derecho de acceso de los ciudadanos a la información y documentos públicos.

5. La **salida y acceso** de los documentos archivados. Se puede dar por parte de otras organizaciones o por parte de ciudadanos en el ejercicio de sus derechos.

Sistema de gestión de documentos electrónicos

Un sistema de gestión de documentos electrónicos podría definirse como la aplicación del

marco definido por la política de gestión de documentos electrónicos de una organización en el que se diseñan, implantan y desarrollan las prácticas de gestión de documentos electrónicos establecidas en forma de programa de actuación, dotándose así de los recursos oportunos para su funcionamiento.

El sistema de gestión de documentos se articula sobre las fases del ciclo de vida de los documentos y se nutre de los documentos incorporados a través del proceso de captura, independientemente de que los documentos hayan sido creados dentro o fuera de la propia organización.

Los componentes del sistema de gestión de documentos electrónicos son los siguientes:

1. La política, como elemento normativo o regulador, que actuará como habilitador para el establecimiento del sistema.
2. Los recursos, tanto humanos como materiales, necesarios para el correcto funcionamiento del sistema.
3. Un programa de tratamiento para la gestión de documentos electrónicos.
4. Los propios documentos y expedientes electrónicos, una vez validados e incorporados al sistema.

Gestión de la interoperabilidad de documento electrónicos

Para garantizar la interoperabilidad en relación con la recuperación y conservación de los documentos electrónicos a lo largo de su ciclo de vida, se toma en cuenta lo establecido por la Dirección General del Archivo Nacional de Costa Rica (DGAN).

De esta manera, el sistema de gestión debe cumplir con la función de transferencia de información de documentos hacia un repositorio de documentos digitales que permita la gestión de objetos digitales a través del tiempo, por medio de programas de preservación digital, el cual debe tener capacidad de (Ver ilustración 2):

- **Ingreso**: De los documentos para la ingesta en el repositorio digital, aplicando controles que permitan el ingreso, control de procedencia, antivirus y formatos.
- **Almacenamiento**: Almacenaje físico de los documentos. Incluye las estrategias de preservación fijadas por la DGAN para garantizar el acceso a la información a través del tiempo.
- **Dirección de Datos**: Es una proceso-fase donde se conservan los metadatos que poseen los documentos, tanto los que se generan en el proceso de ingesta como aquellos que se

irán incorporando durante la vida del documento.

- **Preservación:** Se establecen políticas y los responsables de vigilar los cambios constantes en tecnología como revisión de formatos, hardware y software.
- **Acceso:** Permite la accesibilidad del repositorio digital, y por ende la consulta de los documentos por parte de los usuarios.
- **Administración:** Es la integración de funciones, los sujetos y la tecnología de un modelo abierto de archivo digital.

Para la gestión de interoperabilidad de archivos digitales abiertos se recomienda el envío de documentos entre sistemas por medio de paquetes de información de archivo y paquetes de información de transferencia, como por ejemplo lo estipulado en la normativa OAIS (ISO 14721:2015):

1. **Paquete de transferencia de información**: la información de contenido y descripción de los documentos (procedencia, contexto, referencias, derechos de acceso, autenticidad, integridad, entre otros aspectos) que se entrega por parte de las instancias de las entidades del Gobierno de Costa Rica, para usarla en la construcción o actualización del paquete de información de archivo.
2. **Paquete de información de archivo**: es el paquete de información-intercambio y el mecanismo para contener la información y ejecutar los procesos de preservación. Estos contienen distintos tipos de datos, a saber: la información de contenido, la información descriptiva y de relaciones, la información de conservación asociada, incluidas las modificaciones necesarias para ser almacenado, y el fichero mismo auto contenido. Los paquetes deben ser almacenados de manera que permitan la búsqueda de información por sus nodos o como ficheros comprimidos (El formato del paquete de intercambio será gestionado por la DGAN).

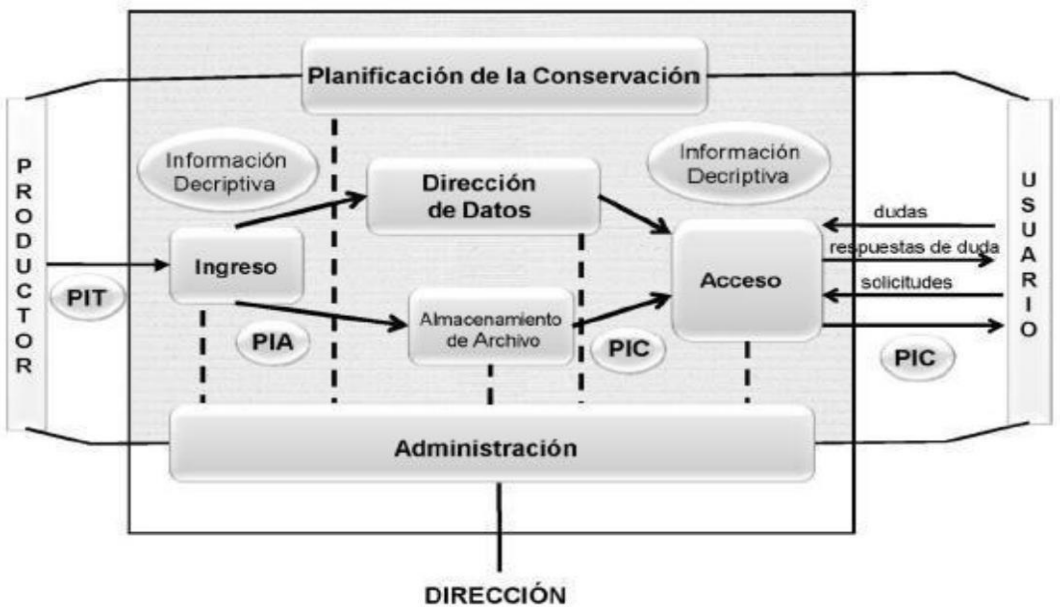

Ilustración 2. Elaboración propia.

Gestión de metadatos para intercambio de documentos digitales

Existen metadatos técnicos, tecnológicos, administrativos y de preservación. Los metadatos se incluyen desde el momento en el que se crea un documento, pueden ser insertados manual o automáticamente y se van acumulando durante los eventos en la vida del documento, son parte integral de la información en custodia y deben ser protegidos de la eliminación no autorizada.

Los metadatos se deberían definir para:

- Permitir la identificación y recuperación de documentos.
- Asociar los documentos con las cambiantes reglas de negocio, políticas y regulaciones.
- Asociar documentos con agentes, sus permisos y sus derechos sobre los documentos.
- Asociar documentos con las actividades de la organización.
- Dejar huella de los procesos llevados a cabo sobre los documentos, tales como cambios en las reglas de acceso o migraciones a nuevas aplicaciones.

Además, los metadatos para la gestión de documentos deberían representar:

- El contexto de la organización.
- Las dependencias y las relaciones entre los documentos y las aplicaciones de gestión documental.

- Las relaciones con el contexto legal y social.
- Las relaciones con los agentes que crean gestionan y usan los documentos.

Por tanto, los metadatos de gestión de documentos se deben describir y documentar en esquemas de metadatos, los cuales se han de basar en los resultados de la identificación y valoración para el área o áreas de la organización que los va a aplicar.

Metadatos para gestión

Los esquemas de metadatos se deben desarrollar para definir qué metadatos se usan para identificar, describir y gestionar procesos de gestión de documentos. Para que los documentos tengan características de documentos fidedignos, los metadatos que tengan asociados deberían basarse en metadatos autorizados por la DGAN.

Por ello se recomienda implementar el conjunto de metadatos recomendados por la DGAN que permitan definir la información que utiliza un repositorio para soportar el proceso de preservación digital, así como a las unidades sistemáticas que utilizan los repositorios garantizar la perdurabilidad de los documentos, que sean recuperables y que evidencian los metadatos, junto con las políticas del repositorio que almacena tales documentos. Un ejemplo de este tipo es la normativa PREMIS (Preservation Metadata: Implementation Strategies), usada por la DGAN.

Metadatos para codificación

Se recomienda la utilización de metadatos de codificación deben dotar de un esquema de metadatos con la estructura de etiquetas XML, para que se permita fácilmente la descripción y gestión de objetos digitales, permitiendo así el intercambio de esos objetos entre repositorios. Por ejemplo, la normativa METS (Metadata Encoding & Transmission Standard).

Metadatos para descripción y preservación

Se recomienda la utilización de metadatos para:

- La descripción archivística para identificar y explicar el contexto y contenido de los documentos de archivo con el fin de hacerlos accesibles. Los procesos descriptivos comienzan con la producción de los documentos y continúan a lo largo de todo su ciclo vital. Los elementos específicos de información sobre los documentos de archivo se establecen en cada una de las fases de su gestión (como producción, selección, acceso, conservación, organización) ya que dichos documentos deben, por un lado, ser protegidos y controlados de una manera segura, y por otro, resultar accesibles a su debido momento para todo aquel que tenga el derecho a consultarlos

- La descripción archivística se refiere a cada uno de los elementos de información con independencia de la fase de gestión en la que se identifique o establezca. En todas las fases, la información sobre dichos documentos permanece dinámica y puede ser objeto de corrección para un mayor conocimiento de su contenido o del contexto de su producción. Especialmente, los sistemas de información automatizados pueden resultar útiles tanto para integrar o seleccionar los elementos de información cuando se precise actualizarlos o modificarlos. Aunque el principal foco de atención de estas reglas se centra en la descripción de los materiales de archivo a partir del momento en el que se han seleccionado para su conservación, también puede aplicarse a las fases previas.

Este conjunto de reglas generales para la descripción archivística tiene como principales objetivos:

- Garantizar la elaboración de descripciones coherentes, pertinentes y claras.
- Facilitar la recuperación y el intercambio de información sobre los documentos de archivo.
- Compartir los datos de autoridad.
- Hacer posible la integración de las descripciones procedentes de distintos lugares en un sistema unificado de información. Por ejemplo, la normativa ISAAD(G) General International Standard Archival Description (Norma Internacional General de Descripción Archivística).
- La descripción de entidades (instituciones, personas y familias) asociadas a la producción y a la gestión de archivos.

  Los registros de autoridad de archivos se pueden utilizar para:

- Describir una institución, persona o familia como unidades dentro de un sistema de descripción archivístico.
- Controlar la creación y utilización de los puntos de acceso en las descripciones archivísticas.
- Documentar las relaciones entre diferentes productores de documentos y entre estas entidades y los documentos creados por ellas, y/o otros recursos que les conciernen.
- Describir los productores de los documentos de archivo. Este proceso requiere una extensa documentación y una actualización continua del contexto de producción y uso de los documentos, especialmente de su procedencia. Por ejemplo, la normativa ISAAR(CPF) International Standard Archival Autorithy o la Records for Corporate

Bodies, Persons and Families, (Norma Internacional sobre los Registros de Autoridad de Archivos relativos a Instituciones, Personas y Familias).

- Describir las instituciones que conservan fondos de archivo, asimismo permitiendo:
    - Proporcionar directrices prácticas para identificar y contactar con las instituciones que detentan los fondos de archivo, y acceder a los mencionados fondos y a los servicios que la institución ofrece.
    - Crear directorios y/o listas autorizadas de instituciones que custodian fondos archivísticos.
    - Establecer enlaces con listas autorizadas de bibliotecas y museos y/o desarrollar directorios comunes de instituciones que custodian el patrimonio cultural a nivel regional, nacional o internacional.
    - Producir estadísticas sobre las instituciones que detentan documentos de archivo a nivel regional, nacional e internacional.

Estas descripciones pueden utilizarse para:

- Describir instituciones como unidades dentro de un sistema de descripción archivística.
- Servir como punto de acceso normalizado a las instituciones que custodian los fondos de archivo, en el seno de un directorio, en un sistema de información archivística o en la red.
- Documentar las relaciones entre las instituciones y entre esas entidades y los documentos de archivo que custodian. Por ejemplo, la normativa ISDIAH (International Standard for Describing Institutions with Archival Holdings) (Norma internacional para describir instituciones que custodian fondos de archivo).
- Describir las funciones de instituciones vinculadas con la producción y conservación de documentos. A lo largo de toda esta norma se utiliza el término "función" para referirse no sólo a la función sino también a cualquiera de las divisiones de la misma como subfunción, proceso, actividad, tarea, acción u otro término de uso internacional, nacional o local; de manera que pueda utilizarse para describir una función o cualquiera de sus divisiones. Por ejemplo, la normativa ISDF (International Standard for Describing Functions) (Norma internacional para la descripción de funciones).

Tecnologías recomendadas para la interoperabilidad de sistemas de información

Antes de iniciar cualquier proyecto de interoperabilidad de sistemas de información es

importante iniciar con un conjunto de preguntas base.

¿Cómo se define la interoperabilidad?

Se entiende por interoperabilidad la habilidad de organizaciones y sistemas dispares y diversos para interactuar con objetivos consensuados y comunes y con la finalidad de obtener beneficios mutuos. La interacción implica que las organizaciones involucradas compartan información y conocimiento a través de sus procesos de negocio, mediante el intercambio de datos entre sus respectivos sistemas de tecnología de la información y las comunicaciones. (Gascó, Mila & Jimenez-Gomez, Carlos & Criado, J. Ignacio, 2010. Bases para una Estrategia Iberoamericana de Interoperabilidad. 10.13140/RG.2.1.4897.8001.).

La interoperabilidad es la capacidad de que las organizaciones interactúen con vistas a alcanzar objetivos comunes que sean mutuamente beneficiosos y que hayan sido acordados de manera previa y conjunta. Para ello recurren a la puesta en común de información y conocimientos a través de los procesos institucionales que apoyan, mediante el intercambio de servicios, datos o documentos entre sus respectivos sistemas de tecnologías de la información y las comunicaciones (TIC) (Comisión Europea, 2010).

¿Cuál es la razón de la interoperabilidad?

La interoperabilidad en sí misma no es un objetivo, es el medio para facilitar un proceso con el fin de brindar un servicio de manera más eficiente.

Desde 2004 se pone énfasis a la interoperabilidad en tanto eje de generación de beneficios para la ciudadanía, las empresas y las organizaciones. Lueders (2004, pág. 3) ya mencionaba por ese entonces que “las últimas iniciativas europeas han colocado la interoperabilidad en el centro de atención de la actividad regulatoria de la Unión Europea en materia de Tecnologías de la Información y Telecomunicaciones (TICs)”.

De acuerdo con el Banco Interamericano de Desarrollo (BID, 2019), la interoperabilidad cumple varias funciones: como factor de progreso, como herramienta para gestionar y compartir información, y como soporte para la formulación de políticas públicas. La interoperabilidad se da cuando varios sistemas y dispositivos pueden intercambiar datos, interpretarlos y mostrarlos en forma sencilla para el usuario.

> “*Permite construir sistemas que pueden iniciarse con pocos actores e ir escalando ordenadamente hasta incorporar un mayor número de instituciones, así como de casos de uso y procesos entre los participantes, rehusando microservicios o construyendo otros nuevos para generar así una plataforma que crece y se fortalece*” (BID, 2019, pág. 8).

¿De dónde sale la necesidad?

Es importante determinar quién es el dueño (persona o departamento de una organización) y que se desea automatizar por medio de la interoperabilidad.

¿Qué se quiere lograr?

Es visualizar, diagramar y documentar el proceso y el servicio que se va a brindar por medio de la interoperabilidad.

¿Cómo se puede aplicar para el beneficio ciudadano?

Explicar cómo va esto a mejorar la calidad de vida, acceso a la información y reducción de trámites.

¿Cómo lo podemos lograr?

Determinar si se poseen los recursos necesarios: personal capacitado tanto en conocimiento de los procesos organizaciones como con conocimientos técnicos, recursos económicos y por último tecnológicos.

Con base en las preguntas anteriores, se recomienda:

1. Determinar la madurez de la organización según se expuso con anterioridad.
2. Determinar el proceso o procesos que se desea automatizar o interoperar y quién es el dueño y líder de ese proceso, con el conocimiento y dominio sobre el mismo (Interoperabilidad Organizativa).
3. Determinar e identificar el marco normativo vigente para garantizar el cumplimiento de este y la protección de los datos de las personas (Interoperabilidad Normativa/Legal).
4. Determinar qué información se requiere recibir, enviar y/o compartir hacia la persona o ente que va a utilizar del servicio del proceso que se pretende interoperar (Interoperabilidad Semántica).
5. Determinar qué tecnología o conjunto de tecnologías necesito para automatizar el proceso del servicio que se desea brindar (Interoperabilidad Técnica).

   Partiendo de los enunciados anteriores, es importante notar que el último paso es la determinación técnica, ya que esta tendrá éxito en la medida que el proceso, los requerimientos y los entregables del servicio por interoperar estén claros y documentados.

De la cadena de Interoperabilidad

- Infraestructura y servicios asociados: con qué infraestructura arquitectónica y tecnológica se cuenta para brindar los servicios que ofrece a los ciudadanos, empresas y organizaciones.

- Modelos de integración de datos: cuáles son los datos que se han de interoperar y cuál es su significado semántico.

- Integración de sistemas y servicios: las tecnologías de software y/o hardware utilizados en la automatización de los procesos por ser interoperables.

- Accesibilidad multicanal integrada y segura: los protocolos de interconexión para la transferencia de información que permita realizar publicaciones del servicio interoperable.

Finalmente, a quien interese profundizar en los estándares internacionales, a continuación, se ofrece la lista completa de aquellos que fueron tomados en cuenta para elaborar el presente capítulo:

OData v4 Open Data Exchange Protocol OASIS (Organization for the Advancement of Structured Information Standards)
REST Representational State Transfer Architectural Styles and the Design of Network-based Software Architectures, Roy Thomas Fielding
WSDL 1.1 Web Services Description Language 1.1 W3C
SOAP 1.1 y 1.2 Simple Object Access Protocol 1.1 y 1.2 W3C
XML 1.0 Extensible Markup Language 1.0 W3C

XSD XML Schema Definition Language W3C
HTTP/1.1
Hypertext Transfer Protocol Internet Engineering Task Force
HTTP/2 Hypertext Transfer Protocol Version 2 Internet Engineering Task Force
FTP FILE TRANSFER PROTOCOL Internet Engineering Task Force
The Text/Plain Format and DelSp Parameters Internet Engineering Task Force
ISO 14721:2012 (CCSDS 650.0-M-2) Preview Space data and information transfer systems Open archival information system (OAIS)
ISDF Norma internacional para la descripción de funciones INTERNATIONAL COUNCIL ON ARCHIVES
ISDIAH Norma internacional para describir instituciones que custodian fondos de archivo INTERNATIONAL COUNCIL ON ARCHIVES
PREMIS Preservation Metadata: Implementation Strategies Data Dictionary for Preservation Metadata, The Library of Congress of United States
ISAAR (CPF) Norma Internacional sobre los Registros de Autoridad de Archivos relativos a Instituciones, Personas y Familias INTERNATIONAL COUNCIL ON ARCHIVES

ISAD(G) Norma Internacional General de Descripción Archivística INTERNATIONAL COUNCIL ON ARCHIVES
METS
Metadata Encoding and Transmission Standard The Library of Congress of United States

MARCO DE INTEROPERABILIDAD NACIONAL

Los proyectos de Interoperabilidad conllevan la integración de sistemas aislados que comparten información, además de que aprovechan el concepto de trabajo en forma coordinada, donde las instituciones tienen un rol y funciones específicas dentro de este marco de trabajo propuesto.

Lo anterior facilita y agiliza la implementación de trámites y gestiones a los usuarios, brindando tanto a personas usuarias, las organizaciones participantes y al Estado beneficios entre los que se pueden mencionar:

- Escalabilidad. Otro aspecto importante de los sistemas, donde se implementa la interoperabilidad, es que los mismos son sistemas escalables, tanto en cantidad de usuarios y/o en procesos, por lo cual se puede empezar por grupos focales aislados y con pocos procesos interoperables.
- Automatización de servicios. Lo cual facilita la agilidad de trámites por parte de las organizaciones; la información se registra una vez con celeridad y la plataforma de intercambio de información, facilita la misma para los diferentes actores involucrados (entidades autorizadas que requieran esta información), velando por la protección de la información del ciudadano y respetando el marco de la legalidad.
- Reducción de costos. El ahorro en consumo de papel, folios, lugares físicos de almacenamiento, la redundancia de documentos, entre instituciones se ve reducida, porque la inversión se haría una única vez en infraestructura tecnológica para el almacenamiento de la información, utilizando las mejores técnicas de seguridad informática y protección de datos que además de brindar tranquilidad a la ciudadanía también se apega y cumple con los principios estipulados en las leyes y en los marcos de seguridad del país en lo referente a datos y tecnología de la información.

- Salud ciudadana. Esto es un gran beneficio a los usuarios venido del descongestionamiento de instituciones, calles y zonas públicas, para una mejor calidad de vida de las personas.
- Transparencia de la información. Los datos no son susceptibles a la edición, sin la debida solicitud, modificación o alteración, además los usuarios saben qué uso se ha dado a su información.
- Visión integral de servicios públicos y privados. Un beneficio obtenido con el marco de servicios de interoperabilidad que ve al usuario como un todo por lo cual, las organizaciones pueden realizar estimaciones, crear políticas y que se facilite la toma de decisiones interinstitucionales, amparados en el marco de la protección de datos.
- Análisis e inteligencia de datos. Técnicas como Big Data podrían ser utilizadas para generar modelos estadísticos y predictivos, lo cual permite dar seguimiento y acercamiento a las regiones sociales más vulnerables, por tanto, en sistemas de intercambio de información se podrían mostrar tendencias sociales en zonas de riesgo y dar pronta respuesta por ejemplo en caso de embarazos en adolescentes, escolarización, delincuencia etc. Todo esto considerando pertinencia, las leyes del país y el marco de legalidad en el uso de los datos.
- Atención proactiva. Implementación proactiva y automatizada de trámites hacia las personas, siguiendo las cadenas de decisión un trámite puede nacer al momento que el sistema detecta que un individuo seleccionado cumple con todos los requerimientos.

El Marco de Interoperabilidad Nacional es un requisito para poder lograr de forma efectiva y eficiente la comunicación digital y el intercambio de información entre las diferentes instituciones de la Administración Pública con la finalidad de lograr servicios digitales para las personas, que se encuentren integrados y con apego a la normativa vigente en el país. Ofrece la posibilidad que las empresas privadas y las instituciones de la academia puedan interactuar con las instituciones del Estado.

La definición de este marco nacional tiene como propósito:

- Simplificar los servicios que el Estado ofrece a las personas, empresas y otras organizaciones.
- Promover la cooperación entre las diferentes instituciones de la Administración Pública para generar mejores servicios.
- Iniciar a definir los estándares de trabajo, organizacionales, semánticos y técnicos para la interacción de las instituciones por medio de la interoperabilidad.
- Reducir los costos y esfuerzos en la implementación e integración de las instituciones para ofrecer servicios a las personas por medio de la interoperabilidad.

- Reducir los costos y esfuerzos de las personas para adquirir los servicios que el Estado le ofrece.
- Mejorar la calidad y la agilidad de los servicios por medio de la automatización, promoviendo la creación de servicios proactivos basados en experiencias de vida de las personas.
- Generar mayor transparencia del Estado, en el uso de los datos y la información de las personas, y por medio de los Datos Abiertos.
- Promover una visión integral en los servicios públicos y privados.
- Propiciar un clima de negocios favorable y competitivo para el país.

El Marco de Interoperabilidad Nacional consiste en la implementación de 9 etapas o pasos con una visión nacional:

1. Participación, sensibilización y homologación del lenguaje.
2. Estructura y organización de la interoperabilidad.
3. Marco de interoperabilidad.
4. Modelo de interoperabilidad.
5. Identificación de la situación actual, conceptos, encuestas y métricas.
6. Definir la estrategia de la interoperabilidad.
7. Servicios de interoperabilidad.
8. Procesos de interoperabilidad.
9. Implementación de la interoperabilidad.

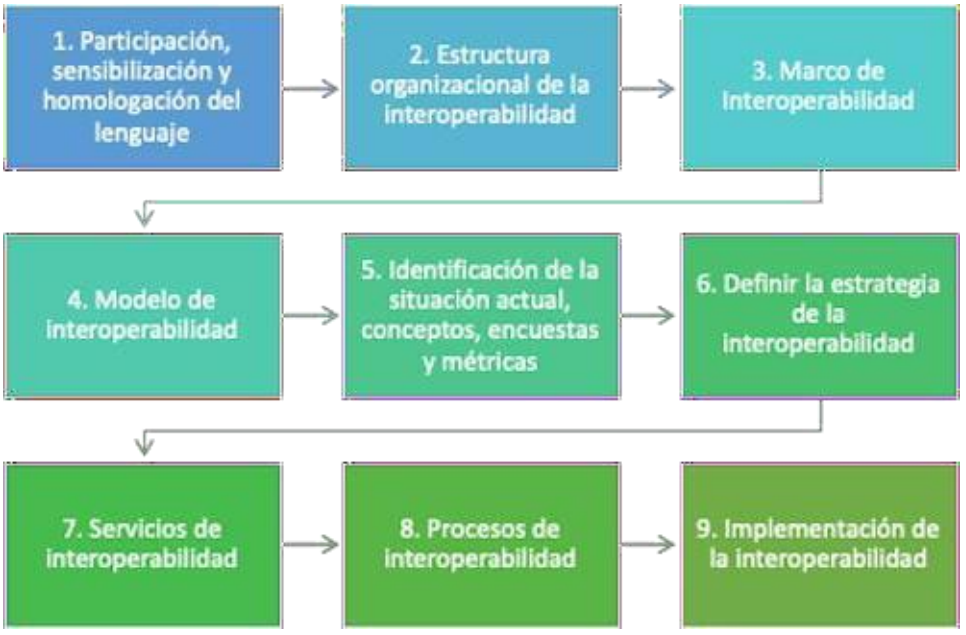

Ilustración 3. Elaboración propia basado en Cepal, 2021.

Las herramientas que se presentan han sido modificadas y adaptadas de las propuestas por el libro de CEPAL titulado Gobernanza Digital e Interoperabilidad Gubernamental, una guía para su implementación. Esta guía metodológica que se presenta en el libro mencionado fue diseñada a partir de la experiencia en el marco de la asistencia técnica sobre interoperabilidad gubernamental prestada al Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) del Gobierno de Costa Rica, durante el período del agosto 2019 a diciembre 2020.

Etapa 1 - Participación, sensibilización y homologación del lenguaje

Este primer paso se encuentra a cargo del MICITT como ente Rector en Tecnología por medio de la Dirección de Gobernanza Digital y Certificadores de firma digital. Consiste en la coordinación para lograr que la mayor cantidad de instituciones de la Administración Pública participen, se sensibilicen y tengan un lenguaje común acerca de la interoperabilidad. El propósito es lograr que las instituciones que se encuentren interoperando y las que no lo hacen aún, adopten el marco nacional y se conecten a la propuesta de interoperabilidad nacional.

Se definen cuatro aspectos bajo los cuales se demanda un cambio de paradigma dentro de las instituciones que son:

1. Cambio en la cultura institucional: para aumentar el enfoque de servicio a las personas, generando procesos que sean impulsados por las personas para el desarrollo de los servicios digitales.
2. Cambio en los procesos institucionales: en el diseño de los servicios digitales de las personas procurando la mayor eficiencia y eficacia.
3. Cambios en la institución: promoviendo una visión compartida para brindar los servicios a las personas y adoptando nuevas formas de organización y coordinación interinstitucional.
4. Cambio en la forma de relación con las personas: generando canales más inclusivos y que permitan un mayor contacto de las personas con la institución para poder ofrecer y atender las necesidades de las personas. Se solicita promover la comunicación de los nuevos servicios digitales por los diferentes canales de comunicación con los que se cuente.

Las instituciones podrán solicitar capacitaciones a la Dirección de Gobernanza Digital y Certificadores de firma digital para la sensibilización y capacitación técnica de sus funcionarios, la cual será realizada por quien indique el MICITT por medio de dicha dirección.

La siguiente herramienta permite identificar el cumplimiento de la participación, sensibilización y homologación del lenguaje:

Participación, sensibilización y homologación del lenguaje			
Acciones	**¿Cumple?**		**Observaciones**
	Sí	**No**	
¿Se tiene conocimiento y claridad en la institución sobre la interoperabilidad y los procesos que esta conlleva?			
¿Se han solicitado capacitaciones a la Dirección de Gobernanza Digital y Certificadores de firma digital, para la capacitación técnica de funcionarios?			
¿Se han realizado de forma adecuada las capacitaciones solicitadas?			
¿Se ha generado un cambio en la cultura institucional, que permita aumentar el enfoque de servicio a las personas y el impulso de desarrollo de servicios digitales?			
¿Se ha generado un cambio en los procesos institucionales que garantice la mayor eficiencia y eficacia en el diseño de servicios digitales?			
¿Se ha generado un cambio en la institución que promueva una visión compartida para brindar servicios a las personas?			
¿Se han adoptado nuevas formas de organización y coordinación interinstitucional? ¿Cuáles?			
¿Se han generado canales más inclusivos que permitan el contacto de las personas con la institución?			
¿Se ha promovido la comunicación de los nuevos servicios digitales por diferentes canales de comunicación?			

Herramienta de Interoperabilidad, 1. Elaboración propia.

Etapa 2 - Estructura y organización de la interoperabilidad

A nivel nacional el MICITT como Rector en Tecnología define la política pública. El país cuenta con un mecanismo de Gobernanza Digital que es la Comisión de Alto Nivel de Gobierno Digital (CNANGD), como un ente asesor para el desarrollo de la estrategia nacional orientada a la implementación de la política pública en gobierno digital, con el objetivo principal de recomendar las acciones que potencien el uso de las tecnologías digitales para mejorar el funcionamiento del Sector Público Costarricense y con ello el bienestar de los habitantes, la productividad de las empresas y la competitividad del país.

El MICITT y la CNANGD generan las recomendaciones para que por medio de la Dirección de Gobernanza Digital y Certificadores de firma digital se generen las coordinaciones interinstitucionales, el desarrollo de la política pública, los lineamientos, directrices y normativas técnicas relacionadas con la interoperabilidad. La DGDCFD articulara la implementación técnica de la interoperabilidad a nivel nacional como un servicio transversal.

Para la implementación de la interoperabilidad es necesario contar con canales de comunicación para que los diferentes sectores puedan brindar sus insumos y necesidades de servicios digitales. Al mismo tiempo, se debe contar con contactos dentro de las diferentes instituciones como enlaces que puedan coordinar con el MICITT y la DGDCFD, y coordinar las implementaciones técnicas.

Ilustración 4. Fuente: ETD,2023, pág. 51.

Para cada una de las instituciones se solicita la creación de un Equipo Ad Hoc Interno de Interoperabilidad el cual debe estar conformado al menos con los siguientes integrantes:

- Persona funcionaria designada como enlace de Tecnologías de Información y Comunicación de la Institución.
- Una persona funcionaria de la Dirección o el Departamento Legal de la institución.
- Persona funcionaria designada como el enlace de ciberseguridad de la institución.
- Persona funcionaria del despacho del jerarca institucional de gobierno digital, quien tendrá el rol del coordinador del Equipo Ad Hoc Interno de Interoperabilidad, basado en el artículo 2 de la Directriz 019-MP-MICITT, a menos que el jerarca de la institución designe a otra persona con este rol o el propio equipo por votación de la mayoría de los

miembros decida nombrar a otra persona.

- Persona funcionaria designada como el Oficial de Simplificación de Trámites.
- Persona funcionaria designada como el Oficial de Acceso a la Información.
- Una persona funcionaria del equipo de Tecno o del departamento o unidad de planificación institucional.

Se ha elaborado la siguiente herramienta de control para guiar la implementación de este paso del marco nacional de interoperabilidad:

Herramienta de control para la Creación del Equipo Ad Hoc Interno de Interoperabilidad			
Se establece el equipo responsable dentro de la institución de la gestión del intercambio de los servicios de información y propuestas de servicios.			
Fecha de aplicación:			
Punto de cumplimiento:	**¿Cumple?**		**Acción por realizar**
	Sí	**No**	
¿Se ha realizado la conformación del Equipo?			
¿Forma parte el enlace institucional de Gobierno Digital?			
¿Forma parte el Oficial de Simplificación de Trámites?			
¿Forma parte el Oficial de Acceso a la Información?			
¿Forma parte un representante de TIC?			
¿Forma parte un representante del departamento legal de la institución?			
¿Forma parte el enlace de ciberseguridad?			
¿Hay representación del despacho del jerarca o de planificación institucional?			
¿El Equipo cuenta con el oficio de conformación para realizar las labores y responsabilidades?			

¿Los miembros del equipo se encuentran capacitados y sensibilizados con el Marco de Interoperabilidad Nacional?			
¿Se ha definido una reunión periódica para la identificación de las iniciativas de servicios para interoperar?			
¿Se cuenta con un plan de trabajo para atender las convocatorias de trabajo necesarias para el funcionamiento de la Comisión Interna de Interoperabilidad?			
¿Se lleva registro en actas de trabajo del Equipo sobre el desarrollo de las propuestas de servicios de interoperabilidad?			
¿Se cuenta con los recursos materiales y de tiempo para ejecutar las labores del Equipo de Interoperabilidad?			

Herramienta de Interoperabilidad, 2. Elaboración propia.

Etapa 3 – Marco de interoperabilidad

El marco de interoperabilidad ha tomado como referencia el Marco Europeo de Interoperabilidad, el Modelo de Madurez de Interoperabilidad propuesto por el BID y la experiencia de los marcos de interoperabilidad de países líderes tales como Estonia, Alemania, Australia, Países Bajos, Reino Unido, Dinamarca y Nueva Zelanda.

En nuestra implementación nacional se propone poder implementar los principios fundamentales definidos por el Marco Europeo de Interoperabilidad en nuestras instituciones, los cuales son:

1. Subsidiariedad y proporcionalidad
2. Apertura
3. Transparencia
4. Posibilidad de reutilización
5. Neutralidad tecnológica y portabilidad de los datos
6. Primacía del usuario
7. Inclusión y accesibilidad
8. Seguridad e intimidad
9. Multilingüismo

10. Simplificación administrativa
11. Conservación de la información
12. Evaluación de efectividad y eficiencia

Para poder lograrlo se define la implementación de las cuatro dimensiones de la interoperabilidad para cada servicio los cuales desarrollaremos sus herramientas de control más adelante y son:

1. Dimensión Legal o normativa.
2. Dimensión Organizacional
3. Dimensión Semántica
4. Dimensión Técnica

Siguiendo las recomendaciones del BID, se definirá en una siguiente versión del CNTD el modelo de madurez para la interoperabilidad de las instituciones de la Administración Pública.

El Equipo Ad Hoc Interno de Interoperabilidad es el encargado de aplicar el marco de interoperabilidad dentro de la institución, velando por el cumplimiento de los 12 principios descritos en esta sección. Para esto, deberán elaborar un informe anual de implementación, seguimiento y estado de cada uno de los principios indicando la forma en la cual se da cumplimiento a cada uno de ellos. Este informe debe ser enviado al despacho del jerarca de la institución. El Equipo Ad Hoc Interno de Interoperabilidad, será también el encargado de aplicar el modelo de madurez para la interoperabilidad en coordinación con la Dirección de Gobernanza Digital y Certificadores de firma digital del MICITT.

Etapa 4 – Modelo de interoperabilidad

Para Costa Rica se ha definido el **modelo de interoperabilidad federado con datos en la institución fuente**.

Este es uno de los modelos más aceptados en la actualidad, en la cual cada institución u organización produce y mantiene sus datos e interopera con un ente rector federado. Para nuestro país, ese ente federado de la interoperabilidad será definido por el MICITT por medio de la Dirección de Gobernanza Digital y Certificadores de firma digital.

En el modelo en ente federado canaliza todas las transacciones del organismo fuente de datos o información hacia el organismo consumidor que solicitante, así como las gestiones de actualización de información que se puedan desarrollar. El sistema federado registra las transacciones que se ejecutan en su sistema, pero no almacena bases de datos, salvo los casos que son necesarios para desarrollar informes del sistema federado. Las bases de datos y la información se encuentran descentralizadas del sistema federado y bajo el control de cada

institución dueña de estas.

El Equipo Ad Hoc Interno de Interoperabilidad deberá identificar el modelo de interoperabilidad actual con el que cuenta la institución, el cual puede ser:

1. Bilateral o descentralizado.
2. Centralizado.
3. Federado con datos en la institución fuente.

Si la institución no cuenta con un modelo de interoperabilidad o cuenta con alguno de los dos primeros, el Equipo Ad Hoc Interno de Interoperabilidad iniciará un plan de trabajo para definir un plazo de migración al modelo federado con datos en la institución fuente, bajo la normativa que lo acoja y en el marco de sus capacidades, siempre realizando una evaluación costo beneficio para la ejecución de ese plan de trabajo.

Se realiza la siguiente herramienta que contiene elementos relacionados con el modelo de interoperabilidad que se debe establecer en las instituciones:

Modelo de interoperabilidad de la institución			
Identificación de modelo de interoperabilidad de la institución			
Elementos de interoperabilidad	**¿Cumple?**		**Acción por realizar**
	Sí	**No**	
¿Se tiene claridad y conocimiento de los modelos de interoperabilidad?			
¿Cuenta la institución con un modelo de interoperabilidad?			
¿El modelo de interoperabilidad es bilateral o descentralizado?			
¿El Equipo Ad Hoc Interno inició un plan de trabajo para migrar del modelo bilateral o descentralizado al modelo federado con datos en la institución fuente?			
¿El modelo de interoperabilidad es centralizado?			
¿El Equipo Ad Hoc Interno inició un plan de trabajo para migrar del modelo centralizado al modelo federado con datos en la institución			
¿El modelo de interoperabilidad es federado con datos en la institución fuente?			

Herramienta de Interoperabilidad, 3. Elaboración propia.

Etapa 5 - Identificación de la situación actual, conceptos, encuestas y métricas

Con el propósito de establecer un punto de partida dentro de la institución, el Equipo Ad Hoc Interno de Interoperabilidad realizará las siguientes actividades:

1. Difundir el diccionario de términos o glosario para definir dentro de la institución un mismo lenguaje para los diferentes conceptos de la interoperabilidad. Una base de estos términos se encuentra en el glosario del presente CNTD.
2. Aplicar la Herramienta de interoperabilidad 4, denominada “Herramienta de interoperabilidad institucional”.

Herramienta de interoperabilidad institucional					
Herramienta de diagnóstico de la institución sobre una base común de consultas y relevantes para la interoperabilidad a nivel nacional.					
Observaciones:					
Fecha de aplicación:					
Nombre del proveedor de servicios de interoperabilidad:					
Responsable actual de la interoperabilidad en la institución:					
Listado de servicios de interoperabilidad vigentes en la institución	Servicio 1	Servicio 2	Servicio 3	…	Servicio N
Consumidor del servicio de interoperabilidad					
Contraparte institucional de la interoperabilidad (Consumidor)					
¿Existen acuerdos firmados de colaboración con otras instituciones?					
¿El servicio se encuentra contenido en un gestor de convenios?					

¿El servicio sigue el principio de gratuidad?					
¿El servicio tiene definidos sus metadatos?					
¿El servicio usa un catálogo de esquemas y metadatos?					
¿El servicio forma parte del catálogo de servicios de la institución?					
¿El servicio exige un acuerdo de competencia?					
¿El servicio se adhiere al principio de finalidad?					
¿El servicio usa documento electrónico?					
¿El servicio cuenta con firma digital certificada?					
¿El servicio cuenta con equivalencia funcional?					
¿El servicio usa directorio de datos?					
¿El servicio usa la estandarización definida para estos efectos?					
¿El servicio está implementado como interfaz de programación de aplicaciones (API) o de servicios Web (Web Services)?					

¿El servicio cumple con la implementación del protocolo de internet IP versión 6 (IPv6)?					
¿Existen procedimientos de modificación y eliminación de un servicio de interoperabilidad?					
¿Existen procedimientos y herramientas de monitoreo?					
¿Existen procedimientos y herramientas de publicación de servicios de interoperabilidad?					
¿Existen procedimientos y herramientas de registro de trazabilidad?					
¿Se ha revisado que el servicio cumpla con la normativa de protección de datos de las personas vigente en el país?					
¿El servicio cuenta con información que pueda ser utilizada para Datos Abiertos?					
¿Si la respuesta anterior es positiva, se han implementado Datos Abiertos sobre este servicio?					

Herramienta de interoperabilidad, 4 Elaboración propia.

3. Aplicar la Herramienta de interoperabilidad 5, denominada “Herramienta de Antecedentes adicionales solicitados”.

Herramienta de antecedentes adicionales solicitados				
Identificación de otros antecedentes relacionados con la interoperabilidad y la institución.				
Otros antecedentes	Nombre de la Institución	Datos solicitados	Tipo de dato	Requerimiento solicitado para interoperar
Instituciones que les han solicitado datos				
…				
Instituciones que les han solicitado datos				
…				
¿Existe una política de interoperabilidad en la institución?				
¿La interoperabilidad se prioriza como un objetivo estratégico de la institución?				
Número de instituciones a las cuales atienden:				
¿De quién depende el área de informática de la institución?				
¿Cuenta con profesionales con experiencia en arquitectura o servicios interoperables?				

¿Con cuántos profesionales cuenta para aplicar la interoperabilidad en su institución?	
En promedio, ¿cuántos años de experiencia tienen en interoperabilidad?	
¿El personal de interoperabilidad es interno o externo?	
¿En qué proporción es interno/externo?	
Enuncie los principales factores que impiden o limitan la interoperabilidad en su institución	
¿Cuáles, a su juicio, serían los incentivos más efectivos para promover mayores niveles de interoperabilidad?	
¿Existe alguna estimación de aumento en la oferta o demanda de servicios de interoperabilidad?	
Detalle la oferta	

Detalle la demanda	
¿Se cuenta con la capacidad de infraestructura tecnológica para soportar el tráfico de requerimientos de interoperabilidad?	
Detalle la actual	
Detalle ¿qué estima que requiere a futuro?	
¿Cuánto es el tiempo promedio para firmar (acordar) un convenio de interoperabilidad en su institución?	

Herramienta de interoperabilidad, 5. Elaboración propia.

4. Implementar la Herramienta de interoperabilidad 6, denominada “Herramienta de indicadores de impacto a nivel de las personas”. Los indicadores iniciales propuestos son los siguientes:

Herramienta de indicadores de impacto a nivel de las personas		
Se proponen los siguientes ámbitos e indicadores para medir el nivel de impacto sobre las personas que pueden tener los servicios que interoperan o se van a interoperar en la institución.		
Ámbito	**Indicador**	**Valor del indicador**
Disminución de viajes, tiempo invertido en viajes y costo asociado al transporte,	Estimación del número de viajes realizados antes y después de la interacción	

debido a menores requerimientos de información de otras instituciones	directa entre instituciones públicas	
	Estimación del costo promedio de cada viaje	
	Estimación del tiempo promedio de espera en cada viaje	
	Estimación de salarios perdidos (indicador indirecto de incremento de la productividad), considerando la diferenciación según los beneficiarios	
	objetivo de cada trámite	
Disminución del tiempo de respuesta de la institución pública	Tiempo de espera del ciudadano en la institución pública para obtener una respuesta del trámite	
	Si corresponde, estimación de salarios perdidos	
Disminución de errores y tiempo asociado a corregir errores	Tiempo utilizado por la persona en asistir a la institución para corregir errores	
Disminución de las tarifas (o costos) de los trámites para las personas	Estimación de costos de tarifas, antes y después de interoperar	

Percepciones sobre la calidad y cantidad de información compartida	Calidad y cantidad de la información compartida entre las instituciones públicas	
Percepciones sobre la calidad del servicio	Independencia de tiempo y lugar para el usuario	
	Calidad de la resolución de problemas	
	Simplicidad de las acciones que deben realizar los usuarios para hacer el trámite (obtener el servicio)	
	Protección de la privacidad y la confidencialidad	
Total de ahorro de tiempo de la persona	Horas ahorradas por las personas en la realización de trámites como la suma de todos los tiempos ahorrados (de espera, de ir a otros servicios, de reducción de errores y demás)	
Total de ahorro de costos de las personas	Disminución de costos para los ciudadanos en la realización de trámites como la suma de todas las disminuciones de costos (por menos desplazamientos entre servicios, por reducción de tarifas y demás)	

Herramienta de interoperabilidad, 6. Elaboración propia.

5. Implementar la Herramienta de interoperabilidad 7, denominada “Herramienta de indicadores de impacto a nivel institucional”.

Herramienta de indicadores de impacto a nivel institucional		
Se proponen los siguientes ámbitos e indicadores para medir el nivel de impacto sobre la institución que pueden tener los servicios que interoperan o se van a interoperar. Esta herramienta se aplica para cada uno de los servicios que se van a interoperar (una ficha por servicio).		
Nombre de la institución:		
Servicio:		
Volumen de operaciones o transacciones mensuales en los últimos 12 meses		
Ámbito	**Indicador**	**Valor del indicador**
Reducción en el tiempo de procesos clave para la entrega de servicio	Porcentaje de reducción del tiempo destinado a almacenar papeles	
	Porcentaje de reducción del tiempo destinado a la digitación de datos	
	Porcentaje de reducción del tiempo de respuesta a las personas	
	Percepción sobre el grado de mejora en los procesos	
Ganancias de productividad	Número de trámites procesados por mes	

	Promedio del número de trámites procesados por funcionario	
Total de ahorro de tiempo del funcionario	Disminución de las horas de trabajo de los funcionarios que participan en las actividades relacionadas con los procesos que se mejoran desde el punto de vista tecnológico	
Ahorro de costos de la institución	Disminución en los gastos de soporte asociados al trámite, representados por el ahorro de papel impreso y almacenamiento	

Herramienta de interoperabilidad 7. Elaboración propia.

6. Coordinar con la Dirección de Gobernanza Digital y Certificadores de firma digital acerca de los lineamientos, directrices y normativas técnicas.

Etapa 6 - Definir la estrategia de la interoperabilidad

El Marco de Interoperabilidad Nacional propone a nivel general cuatro dimensiones: Organizacional, Normativa/Legal, Semántica y Técnica. El Equipo Ad Hoc Interno de Interoperabilidad es el encargado de definir una estrategia institucional para aplicar este Marco de Interoperabilidad Nacional definido en el presente documento. Es importante recordar que cada institución tiene un propósito que contribuye a la generación del valor público para las personas, el sector privado y otras organizaciones.

El Equipo Ad Hoc Interno de Interoperabilidad tiene la libertad para desarrollar su estrategia de interoperabilidad para cumplir con las recomendaciones presentadas en el CNTD. Como una guía para el desarrollo de la estrategia, se propone que al menos se consideren 4 grandes aspectos institucionales:

1. Propuesta de valor: Desarrollo de una propuesta de valor de los servicios digitales que la institución va a ofrecer a las personas, empresas y organizaciones. Validar que pueda ser incorporada en la Estrategia Institucional (o al menos que sea remitida por parte del Equipo al despacho del jerarca para su valoración) y que cuente con un impacto positivo al medio ambiente y que sea digitalmente inclusiva. Se debe validar que las personas, empresas y

organizaciones, entiendan y tengan claridad de esta propuesta de valor.

2. Servicios digitales para las personas: Identificar y definir los servicios digitales que permiten alcanzar la propuesta de valor.
3. Procesos y tecnologías de la información y comunicación de apoyo: Identificar los procesos y tecnologías que permiten a las personas, empresarios y organizaciones, alcanzar los servicios digitales ofrecidos por la institución.
4. Organización de la institución: Contar con la estructura organizacional, roles, perfiles, competencias y valores requeridos para poder aplicar la interoperabilidad en la institución y la propuesta de valor definida.

Se elabora la siguiente herramienta, que sirve como guía para el desarrollo de su estrategia de interoperabilidad, tomando como base los 4 grandes aspectos institucionales establecidos en este CNTD:

Definición de estrategia de Interoperabilidad			
Aspectos	**¿Cumple?**		**Acción por realizar**
	Sí	**No**	
Propuesta de valor			
¿Se desarrolla una propuesta de valor de los servicios digitales que la institución ofrecerá a las personas usuarias, organizaciones y empresas?			
¿La propuesta puede ser incorporada en la Estrategia Institucional?			
¿La propuesta cuenta con un impacto positivo en el medio ambiente y es digitalmente inclusiva?			
¿Las empresas, personas usuarias y organizaciones tienen entendimiento y claridad de la propuesta de valor?			
Servicios digitales			
¿Se identificaron y definieron los servicios digitales que permiten alcanzar la propuesta de valor?			
Procesos y tecnologías de la información y comunicación			
¿Se identifican los procesos y tecnologías que permiten a las personas, empresas y organizaciones alcanzar los servicios digitales ofrecidos?			
Organización de la institución			

¿Se cuenta con la estructura organizacional, roles, perfiles, competencias y valores necesarios para poder aplicar la interoperabilidad y la propuesta de valor definido?			

Herramienta de interoperabilidad, 8. Elaboración propia.

Etapa 7 - Servicios de interoperabilidad

En esta etapa se presentan los servicios que deberían formar parte de cada institución para poder implementar a mediano y largo plazo el Marco de Interoperabilidad Nacional. El Equipo Ad Hoc Interno de Interoperabilidad debe aplicar una mirada holística de las cuatro dimensiones de la interoperabilidad, promover y garantizar que exista una definición clara de la dimensión, su responsabilidad en cada ámbito y la responsabilidad que tienen con cada institución con la que interoperen.

Para los servicios de interoperabilidad normativa/legal, se deben establecer acuerdos, alinear las normativa existentes y relacionadas con las instituciones que se encuentran por iniciar el proceso de interoperabilidad, logrando los acuerdos y consensos que permitan la implementación de los servicios bajo el marco normativo vigente y que la ley permita. Para esto contamos con la Herramienta de interoperabilidad 9, que se denominada “Herramienta de control de servicios de interoperabilidad normativa legal”:

Herramienta de control de servicios de interoperabilidad normativa legal				
Servicio	**Responsabilidad por cumplir**	**¿Cumple?**		**Acciones por realizar**
		Sí	**No**	
Alineamiento de las normativas/leyes intra- e interinstitucionales	Garantizar que las organizaciones que operan sobre la base de diferentes marcos jurídicos, políticas y estrategias puedan trabajar juntas			
	Identificar las leyes y normativas que regulan, restringen o posibilitan			

	el ofrecimiento de un servicio interoperado a la persona			
Establecimiento de acuerdos claros sobre cómo abordar las diferencias en la legislación	Establecer acuerdos claros sobre cómo abordar las diferencias en la legislación (incluida la opción de adoptar nueva legislación)			
	Coordinar con las contrapartes normativas/legales de las instituciones involucradas en el ofrecimiento de un servicio interoperado a la persona			

Herramienta de interoperabilidad, 9. Elaboración propia.

Para los servicios de interoperabilidad organizacional se debe tener claramente definida la relación entre los proveedores de servicios y los consumidores de datos o información en cada uno de los procesos para cada servicio que se haya definido para interoperar, sea para ofrecer o consumir datos o información. Se deben realizar los acuerdos necesarios para habilitar los servicios de interoperabilidad a nivel organizacional. Contamos con la Herramienta de interoperabilidad 10, que se denomina “Herramienta de control de servicios de interoperabilidad organizacional”:

Herramienta de control de servicios de interoperabilidad organizacional				
Servicio	**Responsabilidad por cumplir**	**¿Cumple?**		**Acciones por realizar**
		Si	**No**	

Alineamiento de los procesos institucionales	Entender globalmente (de extremo a extremo) los procesos institucionales asociados a servicios al ciudadano la función de las instituciones dentro de dichos procesos.			
	Participar activamente en el levantamiento, la especificación y el rediseño de los procesos involucrados en el ofrecimiento de un servicio interoperado a la persona.			
Estructura clara de la relación entre los proveedores de servicios y los consumidores	Estructurar claramente la relación entre los proveedores de servicios y los consumidores.			
	Participar activamente en la especificación del papel de la institución (proveedora o consumidora) en el ofrecimiento de un servicio interoperado a la persona.			

Contribución a la formalización de la asistencia mutua, la actuación conjunta y los procesos institucionales interconectados	Contribuir a formalizar la asistencia mutua, la actuación conjunta y los procesos institucionales interconectados (por ejemplo, mediante memorandos de entendimiento y acuerdos de prestación de servicios entre las instituciones participantes).			
	Establecer, en conjunto con las otras instituciones involucradas en un servicio interoperado, los acuerdos de asistencia y los niveles de servicios necesarios.			

Herramienta de interoperabilidad, 10. Elaboración propia.

Para los servicios de interoperabilidad semántica, tiene el propósito de contribuir en la formación, comprensión, tratamiento de los datos (respetando la normativa de protección de datos de las personas vigentes en el país y que se debe contemplar en los servicios de interoperabilidad legal/normativa) y la información asociada para interoperar, garantizando que el formato y el significado de la información que se intercambia se encuentra estandarizada con el formato de la fuente primaria y sea exacta. Se cuenta con la Herramienta de interoperabilidad 11, que se denomina “Herramienta de control de servicios de interoperabilidad semántica”:

Herramienta de control de servicios de interoperabilidad semántica				
Servicio	**Responsabilidad por cumplir**	**¿Cumple?**		**Acciones por realizar**
		Sí	**No**	
Contribución a la formación, la comprensión y el tratamiento de los datos y la información	Contribución a la formación, la comprensión y el tratamiento de los datos y la información.			

	Designar a las contrapartes de datos e información de la institución, que serán responsables de la interoperabilidad de los servicios		
Contribución para garantizar que el formato y el significado de la información intercambiada sean exactos	Contribuir a garantizar que el formato y el significado de la información intercambiada sean exactos, se comprendan y conserven en todos los intercambios entre las partes		
	Participar respecto del significado exacto de la información intercambiada por la institución con otras instituciones		
Establecimiento de normas y contribución a la creación de vocabularios y esquemas	Normar y contribuir a la creación de vocabularios y esquemas para describir los intercambios de datos.		
	Participar y sancionar respecto del significado exacto de la información intercambiada por la institución con otras Instituciones.		

Gestión para que exista una descripción del formato exacto de la información	Gestionar para que exista una descripción del formato exacto de la información que se va a intercambiar en términos de gramática y formato.		
	Participar y sancionar respecto del formato exacto de la información que se va a intercambiar en términos de gramática y formato.		
Garantía de que todas las partes que se comunican entiendan de la misma manera los elementos de datos	Garantizar que todas las partes que se comunican entiendan de la misma manera los elementos de datos que se intercambian.		
	Participar respecto del significado exacto de la Información intercambiada por la institución con otras instituciones		

Herramienta de interoperabilidad, 11. Elaboración propia.

Para los servicios de interoperabilidad técnica, se busca definir y promover las arquitecturas tecnológicas para la interoperabilidad de cada institución y para cada servicio que se defina o se desee consumir, los cuales han sido definidos mediante la gestión de catálogos de servicios, esquemas, metadatos, diccionarios de datos y la correcta administración, trazabilidad y monitoreo del servicio interoperado. Para esto se cuenta con la Herramienta de interoperabilidad 12, que se denomina “Herramienta de control de servicios de interoperabilidad técnica”:

Herramienta de control de servicios de interoperabilidad técnica				
Servicio	**Responsabilidad por cumplir**	**¿Cumple?**		**Acciones por realizar**
		SÍ	**No**	
Definición y promoción de arquitecturas tecnológicas para la interoperabilidad	Definir y promover arquitecturas tecnológicas abiertas y flexibles, contribuyendo en las especificaciones de interfaz, servicios de interconexión, servicios de integración de datos, presentación e intercambio de datos y protocolos de comunicación seguros.			
	Contribuir con la especificación, el diseño, las restricciones y las posibilidades de las arquitecturas de la institución con miras a su integración en la plataforma de interoperabilidad.			
Suministro y gestión de un catálogo de servicios	Proveer y gestionar un catálogo de servicios de interoperabilidad entre instituciones.			

	Publicar y mantener en el catálogo todos los servicios de interoperabilidad que estén bajo su administración y control (se incluye descripción, niveles de servicio comprometido, interfaces de programación de aplicaciones y documentación técnica para la implementación de estos servicios).			
Suministro y gestión de un catálogo de esquemas y metadatos	Proveer y gestionar un catálogo de esquemas y metadatos.			
	Publicar y mantener en el catálogo el listado de esquemas y metadatos utilizados en los servicios y documentos electrónicos.			
Suministro y gestión de un directorio de datos	Proveer y gestionar un directorio de datos.			
	Listado de datos disponibles a partir de los servicios de interoperabilidad publicados en el catálogo de servicios, donde se detalla la descripción y el responsable de cada dato.			
Suministro y administración de un gestor de convenios	Proveer y administrar un gestor de convenios (aplicación) global y específico entre instituciones.			

	Mantener actualizada la aplicación que facilita la tramitación de convenios electrónicos estándar, entre consumidor y proveedor de servicios de interoperabilidad, entregando los permisos y las credenciales de acceso para autorizar el suministro del servicio.			
	Proveer y administrar un registro de trazabilidad.			
Suministro y administración de un registro de trazabilidad	Mantener actualizado el registro resultante de cada servicio de interoperabilidad para que los actores involucrados conozcan y verifiquen las operaciones que se hayan realizado respecto de un determinado servicio interoperado.			
	Proveer y administrar un sistema de monitoreo.			
Suministro y administración de un sistema de monitoreo	Mantener actualizado el sistema de monitoreo que realiza consultas periódicas a todos los servicios de interoperabilidad definidos en el catálogo de servicios, a fin de identificar y notificar de manera oportuna y proactiva las fallas en el servicio.			

Suministro y administración de un gestor de autorizaciones	Proveer y administrar un gestor de autorizaciones que permita a las personas naturales autorizar o desautorizar el uso de sus datos personales, mediante el uso de su identidad digital.			
Identificación de los servicios adecuados para que se invoquen y organicen para prestar el servicio público	Garantizar que las necesidades se identifiquen y que los servicios adecuados se invoquen y organicen para prestar un servicio público.			
	Formalizar los servicios demandados por las personas y las interdependencias que estos tienen con otras instituciones.			
Suministro y gestión de un catálogo de fuentes de información y servicios internos de cada institución	Proveer y gestionar un catálogo de fuentes de información (aplicaciones) de cada institución.			
	Publicar y mantener en el catálogo el listado de sistemas y aplicaciones desde donde se obtienen los servicios y documentos electrónicos interoperables.			
Suministro y gestión de un catálogo de recursos reutilizables	Proveer y gestionar un catálogo de recursos reutilizables de interoperabilidad entre instituciones.			

	Publicar y mantener en el catálogo de recursos reutilizables los módulos, componentes y servicios que puedan reutilizar otras instituciones.			
Suministro y gestión de un catálogo de fuentes de información y servicios externos	Proveer y gestionar un catálogo de fuentes de información y servicios externos utilizados por cada institución.			
	Publicar y mantener el catálogo de fuentes de información y servicios externos, identificando el proveedor y documentando las características técnicas y el uso de estas fuentes.			
Suministro y administración de un mecanismo de seguridad y privacidad de acceso a la información	Proveer y administrar un mecanismo de seguridad y privacidad de acceso a la información interoperable.			
	Hacer uso de las funcionalidades y los ambientes del mecanismo de seguridad y privacidad de acceso a la información Interoperable.			

Herramienta de interoperabilidad, 12. Elaboración propia.

Etapa 8 - Procesos de interoperabilidad

En la presente etapa se definen los macroprocesos y los factores habilitantes para la implementación de la interoperabilidad. En su conjunto podemos identificarlos y colocar su relación con la Gobernanza de la Interoperabilidad representada por las cuatro dimensiones definidas en el Marco de Interoperabilidad Nacional (Organizacional, Legal/Normativa, Semántica y Técnica), de la siguiente manera:

Fuente: Cepal, 2021.

Habilitadores:

Para el desarrollo del Marco de Interoperabilidad Nacional se requieren diferentes habilitadores en los cuales cada institución debe trabajar y velar por su implementación, estos habilitadores son:

- Infraestructura y telecomunicaciones.
- Alfabetización digital del personal.
- Identidad digital, la implementación de métodos seguros de autenticación digital y los aspectos definidos en este tema dentro del CNTD.
- Ciberseguridad, que debe estar presente en todo el ciclo de identificación, definición, desarrollo e implementación para garantizar la seguridad de la información. Este CNTD define una serie de recomendaciones en el apartado de Seguridad Tecnológica.

Soporte a la interoperabilidad:

Parte de las labores del Equipo Ad Hoc Interno de Interoperabilidad es gestionar a nivel interno de la institución que se cuente con el soporte para la implementación del Marco de Interoperabilidad Nacional.

Los soportes institucionales requeridos que deben gestionarse propuestos son:

- Financiero contable para las implementaciones, sean internas o externas.
- Gestión de las personas y de los diferentes equipos de trabajo.

- Gestión de los diferentes contratos y de la normativa/legal existente y que se esté aplicando para cada servicio identificado.
- Gestión de las Tecnologías de Información y Comunicación.

Macroprocesos de gobernanza:

Las diferentes gobernanzas que forman parte del marco de interoperabilidad con sus macroprocesos que deben ser considerados y liderados por el Equipo Ad Hoc Interno de Interoperabilidad, los cuales son:

- Gobernanza estratégica de la interoperabilidad:
  - Planificación, control y gestión de la interoperabilidad.
  - Gestión y la arquitectura del Estado e institucional.
  - Gestión del conocimiento.
  - Evaluación del impacto público, a nivel de las personas, empresas privadas y organizaciones, así como dentro de la institución.
  - Gestión de la comunicación y la difusión de los servicios digitales desarrollados.
- Gobernanza de la interoperabilidad:
  - Se refiere a las cuatro dimensiones de la interoperabilidad:
    - Normativa/Legal.
    - Organizacional.
    - Semántica.
    - Técnica.
- Gobernanza de las personas:
- Gobernanza de los servicios públicos integrados:
  - Procesos para identificar las necesidades de las personas, empresas privadas y organizaciones.
  - Coordinar con el ente rector en Tecnología y Gobernanza Digital.
  - Buscar alternativas para complementar cada uno de los servicios identificados.
  - Garantizar que exista el soporte, mantenimiento, monitoreo y correctos funcionamientos de los componentes técnicos que permiten la interoperabilidad en la institución.

Etapa 9 - Implementación de la interoperabilidad

La etapa final se refiere a la implementación de la interoperabilidad, requiere fortalecer las etapas anteriores y realizar una correcta identificación de las diferentes iniciativas que se van a interoperar. Para lo cual se ha definido la Herramienta de interoperabilidad 13, denominada “Formulario de iniciativa de interoperabilidad institucional”.

Esta herramienta es una guía general para poder validar el Marco de Interoperabilidad Nacional con sus cuatro dimensiones para cada uno de los servicios que el Equipo Ad Hoc Interno de Interoperabilidad va identificando en su proceso de interoperabilidad:

Herramienta de iniciativa de interoperabilidad institucional			
Fecha de aplicación:			
Nombre de la iniciativa de interoperabilidad			
Breve descripción de la iniciativa			
Beneficios para las personas			
Instituciones que intervienen en la solución que se brinda al ciudadano			
Nivel de interoperabilidad	**Descripción**	**Referencia**	**Observaciones**

Normativo/Legal	Revisión de la legislación genérica del Estado y la específica de las instituciones involucradas en la solución que se brinda al ciudadano para detectar los obstáculos a la interoperabilidad, requerimientos contradictorios para procesos iguales o similares, seguridad y necesidad de protección de datos obsoletas, y demás. Debe valorarse la coherencia de la legislación, con vistas a garantizar la interoperabilidad.	Especificar las normas o leyes involucradas.	Indicar su cumplimiento o necesidad de cambio.
Organizacional	Las instituciones que contribuyen en la prestación del servicio deben entender globalmente (de extremo a extremo) los procesos institucionales involucrados y su función en dichos procesos.	Identificar instituciones y procesos involucrados.	Indicar comprensión común y aceptación de la operación interinstitucional.

	Especificar instrumentos que permitan formalizar la asistencia mutua, la actuación conjunta y los procesos institucionales interconectados; indicar, por ejemplo, los memorandos de entendimiento y los acuerdos de nivel prestación de servicios (APS), entre las instituciones participantes.		
Semántico	Garantizar que el formato y el significado exacto de la información intercambiada se comprendan y conserven en todos los intercambios entre las partes, es decir, “que lo que se transmite sea lo que se entiende”.	Semántica y sintáctica.	Detallar los conceptos involucrados en el servicio y su comprensión común en su significado y sintaxis.
	Cumplimiento de estándares que permitan la interpretación correcta de datos provenientes de fuentes no relacionadas.		

		El aspecto semántico se refiere al significado de los elementos de datos y la relación entre ellos. Incluye la creación de vocabularios y esquemas para describir los intercambios de datos y garantiza que todas las partes que se comunican entienden de la misma manera los elementos de datos.	
		El aspecto sintáctico se refiere a la descripción del formato exacto de la información que se va a intercambiar en términos de gramática y formato.	
Técnico	Identificar detalladamente las especificaciones de interfaz, servicios de interconexión (servicios web, microservicios u otro), servicios de integración de datos y protocolos de comunicación utilizados.	Detallar servicios utilizados	Especificar técnicamente cada servicio

Herramienta de interoperabilidad, 13. Elaboración propia.

En la siguiente actualización se estarán agregando herramientas adicionales que complementan este formulario de iniciativas detallando cada una de las dimensiones y la identificación de las fuentes únicas de información con sus respectivos formatos.

CAPÍTULO 6:

NEUTRALIDAD TECNOLÓGICA

EQUIPO DE TRABAJO

Integrante	Institución
Roberto Lemaitre	MICITT
Mauricio Oviedo	SOCIUM
Glenn Peace	NIC-CR

INTRODUCCIÓN AL TEMA

Las soluciones tecnológicas aumentan día con día, por lo que una incorporación correcta y oportuna de las tecnologías con que contamos en nuestro país permiten optimizar recursos para las distintas instituciones del Estado. Sin embargo, cada una de estas instituciones debe tener la libertad de implementar, la o las opciones que mejor le convenga o se adecuen a sus necesidades y requerimientos, precisamente a eso se refiere la neutralidad tecnológica. De esta forma se busca que, a pesar de que las instituciones tengan fines diferentes, puedan brindar opciones tecnológicas de calidad a sus usuarios, que permitan a la Administración no condicionar la tecnología que elijan los ciudadanos para relacionarse con ella, ni tampoco condicionar la tecnología que la misma deba usar en sus proyectos tecnológicos.

PRINCIPIOS

Independencia tecnológica: Se refiere al lograr asegurar la no dependencia de un único proveedor.

Interoperabilidad: La interoperabilidad se configura como un medio para la construcción de un Estado más eficiente, más transparente y participativo, y que presta mejores servicios a los ciudadanos, todo lo anterior, mediante el mejor aprovechamiento de las Tecnologías de la Información y las Comunicaciones. Se entiende por interoperabilidad la habilidad de interactuar cooperar y transferir datos de manera uniforme y eficiente entre varias organizaciones y sistemas sin importar su origen o proveedor, fijando las normas, las políticas y los estándares necesarios para la consecución de esos objetivos (Promoción del Modelo de Interoperabilidad en el Sector Público, 2010).

Libre concurrencia: De acuerdo con la Resolución Nº00998 (Sala Constitucional, 1998), tiene por objeto afianzar la posibilidad de oposición y competencia entre los oferentes dentro de las prerrogativas de la libertad de empresa, según se regula en el artículo 46 de la Constitución Política. Dicho artículo está destinado a promover y estimular el mercado competitivo a través de la participación del mayor número de oferentes para que la Administración pueda contar con una amplia y variada gama de ofertas, de modo que pueda seleccionar la que ofrece las mejores condiciones.

Libre competencia: Se refiere al derecho de igual participación. Al respecto, la Ley de Contratación Administrativa (1995) señala en su artículo 5 que, en los procedimientos de contratación administrativa, se respetará la igualdad de participación de todos los oferentes potenciales. Además, indica que sus propios reglamentos no podrán incluir ninguna regulación que impida la libre competencia entre los oferentes potenciales. También agrega que los carteles y pliegos de condiciones no podrán disponer formas de pago ni contener ninguna regulación que otorgue a los oferentes nacionales un trato menos ventajoso que el otorgado a los oferentes extranjeros.

POLÍTICAS GENERALES

Todo proceso de contratación administrativa del Estado deberá tomar en cuenta los principios Rectores de la Contratación Administrativa Electrónica y Principio de Neutralidad Tecnológica, de acuerdo con la normativa atinente en su última versión, por ejemplo, al momento de la publicación del presente código, se tiene: Ley General de Contratación Pública Nº 9986 y el Reglamento a la Ley General de Contratación Pública Nº 43808-H, sin embargo se reitera la obligación de la utilización de las versiones más actualizadas y en vigencia.

A efecto de mantener la libertad de competencia e igualdad de participación en la contratación administrativa, es importante que la Administración respete el principio de neutralidad tecnológica. Podría vulnerarse ese principio en la medida en que el Estado exija especificaciones que tiendan a favorecer a una determinada tecnología.

Las decisiones administrativas en orden a la prestación de servicios en forma electrónica deben tomar en cuenta las distintas alternativas de tecnologías empleadas, de manera tal que se garantice la más amplia cobertura y sobre todo el acceso universal, equitativo y asequible a dichos servicios por parte de los distintos administrados.

POLÍTICAS ESPECÍFICAS

En la medida de las posibilidades, debe buscarse que un determinado bien o servicio se pueda obtener de empresas distintas y con distintas plataformas, fomentando la libre competencia y que se permita seleccionar la mejor opción que se adapte a las necesidades de la institución.

Se debe desglosar el proyecto en los elementos mínimos de software y hardware de forma que permita analizar las distintas alternativas en cada componente.

Se debe procurar que todos los servicios tecnológicos estén disponibles para los usuarios independientemente de la plataforma o sistema operativo que utilicen.

Es deseable la utilización de formatos estándares para la recolección y el almacenamiento de información en bases de datos.

Debe buscarse que el hardware que se adquiera pueda funcionar con varias plataformas tecnológicas o sistemas operativos.

Deben aplicarse los principios anteriormente detallados para elegir las tecnologías, así como la normativa nacional correspondiente que garantice la pluralidad tecnológica y la libre competencia.

Se debe considerar emplear Estándares abiertos o de uso generalizado (v. gr. software libre o de código abierto) en los desarrollos, entendiendo Estándar abierto como aquel que reúna las condiciones de:

- Es público y su utilización está disponible de manera gratuita o a un coste que no suponga una dificultad de acceso,
- Su uso y aplicación no está condicionado al pago de un derecho de propiedad intelectual o industrial.

Se elabora la siguiente herramienta, que contiene las principales recomendaciones para la contratación de bienes o servicio digitales:

Herramienta de verificación de Neutralidad Tecnológica			
Recomendaciones para la contratación de bienes y/o servicios digitales	**¿Cumple?**		**Observaciones**
	Sí	**No**	
Fomentar la libre competencia en la contratación de bienes y/o servicios a empresas.			
Seleccionar las mejores opciones de bienes y/o servicios que se adapten a las necesidades de la institución			
Desglosar el proyecto en los elementos mínimos de software y hardware para analizar las alternativas de cada componente			
Disponer los servicios tecnológicos para los usuarios independientemente de la plataforma o sistema operativo utilizado			
Utilizar formatos estándares para la recolección y almacenamiento de información en bases de datos			
Lograr que el hardware adquirido pueda funcionar con varias plataformas tecnológicas o sistemas operativos			
Aplicar la normativa nacional correspondiente, para garantizar pluralidad tecnológica			
Emplear estándares abiertos o de uso generalizado; abiertos al público, gratuitos, de fácil acceso			

Herramienta de Neutralidad Tecnológica, 1. Elaboración propia.

CAPÍTULO 7:

INTELIGENCIA ARTIFICIAL

EQUIPO DE TRABAJO

Integrante	Institución
Marlon Ávalos Elizondo	MICITT
Margarita Vargas Ramos	MICITT
Orlando Vega Quesada	MICITT
Antonette Williams Barnett	MICITT

INTRODUCCIÓN AL TEMA

El presente capítulo tiene como objetivo proporcionar un marco comprehensivo para la adopción y gobernanza de la inteligencia artificial en el país. Estos lineamientos han sido desarrollados en concordancia con la Estrategia Nacional de Inteligencia Artificial (ENIA) y se basan en principios fundamentales como la paz, la dignidad humana, la transparencia, la equidad, la responsabilidad, la sostenibilidad y la ciberseguridad.

La ENIA 2024-2027 establece las bases para la integración de la IA en diversos sectores, promoviendo su desarrollo de manera ética y responsable. Los lineamientos presentados en este documento están diseñados para guiar a los diferentes actores involucrados en el ecosistema de IA, incluyendo entidades gubernamentales, empresas, desarrolladores y usuarios finales.

Estos lineamientos abarcan múltiples aspectos críticos para la implementación de la IA, tales como la gobernanza, los derechos de las personas usuarias, la gestión de riesgos, la seguridad y protección, la operación y el mantenimiento de los sistemas, los estándares técnicos, la sostenibilidad y el diseño centrado en las personas. Cada sección proporciona directrices específicas y acciones recomendadas para asegurar que la IA se desarrolle y utilice de manera que beneficie a toda la sociedad costarricense.

Para efecto de estos lineamientos, se adopta la definición de sistemas de IA establecido por la OCDE (2023) que indica que:

“Un sistema de IA es un sistema basado en una máquina que, para objetivos explícitos o implícitos, infiere, a partir de la entrada que recibe, cómo generar resultados como

predicciones, contenido, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales. Los diferentes sistemas de IA varían en sus niveles de autonomía y adaptabilidad después del despliegue".

Con relación al ciclo de vida de un sistema que utiliza IA, se adopta la definición del ciclo de vida de sistemas de IA establecido por la OCDE (2023) que indica que:

"Las fases del ciclo de vida del sistema de IA implican: i) "diseño, datos y modelos"; que es una secuencia dependiente del contexto que abarca la planificación y el diseño, la recopilación y el procesamiento de datos, así como la construcción de modelos; ii) "verificación y validación"; iii) "despliegue"; y iv) "operación y seguimiento". Estas fases suelen tener lugar de forma iterativa y no necesariamente secuenciales. La decisión de retirar de funcionamiento un sistema de IA puede ocurrir en cualquier momento durante la fase de operación y monitoreo."

PRINCIPIOS

Los siguientes principios se establecen en la ENIA, para efectos de este documento se muestran de manera resumida.

- **Paz y dignidad humana:** La ENIA prioriza la paz, la dignidad humana y el bienestar colectivo en el desarrollo y aplicación de la IA, desincentivando usos militares y promoviendo la inclusión y la equidad.
- **Supervisión humana**: El principio de supervisión humana en la IA garantiza que el control final y la responsabilidad ética y jurídica recaigan en los seres humanos, evitando que decisiones críticas se deleguen por completo a la IA. Este principio asegura la intervención humana continua, promoviendo la transparencia y la revisión para el uso ético y responsable de la tecnología.
- **Transparencia y explicabilidad:** La transparencia en la IA requiere que los desarrolladores proporcionen información clara sobre sus capacidades y limitaciones, permitiendo a los usuarios entender e interactuar conscientemente con estos sistemas. Esto incluye detallar las fuentes de datos y los procesos de decisión, garantizando que los resultados automatizados puedan ser comprendidos y cuestionados. Las decisiones automatizadas en el sector público deben ser explicadas claramente, y en el sector privado, las empresas deben informar a sus clientes sobre el uso de IA, proporcionando opciones para evitar ser afectados por estos sistemas.

- **Equidad y no discriminación:** Los sistemas de IA deben promover la inclusión y evitar la discriminación, garantizando accesibilidad para todos los sectores de la sociedad y adaptándose cultural y lingüísticamente. Esto requiere minimizar sesgos en algoritmos mediante auditorías y promover la diversidad en su desarrollo. La equidad en la IA incluye programas de capacitación para grupos subrepresentados y políticas públicas que fomenten la igualdad de acceso a la educación en IA. Este principio destaca la importancia de que la IA fomente la inclusión, diversidad y respeto a los derechos humanos .

- **Responsabilidad:** El principio de responsabilidad en la IA requiere que los actores asuman la responsabilidad ética y jurídica de sus operaciones, asegurando una rendición de cuentas clara. Incluye la supervisión y capacidad de intervención en sistemas automáticos, con mecanismos robustos de evaluación y auditoría para la transparencia y trazabilidad de decisiones. La colaboración entre sectores es esencial para una gobernanza inclusiva y equitativa, adaptada a cambios tecnológicos y sociales, protegiendo derechos y fomentando la confianza.

- **Sostenibilidad y bienestar:** El principio de sostenibilidad y bienestar en la IA promueve el desarrollo sostenible en sus dimensiones social, económica, ambiental y cultural. Exige evaluar continuamente los impactos de la IA en la sociedad, vida animal y ambiente, asegurando que su uso contribuya a la equidad, inclusión y protección del entorno. Los responsables deben comprometerse con una gestión responsable que armonice la innovación tecnológica con la ética ambiental y social, respetando y protegiendo la vida animal y los ecosistemas.

- **Seguridad, ciberseguridad y protección de la información:** La IA debe desarrollarse y aplicarse de manera segura que proteja a los ciudadanos y al país, identificando y mitigando riesgos para garantizar la seguridad y confianza. Es fundamental que los sistemas de IA sean robustos, seguros y confiables durante todo su ciclo de vida, con mecanismos para supervisión, intervención y desactivación segura en caso de comportamientos no deseados. La seguridad y ciberseguridad implican la creación de sistemas resilientes que resistan ataques cibernéticos y fallos técnicos, adhiriéndose a normativas de seguridad y protección de datos.

POLÍTICAS GENERALES

Para efectos de estos lineamientos se utiliza como marco general la legislación y normativa

nacional atinente, entre las que destacan:

Constitución Política de la República de Costa Rica.

La Constitución Política, como norma legal máxima que define el ordenamiento jurídico de Costa Rica, indica en su artículo 24 que:

> "(...) *Toda persona tiene el derecho fundamental al acceso a las telecomunicaciones, y tecnologías de la información y comunicaciones en todo el territorio nacional. El Estado garantizará, protegerá y preservará este derecho."*

Por su parte el artículo 27 indica que:

> *"Se garantiza la libertad de petición, en forma individual o colectiva, ante cualquier funcionario público o entidad oficial, y el derecho a obtener pronta resolución."*

Así como en su artículo 46 establece que:

> *"(...) Los consumidores y usuarios tienen derecho a la protección de su salud, ambiente, seguridad e intereses económicos; a recibir información adecuada y veraz; a la libertad de elección, y a un trato equitativo. El Estado apoyará los organismos que ellos constituyan para la defensa de sus derechos (...)"*

Ley General de la Administración Pública

La Ley General de la Administración Pública" en su artículo 4°, Ley N° 6227, señala que:

> *"La actividad de los entes públicos deberá estar sujeta en su conjunto a los principios fundamentales del servicio público, para asegurar su continuidad, su eficiencia, su adaptación a todo cambio en el régimen legal o en la necesidad social que satisfacen y la igualdad en el trato de los destinatarios, usuarios o beneficiarios."*

Ley de Promoción del Desarrollo Científico y Tecnológico

La Ley N°7169 denominada "Ley de Promoción del Desarrollo Científico y Tecnológico y creación del MYCIT" en su artículo 3º, inciso b), establece que uno de los objetivos específicos para el desarrollo científico y tecnológico es:

> *"Apoyar la actividad científica, tecnológica y de innovación que realice cualquier entidad privada o pública, nacional o extranjera, que contribuya a la productividad, al intercambio científico y tecnológico con otros países, o que esté vinculada con los objetivos del desarrollo nacional. Asimismo, generar las políticas públicas que garanticen el derecho de los habitantes a obtener servicios de telecomunicaciones, así como asegurar la*

aplicación de los principios de universalidad y solidaridad del servicio de telecomunicaciones y fortalecer los mecanismos de universalidad y solidaridad de las telecomunicaciones, garantizando el acceso a los habitantes que lo requieran".

El artículo 4 de la misma ley indica:

"(…) a) Velar por que la ciencia, la tecnología y la innovación estén al servicio de los costarricenses, les provea bienestar y les permita aumentar el conocimiento de sí mismos, de la naturaleza y de la sociedad.

(…) c) Proporcionar los instrumentos específicos para incentivar y estimular las investigaciones, la transferencia del conocimiento, la ciencia, la tecnología e innovación, como condiciones fundamentales del desarrollo económico, social y productivo y como elementos de la cultura universal.

(…) d) orientar sobre la ejecución y el seguimiento de las políticas sobre ciencia, tecnología

(...) i) Impulsar la incorporación selectiva de la tecnología moderna en la Administración Pública, a fin de agilizar y actualizar, permanentemente, los servicios públicos, en el marco de una reforma administrativa, para lograr la modernización del aparato estatal costarricense, en procura de mejores niveles de eficiencia (...)".

Ley de Protección de la Persona frente al tratamiento de sus datos personales

La Ley de Protección de la Persona frente al tratamiento de sus datos personales, Ley N°8968, establece en su artículo 4 que:

"Toda persona tiene derecho a la autodeterminación informativa, la cual abarca el conjunto de principios y garantías relativas al legítimo tratamiento de sus datos personales reconocidos en esta sección.

Se reconoce también la autodeterminación informativa como un derecho fundamental, con el objeto de controlar el flujo de informaciones que conciernen a cada persona, derivado del derecho a la privacidad, evitando que se propicien acciones discriminatorias."

Plan Nacional de Ciencia, Tecnología e Innovación 2022-2027

El Plan Nacional de Ciencia, Tecnología e Innovación (2022-2027) oficializado por medio del Decreto Ejecutivo N° 43474 define cinco áreas temáticas transversales a las intervenciones públicas que conforman las áreas estratégicas, relacionadas a industrias, subsectores e

instituciones que tienen un papel fundamental en el presente y futuro del sector CTI en Costa Rica, dentro de las áreas incluidas se define a la IA como área temática transversal debido a que según la sección 2.4 de dicho plan establece que:

> *"(...) la inteligencia artificial (IA) se ha posicionado como un instrumento transversal en muchas industrias a nivel mundial, entre ellas las de salud, manufactura, aeroespacial, bancaria y de ventas al por menor; así como a otras tareas y procesos dentro de las industrias, como mercadeo, desarrollo de nuevos productos y manejo de cadenas de suministros. Producto de esta transversalidad es que serán cada vez más las ocupaciones que requerirán competencias relacionadas con IA en nuestro país".*

POLÍTICAS ESPECÍFICAS

A continuación, se presentan los distintos lineamientos específicos, entendiendo que algunos de ellos podrían ser necesarios mientras que otros no, según el análisis de aplicabilidad que se realice durante la evaluación preliminar del proyecto. Cabe destacar que la implementación de estos lineamientos no se limita exclusivamente al alcance del proyecto, sino que deben ser gestionados a nivel operativo del producto y/o servicio implementado, asegurando su sostenibilidad en el tiempo de vida del mismo de manera segura.

A NIVEL DE GOBERNANZA Y ÉTICA

Se deben establecer políticas, estructuras y procesos para la supervisión, gestión responsable y ética de los sistemas de IA, asegurando su alineación con principios éticos y valores sociales.

Gobernanza de la IA en las instituciones: Establecer políticas, estructuras y procesos para la supervisión y gestión responsable de los sistemas de IA dentro de las instituciones.

1. Las entidades deben desarrollar políticas claras y comprensivas para la gobernanza de los sistemas y plataformas basadas en IA, asegurando su alineación con principios éticos definidos en ENIA, seguros y regulatorios mediante la colaboración con comités de tecnologías de información institucionales o unidades pertinentes.
    - Instrumentos de referencia: ISO/IEC 38507:2022, NIST AI 100-1 AI
2. Para la gestión de gobernanza de la IA se debe asegurar la supervisión adecuada de los sistemas de IA, por medio de metodologías de control, aplicadas por los comités de

tecnología de información, o en su defecto unidades pertinentes, presentes en las instituciones y requeridos mediante este Código.

- Instrumentos de referencia: ISO 42001:2023

3. Se debe asegurar la transparencia en todos los aspectos del desarrollo, implementación y uso de sistemas de IA, proporcionando información clara y accesible a todas las partes interesadas mediante la publicación de reportes y documentos explicativos; al menos una publicación anualmente, salvo prohibición legal expresa.

   - Instrumentos de referencia: ISO/IEC DIS 12792

4. Se deben desarrollar programas de capacitación que cubran aspectos clave de la gobernanza de IA, incluyendo ética, seguridad, normativa y supervisión, mediante actividades de formación continua dirigida al personal a cargo de la administración y uso de los sistemas.

   - Instrumentos de referencia: N/A

5. Se deben implementar mecanismos de supervisión, seguimiento y auditoría continua, alineados con los estándares internacionales, para asegurar el cumplimiento de las políticas de gobernanza y la identificación oportuna de problemas y/o vulnerabilidades, utilizando herramientas de monitoreo y auditorías periódicas. Deberá ser implementada por las estructuras internas atinentes.

   - Instrumentos de referencia: ISO/IEC DIS 42006

6. Se deben establecer procedimientos claros para la gestión de incidentes relacionados con los sistemas de IA, asegurando una respuesta rápida y efectiva a cualquier problema que surja, mediante la creación de protocolos de atención de emergencia y actuación de los equipos de respuesta. Según lo establecido en este Código en lo que respecta a normas de seguridad y similares.

   - Instrumentos de referencia: ISO IEC 20000; ISO IEC 22301; ISO/IEC 23894:2023; ISO 27000; NIST CSF; NIST AI 600-1

Ética en los sistemas de IA en las instituciones: Las entidades deben asegurar que los recursos públicos destinados a sistemas de IA se utilicen conforme a los más estrictos criterios éticos, priorizando siempre el interés público y el bienestar común.

1. Las entidades deben asegurar una adecuada gobernanza, integridad, calidad y representatividad de los datos utilizados en la IA, evitando el uso de los sistemas o datos

para manipular e influir en la percepción de personas o grupos, afectando su capacidad para tomar decisiones informadas. Para lo cual se deberán realizar auditorías periódicas del sistema y los datos utilizados.

2. Los sistemas de IA no deben ser utilizados para potenciar y/o profundizar condiciones de vulnerabilidades de personas o grupos, incluyendo factores como género, orientación sexual, edad, etnia, discapacidad o condiciones socioeconómicas, para influir significativamente su comportamiento, ni para fomentar sesgos de ningún tipo en la toma de decisiones.
    - Instrumentos de referencia: ISO/IEC TR 24368:2022
3. Las entidades deben evitar la utilización de sistemas de IA para la evaluación o clasificación de personas físicas o grupos de personas durante un determinado período de tiempo en función de su comportamiento social o de sus características personales conocidas, deducidas o previstas.
    - Instrumentos de referencia: ISO/IEC TR 24368:2022
4. Las decisiones críticas no deben ser tomadas de manera autónoma por sistemas de IA sin supervisión y validación humana calificada. Para lo cual se deberán establecer protocolos rigurosos necesarios de supervisión humana en todas las decisiones críticas para prevenir errores que puedan afectar la vida o los derechos fundamentales de las personas.
    - Instrumentos de referencia: ISO/IEC AWI 42105
5. Los sistemas de seguridad autónomos que utilicen IA no deben operar sin intervención humana, por lo que deben de contar con esta funcionalidad provista por el fabricante, en cumplimiento con las normativas nacionales e internacionales sobre armamento y seguridad nacional, para lo cual se deberá garantizar que siempre haya supervisión humana sobre cualquier acción llevada a cabo por sistemas de esta índole.
6. En los servicios esenciales, así como los de salud, educación, financieros, otorgamiento de beneficios, seguros y de reclutamiento, los sistemas de IA deben ser diseñados para evitar cualquier forma de discriminación sistémica, incluso inadvertida. Para lo cual se deberán realizar evaluaciones de impacto y ajustes continuos para asegurar la inclusión y equidad en estos sectores.
    - Instrumento de referencia: ISO/IEC TR 24368:2022
7. Las entidades deben garantizar que los sistemas que utilizan IA no deben ser utilizados para tener ningún tipo de incidencia en las emociones y comportamientos de las personas

usuarias.

Derechos de las personas usuarias: Se deben proteger los derechos de las personas usuarias, garantizando la transparencia, privacidad y posibilidad de entendimiento y control sobre los sistemas de IA que los afectan.

1. Las personas tienen derecho a saber cuándo interactúan con un sistema de IA en la prestación de servicios. Para ello, las entidades deben garantizar que dichos sistemas indiquen claramente que se está utilizando Inteligencia Artificial.

2. Las personas usuarias, deben ser informadas cuando están frente a un contenido generado por IA, ya sea digital o impreso, mediante la etiqueta "Generado con Inteligencia Artificial". La etiqueta deberá adaptarse a las necesidades de accesibilidad de las personas.

3. Las entidades deben velar que se implementen directrices y políticas de privacidad de datos que sean accesibles y fáciles de entender, adaptadas a las necesidades de los grupos etarios y que se explique claramente cómo se tratan, procesan y utilizan los datos personales de las personas usuarias.

4. Las personas usuarias deben proporcionar su consentimiento explícito e informado para el debido tratamiento de sus datos personales, para lo cual se deben implementar mecanismos fáciles y comprensibles para otorgar o revocar el consentimiento.

5. Se debe asegurar la transparencia de los sistemas de IA, incluyendo la toma de decisiones autónomas, proporcionando explicaciones comprensibles sobre cómo y por qué se toman estas decisiones.

    - Instrumento de referencia: ISO/IEC DIS 12792

6. Las personas usuarias tienen derecho a solicitar la rectificación, modificación o supresión de sus datos personales. Las entidades deben establecer procesos claros y eficientes para estas acciones, alineados con la Ley de Protección de Datos Personales, Ley N° 8968 y su reglamento.

7. Se debe velar que, en la interacción con sistemas de IA, la persona usuaria reciba un trato justo y no discriminatorio, revisando y ajustando periódicamente los modelos y algoritmos para asegurar la equidad en sus decisiones.

    - Instrumento de referencia: ISO/IEC TR 24368:2022

8. Las explicaciones sobre las decisiones autónomas de los sistemas de IA que afecten a las personas usuarias deben ser proporcionadas en un lenguaje comprensible, accesible y

adecuado para todas las personas.

- Instrumento de referencia: ISO/IEC 5339:2024

9. Se deben implementar las medidas de seguridad necesarias para proteger los datos personales integrados en sistemas de IA, contra accesos no autorizados, alteraciones, divulgaciones o destrucciones, tomando como referencia lo indicado en el capítulo 3 de este código relacionado con la Seguridad Tecnológica, Seguridad de la Información y Ciberseguridad.

Sesgo y equidad: Se deben implementar medidas para identificar, mitigar y prevenir sesgos en los sistemas de IA, asegurando un tratamiento justo y equitativo para todas las personas usuarias.

1. Las entidades deben implementar procesos para identificar, medir y mitigar sesgos en los sistemas de IA utilizados. Para ello, se deben establecer procedimientos que incluyan la revisión periódica de datos y modelos, alineados con estándares internacionales que permitan la identificación y corrección de sesgos.

   - Instrumentos de referencia: ISO/IEC DTS 12791.2; ISO/IEC TR 24027:2021

2. Se debe garantizar, la transparencia en la recolección, procesamiento y uso de datos, asegurando que los conjuntos de datos sean representativos y no estén sesgados. Para lograrlo, se debe realizar revisiones periódicas y documentar cualquier ajuste realizado.

   - Instrumentos de referencia: ISO/IEC 5339:2024

3. Las entidades que desarrollen o adquieran sistemas de IA deben asegurar que los modelos promuevan la equidad, evitando perpetuar o amplificar sesgos existentes. Esto se logra mediante pruebas exhaustivas antes del despliegue y el uso de técnicas o estándares generalmente aceptadas en la industria para ajustar los modelos. Esto debe quedar debidamente documentado.

   - Instrumentos de referencia: ISO/IEC TR 24368:2022

4. Se debe promover la evaluación de sistemas de IA desde la perspectiva de las personas usuarias que incluya a los diversos grupos beneficiarios de los servicios prestados, así también, desde la perspectiva técnica, incluyendo actores acreditados o certificados en IA.

   - Instrumentos de referencia: ISO/IEC TR 24368:2022

Explicabilidad e interpretabilidad. Las entidades deben garantizar que los sistemas de IA puedan proporcionar explicaciones claras y comprensibles sobre su funcionamiento y decisiones.

1. Las entidades deben asegurar que las personas usuarias tengan el derecho de recibir explicaciones claras y comprensibles sobre las decisiones automatizadas que les afecten significativamente.

2. Las entidades que desarrollen o implementen sistemas de IA deben mantener una documentación exhaustiva y accesible que explique el funcionamiento de los algoritmos y modelos de IA, los datos utilizados y los procesos de toma de decisiones. Para este lineamiento se recomienda, pero no se limita, incluir en la documentación, manuales de usuario, registro de cambios, diagramas de flujo, ejemplos de decisiones tomadas, glosarios de términos técnicos y cualquier otro instrumento que facilite comprender el funcionamiento del sistema de IA.

3. Las entidades deben implementar procesos de revisión y supervisión humana para monitorear y ajustar las decisiones automatizadas, asegurando que las explicaciones proporcionadas sean precisas y comprensibles. Para lo cual se debe destinar recurso humano calificado para la supervisión regular de las decisiones automatizadas.

    - Instrumentos de referencia: ISO/IEC DIS 42006

4. Las entidades deben informar a las personas usuarias sobre la fuente y los datos utilizados por los sistemas de IA y cómo estos datos influyen en las decisiones automatizadas.

5. Las entidades deben promover el uso de modelos interpretables y desarrollar herramientas de visualización; tomando en cuenta aspectos de accesibilidad, para que las personas usuarias de manera intuitiva, clara y comprensible entiendan las decisiones de IA.

Responsabilidad: Se deben establecer mecanismos de rendición de cuentas para asegurar que las entidades sean responsables de las decisiones y resultados de los sistemas de IA.

1. Las entidades deben establecer protocolos y/o mecanismos claros de rendición de cuentas para todos los procesos relacionados con el desarrollo y uso de sistemas de IA, documentando, reportando y revisando las decisiones automatizadas y los procesos algorítmicos, alineando estos mecanismos con estándares internacionales y las Normas de Control Interno para el Sector Público.(N-2-2009-CO-DFOE)

    - Instrumentos de referencia: ISO/IEC 42001:2023; ISO/IEC 38507:2022

2. Se debe revisar y ajustar, de forma continua, los sistemas de IA por equipos calificados, estableciendo procedimientos de revisión regular para evaluar la efectividad, la precisión y responsabilidad de las decisiones automatizadas.

    - Instrumentos de referencia: ISO/IEC 42001:2023; ISO/IEC 38507:2022; ISO/IEC DIS 42005

3. Las entidades deben asegurar la implementación transparente en todas las fases del desarrollo y uso de sistemas de IA, proporcionando información detallada sobre los algoritmos, modelos, fuentes de datos y metadatos utilizados.

    - Instrumentos de referencia: ISO/IEC DIS 12792

4. Se deben establecer procedimientos claros para la corrección de errores y la rectificación de impactos negativos causados por decisiones automatizadas, desarrollando un plan de respuesta a incidentes. Se debe considerar lo establecido sobre la gestión de cambios contenida en este código.

    - Instrumentos de referencia: ISO/IEC 22301; ISO/IEC 23894:2023; ISO/IEC TR 24028:2020; NIST 800-61; ISO 27035

A NIVEL DE GESTIÓN DE RIESGOS

Se deben identificar, evaluar y mitigar riesgos asociados con el desarrollo y uso de sistemas de IA a lo largo de su ciclo de vida, asegurando la seguridad y fiabilidad.

Identificación del riesgo en el ciclo de vida de los sistemas que utilizan IA: Se deben identificar y evaluar riesgos potenciales en todas las fases del ciclo de vida de los sistemas de IA.

1. Se debe establecer un proceso sistemático y continuo para identificar riesgos potenciales en todas las fases del ciclo de vida de los sistemas de IA, involucrando a todas las partes interesadas y utilizando herramientas y metodologías apegadas a estándares internacionales. Este proceso debe ser documentado y revisado periódicamente para asegurar su efectividad y relevancia.

    - Instrumentos de referencia: NIST-AI-600-1; ISO/IEC 5338:2023; ISO/IEC 23894:2023

2. Se debe realizar una identificación de riesgos en todas las fases del ciclo de vida de los sistemas de IA, considerando riesgos técnicos, éticos, legales, de privacidad, seguridad, reputacionales operacionales, reputacionales, lo cual debe estar debidamente documentado.

- Instrumentos de referencia: NIST-AI-600-1; ISO/IEC 5338:2023; ISO/IEC 23894:2023

3. Las entidades deben realizar una evaluación detallada para determinar la probabilidad y el impacto de cada riesgo identificado, utilizando metodologías cuantitativas y cualitativas como, por ejemplo: el análisis de Fortalezas, Oportunidades, Debilidades y Amenazas (FODA), el Análisis de Fallas y Efectos (FMEA, por sus siglas en inglés) y análisis Montecarlo. Esta evaluación debe ser documentada y actualizada regularmente.

   - Instrumentos de referencia: NIST-AI-600-1; ISO/IEC 5338:2023; ISO/IEC 23894:2023

4. Los riesgos identificados deben clasificarse y priorizarse en función de su probabilidad e impacto, utilizando una matriz de riesgos u otra herramienta de priorización (podrá utilizarse la del Sistema de Valoración de Riesgos Institucional SEVRI), asegurando que se abordan primero los riesgos más críticos.

   - Instrumentos de referencia: NIST-AI-600-1; ISO/IEC 5338:2023; ISO/IEC 23894:2023

5. Se deben desarrollar e implementar estrategias y controles específicos para mitigar los riesgos identificados, alineados con las mejores prácticas de la industria, e integrados al Sistema de Valoración de Riesgos Institucional (SEVRI) o ISO 31000.

6. Se debe establecer un sistema de monitoreo periódico para detectar y evaluar cambios en el perfil de riesgos de los sistemas de IA, utilizando herramientas y tecnologías que permitan la detección temprana y proporcionar alertas en tiempo real.

   - Instrumentos de referencia: NIST-AI-600-1; ISO/IEC 5338:2023; ISO/IEC 23894:2023

7. Se deben documentar todos los procesos de identificación, evaluación, mitigación y monitoreo de riesgos, manteniendo un registro detallado y de fácil acceso a todas las partes (personas beneficiarias, entidades o desarrolladores). Esto debe ser revisado y actualizado regularmente.

   - Instrumentos de referencia: NIST-AI-600-1; ISO/IEC 5338:2023; ISO/IEC 23894:2023

8. Se deben proporcionar informes periódicos a la alta dirección y otras partes interesadas sobre el estado de los riesgos y las medidas de mitigación adoptadas, facilitando la toma de decisiones informada y asegurando la transparencia y responsabilidad en la gestión de riesgos.

   - Instrumentos de referencia: NIST-AI-600-1; ISO/IEC 5338:2023; ISO/IEC 23894:2023

Evaluación de impacto en servicios públicos: Analizar los efectos potenciales de los

sistemas de IA en los servicios públicos, evaluando tanto beneficios como riesgos.

1. Antes de decidir implementar o desarrollar un sistema de IA en servicios públicos, se debe realizar una evaluación de viabilidad que considere beneficios potenciales, riesgos y desafíos. Esta evaluación debe incluir un análisis costo-beneficio y evaluación de la infraestructura tecnológica necesaria.
    - Instrumentos de referencia: NIST-AI-600-1; ISO/IEC 5338:2023; ISO/IEC 23894:2023
2. Se debe asegurar que el diseño e implementación del sistema de IA se realicen de manera transparente y alineados con las mejores prácticas, estándares técnicos y principios éticos, establecidos en capítulos anteriores de este código.
    - Instrumentos de referencia: NIST-AI-600-1; ISO/IEC 5338:2023; ISO/IEC 23894:2023
3. Se debe establecer un sistema de monitoreo y evaluación continua para asegurar que el sistema de IA opere de manera efectiva y se ajuste según sea necesario.
    - Instrumentos de referencia: NIST-AI-600-1; ISO/IEC 5338:2023; ISO/IEC 23894:2023; ISO-IEC 22301; ISO-IEC 20000

Respuesta a incidentes en sistemas de IA: Establecer procedimientos para gestionar, mitigar y resolver incidentes que afecten el funcionamiento de los sistemas de IA.

1. Las entidades deben desarrollar y mantener un plan integral de respuesta a incidentes en los sistemas de IA de acuerdo con el capítulo de ciberseguridad de este código.
    - Instrumentos de referencia: NIST-AI-600-1; ISO/IEC 5338:2023; ISO/IEC 23894:2023; ISO-IEC 22301; ISO-IEC 20000; ISO 27035; NIST 800-61
2. Se deberán reportar los incidentes de los sistemas de IA al Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) a la dirección electrónica incidentesia@micitt.go.cr con nombre, vía de contacto, institución afectada, servicio público afectado y descripción del problema.
3. Se deben implementar acciones correctivas y preventivas para resolver los incidentes y mitigar su impacto en el sistema de IA y las personas beneficiarias. Esto incluye realizar revisiones post-incidentes y auditorías periódicas para evaluar la respuesta y actualizar el plan de gestión de incidentes.

A NIVEL DE SEGURIDAD Y PROTECCIÓN

Se deben implementar medidas técnicas y operativas para garantizar la robustez, seguridad

y protección de los sistemas de IA y la privacidad y seguridad de los usuarios.

Robustez, seguridad y protección: Se deben implementar medidas técnicas y operativas para garantizar la robustez, seguridad y protección de los sistemas de IA contra amenazas y fallos, entre ellas:

1. Se debe diseñar el sistema de IA para ser seguro, incluyendo que pueda manejar errores, perturbaciones y condiciones adversas sin fallar. Para ello, se deben implementar pruebas de estrés y simulaciones de fallos para evaluar y mejorar la robustez del sistema, así como integrar redundancias y mecanismos de recuperación para minimizar el impacto de fallos.
    - Instrumentos de referencia: ISO/IEC TR 5469:2024; ISO-IEC 24028
2. Se deben implementar medidas de seguridad robustas para proteger el sistema de IA y los datos que procesa contra accesos no autorizados y ciberataques, siguiendo los lineamientos establecidos en capítulos previos de este código.
    - Instrumentos de referencia: ISO/IEC TR 5469:2024; ISO-IEC 24028
3. Se debe asegurar la integridad, confidencialidad y disponibilidad de los datos utilizados y generados por el sistema de IA, mediante la implementación de medidas de protección de datos como encriptación, anonimización y respaldo de datos, entre otras.
    - Instrumentos de referencia: ISO/IEC TR 5469:2024; ISO-IEC 24028; ISO/IEC 5259; ISO 27001; NIST CSF; NIST 800-53
4. Se deben realizar actualizaciones y mantenimiento regular del sistema de IA para asegurar que opere protegido contra nuevas amenazas y vulnerabilidades. Para ello, se debe establecer un ciclo de vida de mantenimiento que incluya evaluaciones regulares de la seguridad del sistema y la implementación de mejoras continuas.
    - Instrumentos de referencia: ISO/IEC TR 5469:2024; ISO-IEC 24028; ISO/IEC 5259

Protección de los datos de las personas: Salvaguardar la privacidad, seguridad y bienestar de las personas afectadas por los sistemas de IA.

1. Las entidades deben ser transparentes en el tratamiento de los datos personales, proporcionando a los usuarios acceso a su información y la posibilidad de garantizar a las personas usuarias el ejercicio de su derecho de rectificación. Para ello, se deben establecer políticas claras sobre la recopilación y el uso de datos personales, asegurando que solo se recopilen los datos necesarios y que se utilicen de manera ética y legal, alineado con la Ley N°8968 denominada Ley de Protección de la persona frente al tratamiento de sus datos

personales.

- Instrumentos de referencia: ISO/IEC TR 5469:2024; ISO-IEC 24028; ISO/IEC 5259

2. Se deben implementar medidas de seguridad para proteger los datos personales contra accesos no autorizados, alteraciones, eliminaciones no autorizadas, divulgaciones o destrucciones.

   - Instrumentos de referencia: ISO/IEC TR 5469:2024; ISO-IEC 24028; ISO/IEC 5259

3. Se debe limitar la recopilación y el almacenamiento de datos personales a lo estrictamente necesario para los fines institucionales establecidos.

   - Instrumentos de referencia: ISO/IEC TR 5469:2024; ISO-IEC 24028; ISO/IEC 5259

Resiliencia de infraestructuras críticas: Desarrollar estrategias y medidas para asegurar que las infraestructuras críticas que soportan los sistemas de IA sean resilientes y capaces de recuperarse de perturbaciones.

1. Las entidades deben identificar y evaluar las infraestructuras críticas que soportan los sistemas de IA para determinar su vulnerabilidad.

   - Instrumentos de referencia: ISO/IEC TR 5469:2024; ISO-IEC 24028; ISO 22301; ISO 27001; ISO 31001; NIST 800-53

2. Se deben establecer y mantener planes de continuidad de negocios o Bloques de Control de Proceso (BCP) para asegurar que las infraestructuras críticas puedan continuar operando durante y después de un incidente. Para ello, se deben desarrollar BCPs específicos para cada infraestructura crítica, incluyendo procedimientos detallados para la recuperación y la continuidad operativa.

   - Instrumentos de referencia: ISO/IEC TR 5469:2024; ISO-IEC 24028; ISO 22301; ISO 27001; ISO 31001; ISO 27031

3. Se debe asegurar que las infraestructuras críticas cuenten con redundancias y sistemas de respaldo para mantener la operatividad en caso de fallos o interrupciones. Se recomienda utilizar soluciones de almacenamiento en la nube, sitios alternativos y redundancias físicas y virtuales para asegurar la continuidad operativa.

   - Instrumentos de referencia: ISO/IEC TR 5469:2024; ISO-IEC 24028; ISO 22301; ISO 27001; ISO 31001; NIST 800-53; NIST CSF

A NIVEL DE OPERACIÓN Y MANTENIMIENTO

Se debe gestionar de manera continua el funcionamiento de los sistemas de IA, asegurando su eficiencia, fiabilidad y actualización constante.

Operación del sistema de IA: Gestionar de manera continua el funcionamiento de los sistemas de IA, asegurando su eficiencia, fiabilidad y actualización constante.

1. Se debe establecer un sistema de monitoreo continuo para detectar anomalías y evaluar el rendimiento del sistema de IA en tiempo real, utilizando software de monitoreo continuo que registre el rendimiento del sistema, la utilización de recursos y la precisión de las decisiones de IA.
    - Instrumentos de referencia: ISO/IEC TR 5469:2024; ISO-IEC 24028; ISO 22301; ISO 27001; ISO 31001
2. Las entidades deben establecer procedimientos claros para la gestión de incidentes que incluyan la detección temprana, reporte y resolución de problemas en el sistema de IA, incluyendo al menos protocolos para la escalación de problemas, la comunicación interna y externa durante un incidente, y la documentación de todos los pasos tomados para resolver el problema.
    - Instrumentos de referencia: ISO/IEC TR 5469:2024; ISO-IEC 24028; ISO 22301; ISO 27001; ISO 31001
3. Se debe mantener una documentación técnica exhaustiva y actualizada que detalle el funcionamiento, configuración y mantenimiento del sistema de IA.
    - Instrumentos de referencia: ISO/IEC TR 5469:2024; ISO-IEC 24028; ISO 22301; ISO 27001; ISO 31001

A NIVEL DE ESTÁNDARES Y TECNOLOGÍAS.

Se deben definir y adoptar estándares técnicos nacionales e internacionales para garantizar la interoperabilidad, calidad y seguridad de los sistemas de IA.

Estándares técnicos: Definir y adoptar estándares técnicos nacionales e internacionales para garantizar la interoperabilidad, calidad y seguridad de los sistemas de IA.

1. Las entidades deben adoptar estándares técnicos para la seguridad de la información y de los sistemas de IA reconocidos a nivel nacional e internacional para asegurar la calidad y seguridad de los sistemas de IA.
    - ISO/IEC 38507:2022 ; NIST AI 100-1 AI; ISO/IEC DIS 42006; ISO/IEC TR 5469:2024; ISO-IEC 24028

2. Se debe garantizar que los sistemas de IA puedan interactuar y funcionar de manera conjunta con otros sistemas y tecnologías, para lo cual se deben implementar protocolos y/o interfaces de programación de aplicaciones (API) que aseguren la interoperabilidad de los sistemas de IA con otras plataformas y tecnologías. Esto se debe alinear a lo descrito en el capítulo de interoperabilidad del presente código.

    - ISO/IEC 38507:2022; NIST AI 100-1 AI; ISO/IEC DIS 42006; ISO/IEC TR 5469:2024; ISO-IEC 24028

3. Se debe asegurar que los modelos de IA se desarrollen y validen de acuerdo con estándares técnicos nacionales e internacionales definidos para este efecto.

    - ISO/IEC 38507:2022; NIST AI 100-1 AI; ISO/IEC DIS 42006; ISO/IEC TR 5469:2024; ISO-IEC 24028

A NIVEL DE SOSTENIBILIDAD Y RESPONSABILIDAD SOCIAL

Promover prácticas sostenibles y responsables en el desarrollo y uso de sistemas de IA, minimizando el impacto ambiental y fomentando el diseño centrado en la persona.

Sostenibilidad ambiental: Promover prácticas y tecnologías que minimicen el impacto ambiental de los sistemas de IA y contribuyan a la mitigación del cambio climático.

1. Valorar el impacto ambiental de la infraestructura que requieren las soluciones de IA para la determinación de las estrategias de mitigación adoptadas en cada caso, para fomentar la eficiencia y minimizar el impacto en términos de consumo de energía, generación de residuos electrónicos y uso de recursos naturales.

    - Instrumento de referencia: ISO 50001

2. Implementar prácticas y tecnologías que mejoren la eficiencia energética de los sistemas de IA y reduzcan el consumo de energía, para lo cual se debe utilizar hardware eficiente en términos de energía y optimizar los algoritmos de IA para minimizar el consumo energético.

    - Instrumento de referencia: ISO 50001

3. Se debe promover el uso de energías renovables para alimentar los sistemas de IA y reducir la dependencia de fuentes de energía no sostenibles.

    - Instrumento de referencia: ISO 50001

4. Implementar prácticas de gestión responsable de residuos electrónicos para minimizar el impacto ambiental de los sistemas de IA, esto tanto a nivel interno de las instituciones,

como en el establecimiento de criterios sustentables cuando el sistema de IA sea adquirido mediante contratación pública.

- Instrumento de referencia: ISO 50001

Diseño centrado en la persona: Priorizar las necesidades, expectativas y experiencias de los usuarios en el diseño de los sistemas de IA, asegurando accesibilidad, comprensión y beneficios para todos.

1. Durante la fase de conceptualización del sistema de IA, se deberán realizar diagnósticos de identificación de necesidades, expectativas y preferencias de las personas usuarias. Para la cual, se pueden utilizar métodos de investigación cualitativa y cuantitativa, como encuestas, entrevistas, grupos focales, encuentros de desarrollo colaborativo de software (hackathones), innovación abierta, entre otras, para involucrar a una muestra representativa de personas usuarias que permita asegurar una comprensión amplia y precisa de sus necesidades mediante procesos de co-creación.
2. Se debe asegurar que los sistemas de IA sean accesibles e inclusivos para todas las personas, independientemente de su ubicación geográfica, género, edad, etnia, condición o nivel socioeconómico.
   - Instrumentos de referencia: ISO/IEC AWI 42105; ISO/IEC TR 24368:2022
3. Utilizar un enfoque iterativo en el diseño, creando prototipos y realizando pruebas constantes con usuarios para refinar y mejorar el sistema de IA y asegurar que el producto final cumpla con sus **expectativas** y necesidades.
   - Instrumentos de referencia: ISO/IEC AWI 42105; ISO/IEC TR 24368:2022
4. Se deben considerar otros lineamientos establecidos en capítulos previos en este mismo código sobre personas usuarias.
   - Instrumentos de referencia: ISO/IEC AWI 42105; ISO/IEC TR 24368:2022

A NIVEL DE EVALUACIONES PERIÓDICAS

1. Las entidades deben realizar evaluaciones de impacto iniciales que identifiquen y analicen los efectos potenciales del sistema de IA en los servicios públicos críticos y la sociedad, incluyendo análisis de transparencia y explicabilidad, antes de su implementación a gran escala.
   - Instrumentos de referencia: ISO/IEC TR 5469:2024; ISO-IEC 24028; ISO 22301; ISO 27001; NIST800-34; ITIL; COSO; ISO 20000

2. Las entidades deben llevar a cabo evaluaciones y auditorías internas y externas periódicas para verificar el cumplimiento de los estándares de responsabilidad, documentando los resultados para mejorar continuamente las estrategias de mitigación de riesgos.
    - Instrumentos de referencia: ISO/IEC TR 5469:2024; ISO-IEC 24028; ISO 22301; ISO 27001; NIST800-34; ITIL; COSO; ISO 20000
3. Se deben realizar revisiones periódicas de la evaluación y mitigación de riesgos, asegurando la documentación y el uso de los resultados para fortalecer las estrategias de mitigación y garantizar mejoras continuas.

ESTÁNDARES

La adopción y aplicación de normas técnicas y estándares internacionales es fundamental para asegurar la calidad, seguridad, transparencia y responsabilidad en el desarrollo y uso de sistemas de Inteligencia Artificial (IA). Estos estándares proporcionan un marco sólido para la interoperabilidad, gestión de riesgos y protección de la privacidad, alineando las prácticas nacionales con las mejores directrices globales.

A continuación, se presentan una serie de normas y estándares reconocidos a nivel internacional que complementan y fortalecen los lineamientos establecidos, asegurando que los sistemas de IA implementados en Costa Rica cumplan con los más altos niveles de excelencia y responsabilidad.

Compendio de normas y estándares de IA en Costa Rica:

Instrumento	Descripción	Valor	Enlace
ISO/IEC 27701:2019	Proporciona un marco para la gestión de la privacidad de la información basado en la gestión de la seguridad de la información.	Ayuda a las organizaciones a cumplir con las regulaciones de privacidad, protegiendo la información personal procesada por los sistemas de IA.	https://www.iso.org/standard/71670.html
NIST SP 800-53:	Ofrece un catálogo de controles de seguridad y privacidad para proteger las operaciones y activos	Fortalece la seguridad y privacidad de los sistemas de IA a través de controles específicos	https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

	de información de las organizaciones.	y recomendaciones de implementación.	
IEEE 7000-2021	Estándar para el diseño de sistemas autónomos y de IA con principios éticos.	Proporciona directrices para incorporar consideraciones éticas en el diseño de sistemas de IA.	https://standards.ieee.org/ieee/7000/6781/
ISO/IEC TR 24028:2020	Proporciona un informe técnico sobre la evaluación de la transparencia de los sistemas de IA.	Ayuda a las organizaciones a implementar prácticas de transparencia en el desarrollo y uso de sistemas de IA.	https://www.iso.org/standard/77608.html
OECD AI Principles	Conjunto de principios para asegurar el desarrollo y uso responsable de la IA, promovido por la Organización para la Cooperación y el Desarrollo Económico.	Establece un marco internacional para la gobernanza ética de la IA.	https://oecd.ai/en/ai-principles
ISO 9241-210:2019	Proporciona directrices para el diseño centrado en el usuario de sistemas interactivos.	Garantiza que los sistemas de IA sean accesibles y usables, promoviendo un enfoque centrado en la persona.	https://www.iso.org/standard/77520.html
GDPR (General Data Protection Regulation)	Reglamento de la Unión Europea sobre la protección de datos personales y la privacidad.	Establece estándares para la recopilación, procesamiento y almacenamiento de datos personales, asegurando la privacidad de los usuarios.	https://gdpr-info.eu/
IEEE 12207	Proceso estándar para el ciclo de vida de los sistemas de software y sistemas	Proporciona un marco para la gestión y el desarrollo de proyectos de software, incluyendo sistemas de IA.	https://standards.ieee.org/ieee/12207/5672/
ISO 31000:2018	Proporciona directrices	Ayuda a las	https://www.iso.org/obp/ui#iso:std:iso:310

	sobre la gestión del riesgo.	organizaciones a gestionar los riesgos asociados con el desarrollo y el uso de sistemas de IA.	00:ed-2:v1:es
ISO 27017:2015	Código de práctica para controles de seguridad de la información basados en la nube.	Proporciona controles adicionales para la seguridad de los servicios en la nube, relevante para sistemas de IA que utilizan infraestructura en la nube.	https://www.iso.org/standard/43757.html
ISO 26000:2010	Guía sobre responsabilidad social.	Ayuda a las organizaciones a operar de manera socialmente responsable, alineando los sistemas de IA con principios de sostenibilidad y responsabilidad social.	https://www.iso.org/obp/ui#iso:std:iso:26000:ed-1:v1:es
AI Fairness 360 Toolkit (IBM)	Conjunto de herramientas para la detección y mitigación de sesgos en los modelos de IA.	Facilita la implementación de prácticas de equidad en el desarrollo de sistemas de IA.	https://aif360.res.ibm.com/
Ethics Guidelines for Trustworthy AI (European Commission)	Directrices desarrolladas por el Grupo de Expertos de Alto Nivel sobre Inteligencia Artificial de la Comisión Europea.	Proporciona un marco para desarrollar sistemas de IA que sean éticos, transparentes y responsables.	https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

CAPÍTULO 8:

IMPLEMENTACIÓN DEL PROTOCOLO DE INTERNET IPv6 EN EL SECTOR PÚBLICO COSTARRICENSE

EQUIPO DE TRABAJO

Integrante	Institución
Rosa Zúñiga Quesada	MICITT
César Díaz	LACNIC

INTRODUCCIÓN AL TEMA

La implementación del Protocolo de Internet versión 6 (IPv6) constituye un elemento fundamental para garantizar la continuidad y evolución de Internet, ante el agotamiento de las direcciones IPv4 y el crecimiento sostenido de los servicios digitales, las plataformas tecnológicas y las infraestructuras de conectividad en el sector público.

En este contexto, las entidades del Estado deben incorporar IPv6 como parte de la gestión, desarrollo e implementación de sus redes y servicios digitales, de manera que se asegure la operación adecuada de los sistemas institucionales, la interoperabilidad entre plataformas, la disponibilidad de los servicios públicos digitales y la capacidad de crecimiento de la infraestructura tecnológica.

Asimismo, considerando que en el país se han emitido disposiciones orientadas a la adopción de este protocolo en el sector público, y que persisten oportunidades de mejora en su implementación, resulta necesario integrar IPv6 dentro de un marco estructurado que permita su incorporación de forma planificada y consistente en las iniciativas tecnológicas institucionales.

En este sentido, la adopción de IPv6 deberá contemplarse desde las etapas de diseño, adquisición, desarrollo e implementación de soluciones tecnológicas, asegurando su coexistencia con IPv4 mediante esquemas que permitan la continuidad operativa de los servicios, así como la alineación con estándares técnicos internacionales aplicables.

PRINCIPIOS

Evolución tecnológica y continuidad operativa

Incorporar IPv6 como parte del proceso de evolución de las redes institucionales y de los servicios y trámites digitales brindados a la ciudadanía, asegurando su implementación y su coexistencia con IPv4 mediante esquemas que garanticen la continuidad de los servicios digitales.

Disponibilidad y crecimiento sostenible de las redes

Implementar IPv6 como mecanismo para asegurar la disponibilidad de recursos de direccionamiento, el crecimiento ordenado de las redes y la sostenibilidad de la infraestructura de conectividad del sector público.

POLÍTICAS GENERALES

Establecer los lineamientos para la implementación del Protocolo de Internet versión 6 (IPv6) en las instituciones del sector público costarricense, a fin de garantizar la continuidad, y crecimiento de las redes gubernamentales, en cumplimiento de las Directrices 049-MICITT y 064-MICITT.

Directriz 049-MICITT

El 23 de mayo de 2013, en el Diario Oficial La Gaceta N° 98, se publicó la Directriz 049-MICITT, denominada: “Define fecha límite para la implementación del Protocolo de Internet IPv6 en el Sector Público Costarricense”, con el objetivo de que los órganos, entes, instituciones y empresas del sector público central y descentralizado, implementaran como fecha límite el Protocolo de Internet IPv6, el 30 de junio de 2015, para así garantizar que las personas usuarias accedan a los servicios gubernamentales a través de este protocolo.

Directriz 064-MICITT

El 02 de diciembre de 2019, en el Alcance 268 al Diario Oficial La Gaceta N° 229, se publicó la Directriz N° 064-MICITT denominada: “Lineamientos para el fortalecimiento y la escalabilidad de la infraestructura de red en el sector público costarricense”, con el objetivo de fortalecer y permitir la escalabilidad de la infraestructura de red en el sector público

costarricense, estableciendo el deber de implementar un conjunto de protocolos en la infraestructura tecnológica de las instituciones públicas del país, entre ellos, el Protocolo de Internet IPv6.

POLÍTICAS ESPECÍFICAS

1) Cumplir con la Directriz N° 049-MICITT denominada: “Define fecha límite para la implementación del Protocolo de Internet IPv6 en el Sector Público Costarricense”, publicada en el Diario Oficial La Gaceta N° 98 del 23 de mayo de 2013.

2) Cumplir con la Directriz N° 064-MICITT denominada: “Lineamientos para el fortalecimiento y la escalabilidad de la infraestructura de red en el sector público costarricense”, publicada en el Alcance 268 al Diario Oficial La Gaceta N° 229, del 02 de diciembre de 2019.

3) Los sitios web institucionales, así como los servicios, aplicaciones y trámites digitales brindados a la ciudadanía a través de plataformas tecnológicas, deberán ser accesibles y funcionales mediante IPv6, de forma que los usuarios puedan acceder a ellos y utilizarlos a través de dicho protocolo.

4) Las redes internas de las instituciones públicas, así como los equipos (hardware) y los servicios de infraestructura de red —incluidos DNS, DHCP, correo electrónico, servicios web y servicios en la nube, entre otros— deberán contar con habilitación, configuración y operación efectiva sobre IPv6, garantizando su coexistencia con IPv4.

5) Los carteles de contratación administrativa, así como los términos de referencia y las especificaciones técnicas, deberán incluir como requisito la compatibilidad con el Protocolo IPv6 en los bienes (equipos), servicios y soluciones tecnológicas por adquirir.

6) Gestionar la asignación de prefijos IPv6 conforme al modelo de conectividad y los requerimientos de direccionamiento de cada institución, ya sea a través de sus proveedores de servicios, por medio de las instancias competentes de administración de recursos de Internet, o mediante otros mecanismos habilitados para su asignación.

7) Coordinar con los Proveedores de Servicio de Internet (ISP) de cada institución las acciones técnicas necesarias para habilitar el enrutamiento de tráfico IPv6 en las redes institucionales.

8) Elaborar e implementar un plan interno de implementación de IPv6, basado en un

diagnóstico del estado actual de su infraestructura, que contemple cronograma, responsables y metas verificables.

9) Garantizar que la implementación de IPv6 contemple controles de seguridad equivalentes o superiores a los establecidos para IPv4, incluyendo mecanismos de filtrado, monitoreo, detección de amenazas y gestión de tráfico en entornos IPv6.

10) Fortalecer las capacidades del personal técnico en la gestión, operación, monitoreo y seguridad de redes y servicios basados en IPv6.

11) Establecer mecanismos de seguimiento y reporte del avance anual en la implementación de IPv6, conforme a los requerimientos que establezca el MICITT.

ESTÁNDARES

Las instituciones del sector público deberán aplicar los estándares técnicos definidos por la Internet Engineering Task Force (IETF) para la implementación, operación y gestión del Protocolo de Internet versión 6 (IPv6).

SIGLAS

ACD: Áreas clave de dominio.

AMF: Autenticación de múltiples factores.

ANATEL: Agencia Nacional de Telecomunicaciones de Brasil.

ANSI: American National Standards Institute.

APT: Advanced Persistent Threats.

ASVS: Application Security Verification Standard.

BCCR: Banco Central de Costa Rica.

CA: Certificate Authority / Certification Authority / Autoridad Certificadora.

CCSS: Caja Costarricense de Seguro Social.

CENAREC: Centro Nacional de Recursos para la Educación Inclusiva.

CMM: Capability Maturity Model.

CMMI: Capability Maturity Model Integration.

CNTD: Código Nacional de Tecnologías Digitales.

COBIT: Control Objectives for Information and Related Technologies u Objetivos de Control para Información y Tecnologías Relacionadas.

CPU: Central Processing Unit.

CSIRT: Computer Security Incident Response Team.

DAISY: Digital Accessible Information System / Sistema de Información Digital Accesible.

DGAN: Dirección General del Archivo Nacional de Costa Rica.

DGDCFD: Dirección de Gobernanza Digital y Certificadores de firma digital.

DGME: Dirección General de Migración y Extranjería.

DHCP: Dynamic Host Configuration Protocol

DKIM: Domain Keys Identified Mail.

DMARC: Domain Based Message Authentication

DNS: Domain Name System.

EOF: End-of-life.

ETD: Estrategia de Transformación Digital.

ICT: Instituto Costarricense de Turismo.

IDS: Intrusion Detection System.

IETF: Internet Engineering Task Force.

INCAE: Instituto Centroamericano de Administración de Empresas.

IA: Inteligencia Artificial

IoT: Internet of things.

IP: Internet Protocol.

IPv4: Internet Protocol version 4.

IPv6: Internet Protocol version 6.

IPS: Intrusion Prevention System.

IT: Information Technology / Tecnología de la información.

ITGI: IT Governance Institute / Instituto de Gobernanza de TI.

ITIL: Information Technology Infrastructure Library.

ITL: Information Technology Laboratory.

ITSM: IT service management.

ISACA: Information Systems Audit and Control Association / Asociación de Auditoría y Control de Sistemas de Información.

ISP: Internet Service Provider / Proveedor de Servicio de Internet.

LESCO: Lenguaje de Señas Costarricense.

METS: Metadata Encoding & Transmission Standard.

MICITT: Ministerio de Ciencias, Innovación, Tecnología y Telecomunicaciones.

NFIQ: NIST Fingerprint Image Quality.

NIST: National Institute of Standards and Technology.

OWASP: Open Web Application Security Project.

PcD: Personas con discapacidad.

PCII: Protected Critical Infrastructure Information.

PNCTI: Plan Nacional de Ciencia, Tecnología e Innovación.

PNDIP: Plan Nacional de Desarrollo e Inversión Pública**.**

PNDT: Plan Nacional de Desarrollo de las Telecomunicaciones.

PREMIS: Preservation Metadata: Implementation Strategies.

PRODHAB: Agencia de Protección de Datos de los Habitantes.

RN: Registro Nacional.

SDCM: Service Delivery Capability Model, Modelo de Capacidades de Entrega de Servicios.

SECIT: Seguridad en tecnología de información

SEI: Software Engineering Institute, Instituto de Ingeniería de Software.

SPF: Sender Policy Framework.

S-SDLC/ Secure SDLC: Secure Software Development Life Cycle.

SSL: Secure Sockets Layer.

TI: Ver IT.

TIC: Tecnologías de Información y Conocimiento.

TLS: Transport Layer Security.

TSE: Tribunal Supremo de Elecciones.

UCR: Universidad de Costa Rica.

UE: Unión Europea.

UIT: Unión Internacional de Telecomunicaciones.

UKAAF: United Kingdom Association for Accessible Formats.

URL: Uniform Resource Locator.

UX: User Experience.

VLAN: Virtual Local Area Network.

W3C: World Wide Web Consortium.

WAF: Web Application Firewall.

WCAG: Web Content Accessibility Guidelines / Pautas de Accesibilidad para el Contenido Web.

WWW: World Wide Web.

GLOSARIO

Accesibilidad: La accesibilidad es una condición que deben cumplir los espacios, procesos, productos y servicios, para ser comprensibles, utilizables y practicables por todas las personas en condiciones de seguridad y comodidad y de la forma más autónoma y natural posible, de tal manera que permita la participación plena de todas las personas (Pérez- Castilla, 2010).

Accesibilidad digital: Se entiende por accesibilidad digital el grado en que la información y los servicios digitales están disponibles para personas con diferentes tipos de discapacidades (Sui *et al*., 2017).

Amenazas Persistentes Avanzadas (Advanced Persistent Threats): Son ataques coordinados dirigidos contra una empresa u organización, que tratan de robar o filtrar información sin ser identificados.

APT o Amenazas Persistentes Avanzadas (Advanced Persistent Threats): son ataques coordinados dirigidos contra una empresa u organización, que tratan de robar o filtrar información sin ser identificados.

Arquitectura Orientada a Servicios: Se define como dos instancias computacionales (por ejemplo, programas) que interactúan de manera que una instancia ejecuta cargas de trabajo en función de la otra. Cada interacción del servicio está definida por un lenguaje de descripción, cada interacción es autocontenida y con bajo acoplamiento. Estas son independientes de otras interacciones.

Aplicación: Programa o conjunto de programas cuyo objeto es la resolución de un problema mediante el uso de la informática.

Autenticación: Verificación de la identidad de un usuario, proceso o dispositivo, a menudo como un requisito previo para permitir el acceso a los recursos en un sistema de información. Fuente: SP 800-53; SP 800-53A; SP 800-27; FIPS 200; SP 800-30.

Autenticación de múltiples factores: Es un método de autenticación que emplea dos o más factores para lograr dicho proceso. Los factores incluyen: (i) algo que el usuario sabe (por ejemplo, contraseña / PIN); (ii) algo que el usuario posee (por ejemplo, dispositivo de

identificación criptográfica, token); o (iii) algo que forma parte del usuario (por ejemplo, biométrico). Fuente: SP 800-53.

Bases de datos: cualquier archivo, fichero, registro u otro conjunto estructurado de datos personales, que sean objeto de tratamiento o procesamiento, automatizado o manuales, cualquiera que sea la modalidad de su elaboración, organización o acceso.

Biometría: Es el conjunto de características fisiológicas y de comportamiento que pueden ser utilizadas para verificar la identidad del individuo, lo cual incluye huellas digitales, reconocimiento del iris, reconocimiento facial y otras técnicas.

Botnets: Son redes de robots infectadas y controladas remotamente, quedando incorporadas a redes distribuidas de computadores, los cuales envían mensajes de correo “spam” o código malicioso de forma masiva, con el objetivo de atacar otros sistemas.

Cadena de interoperabilidad: Expresión de la interoperabilidad en el despliegue de los sistemas y los servicios como una sucesión de elementos enlazados e interconectados, de forma dinámica, a través de interfaces y con proyección a las dimensiones técnica, semántica y organizativa.

Capability Maturity Model o Modelo de Madurez de Capacidades: Modelo que comprende un conjunto de mejores prácticas para la evaluación de procesos de desarrollo de software en la organización. Es un modelo anterior al CMMI.

Capability Maturity Model Integration o Modelo de la Madurez de Capacidades de Integración: Conjunto de mejores prácticas para la evaluación y mejoramiento en la industria de desarrollo de software, que clasifica en 5 niveles o etapas el desarrollo de la industria a partir de la implementación de las mejores prácticas.

Centro de Datos: Espacio físico destinado a las redes de datos.

Ciberseguridad: “El conjunto de procesos utilizados para la gestión y protección de la transmisión, el procesamiento, el uso y el almacenamiento de datos e información, mediante tecnologías de información y comunicación (TIC).”

Ciberespacio: El conjunto de espacios físicos e intangibles, compuestos por sistemas informáticos, redes informáticas y de comunicaciones, información digital, contenido transmitido por computadoras y datos de control y comunicaciones, y los usuarios de todo lo anterior.

Ciclo de vida de un documento electrónico: Conjunto de las etapas o períodos por los que atraviesa la vida del documento, desde su identificación en un sistema de gestión de

documentos hasta su selección para conservación permanente, de acuerdo con la legislación sobre archivos de aplicación en cada caso, o para su destrucción reglamentaria.

Ciudadano: Refiere al conjunto de deberes y derechos que corresponde a los costarricenses mayores de dieciocho años (Constitución Política de Costa Rica, 1949).

Computación en la Nube: Paradigma de computación en la Nube para permitir el acceso a la red a un conjunto escalable y elástico de recursos físicos o virtuales que se pueden compartir con administración y aprovisionamiento de autoservicio a pedido (ISO/IEC, 2014).

Control de acceso lógico: Sistema automatizado que controla la capacidad de una persona para acceder a uno o más recursos del sistema informático, como una estación de trabajo, una red, una aplicación o una base de datos. Un sistema de control de acceso lógico requiere la validación de la identidad de un individuo a través de algún mecanismo como un PIN, una tarjeta, un biométrico u otro token. Tiene la capacidad de asignar diferentes privilegios de acceso a diferentes personas dependiendo de sus roles y responsabilidades en una organización. Fuente: NIST SP 800-53 Rev. 4.

Control Objectives for Information and Related Technologies u Objetivos de Control para Información y Tecnologías Relacionadas: Marco de trabajo de buenas prácticas para la gobernanza de TI.

Datos abiertos: Información públicamente disponible que puede ser utilizada a un bajo costo o a ningún costo los cuales son expresados en formatos que puedan ser reutilizados para el desarrollo del sector privado, creación de fuentes de empleo, crecimiento económico, una gobernanza más eficaz y compromiso del ciudadano (Petrov, Gurin y Manley, 2016).

Datos personales: cualquier dato relativo a una persona física identificada o identificable.

Datos sensibles: información relativa al fuero íntimo de la persona, como por ejemplo los que revelen origen racial, opiniones políticas, convicciones religiosas o espirituales, condición socioeconómica, información biomédica o genética, vida y orientación sexual, entre otros.

Decisiones críticas: se refieren a áreas donde las decisiones automatizadas pueden tener un impacto directo y significativo en la vida de las personas y en su bienestar socioeconómico. Estas incluyen diagnósticos médicos, donde la IA analiza datos para ofrecer diagnósticos o recomendaciones de tratamiento; el otorgamiento de beneficios sociales, con sistemas que determinan la elegibilidad para recibir apoyo gubernamental; procesos de reclutamiento y selección de personal, donde la IA evalúa candidatos para tomar decisiones de contratación; y evaluaciones académicas y profesionales que miden el rendimiento de estudiantes o empleados. Además, se extienden a la administración de permisos, licencias y concesiones,

que afectan la aprobación o denegación de solicitudes críticas en sectores como la construcción y comercio; en el sistema de justicia, donde la IA puede asistir en la toma de decisiones judiciales; en la gestión de emergencias, optimizando las respuestas en situaciones de crisis; y en la planificación urbana y territorial, influenciando el desarrollo de infraestructura y servicios urbanos.

Discapacidad: “La discapacidad es el resultado de la relación entre la persona con deficiencias y las barreras que le impiden que participe en la sociedad como los demás” (Naciones Unidas, 2007).

Diseño universal: “Se entenderá el diseño de productos, entornos, programas y servicios que puedan utilizar todas las personas, en la mayor medida posible, sin necesidad de adaptación ni diseño especializado. El “diseño universal” no excluirá las ayudas técnicas para grupos particulares de personas con discapacidad, cuando se necesiten” (Convención sobre los derechos de las personas con discapacidad, 2007) (Ley Nº8661, 2008).

Documento electrónico: Cualquier manifestación con carácter representativo o declarativo, expresada o transmitida por un medio electrónico o informático, y se tendrá por jurídicamente equivalente a los documentos que se otorguen, residan o transmitan por medios físicos (Ley Nº8454, 2005).

E-government: Iniciativa a nivel de gobierno para proveer servicios y productos al habitante y a la industria, utilizando las tecnologías de información y mejorar la calidad de dichos servicios brindados.

Equipo ad-hoc: Grupo de personas que cuentan con el perfil técnico adecuado o especializado para abordar una temática específica.

Ergonomía cognitiva (o ingeniería cognitiva): Es una disciplina que estudia la interacción entre el sistema cognitivo humano y los instrumentos para la elaboración de información, para luego, con los hallazgos obtenidos, sustentar la elaboración de los instrumentos adecuados en usos variados, ya sea para el trabajo, educación, entretenimiento, entre otros (Rizzo, 1995, p.1).

Esquema de metadatos: Instrumento que define la incorporación y gestión de los metadatos de contenido, contexto y estructura de los documentos electrónicos a lo largo de su ciclo de vida.

Estándar: Especificación técnica aprobada por un organismo de normalización reconocido para una aplicación repetida o continuada cuyo cumplimiento no sea obligatorio y que esté incluida en una de las categorías siguientes:

1) Norma internacional: norma adoptada por una organización internacional de

normalización y puesta a disposición del público.

2) Norma nacional: norma adoptada por un organismo nacional de normalización y puesta a disposición del público.

Estándar abierto: Aquél que reúne las siguientes condiciones:

1) Es público y su utilización está disponible de manera gratuita o a un coste que no suponga una dificultad de acceso.
2) Su uso y aplicación no está condicionado por el pago de un derecho de propiedad intelectual o industrial.

Exploits: Es un ataque que se aprovecha de las vulnerabilidades de las aplicaciones, las redes o el hardware, en el cual se obtiene el control de un sistema informático para así poder robar datos guardados en una red.

Firma digital: Cualquier conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permita verificar su integridad, así como identificar en forma unívoca y vincular jurídicamente al autor con el documento electrónico.

Firma digital certificada: Una firma digital se considerará certificada cuando sea emitida al amparo de un certificado digital vigente, expedido por un certificador registrado (Ley Nº8454, 2005).

Gobierno a Ciudadanos (G2C): Son productos o servicios interoperables enfocados en las personas.

Gobierno a Gobierno (G2G): Son productos o servicios interoperables que buscan mejorar los procesos entre las organizaciones del gobierno, brindando transparencia y eficacia hacia los organizaciones, empresas y ciudadanos.

Gobierno a Negocios (G2B): Son productos o servicios interoperables brindados entre las organizaciones del Gobierno y las empresas.

Gobierno Electrónico: Ver E-government.

Identificación: Es el proceso de verificación de la identidad de un usuario, proceso o dispositivo, generalmente como un requisito previo para otorgar acceso a los recursos en un sistema de TI. Fuente: SP 800-47.

Interacción Humano-Computador: “Es un campo de estudio multidisciplinario que se centra en el diseño de la tecnología informática y, en particular, la interacción entre los humanos (los usuarios) y las computadoras. Aunque inicialmente se ocupaba de las computadoras, HCI se ha expandido para cubrir casi todas las formas de diseño de tecnología de la información (IDF,

s.f.).

Interfaz: Se entiende por interfaz **"**un dispositivo o programa que habilita a un usuario a comunicarse con un computador" (Oxford, 2019).

Interoperabilidad: Habilidad de organizaciones y sistemas dispares y diversos para interactuar con objetivos consensuados y comunes, con la finalidad de obtener beneficios mutuos. La interacción implica que las organizaciones involucradas compartan información y conocimiento a través de sus procesos de negocio, mediante el intercambio de datos entre sus respectivos sistemas de tecnología de la información y las comunicaciones (Criado, Gascó y Jiménez, 2010).

Interoperabilidad Organizativa: Aborda la definición de los objetivos de procesos y servicios de las organizaciones implicadas en la prestación de servicios telemáticos o de iniciativas de cooperación e integración de *back offices*. Específicamente, hace referencia a la colaboración de organizaciones que desean intercambiar información manteniendo diferentes estructuras internas de gobierno y procesos de negocio variados. La interoperabilidad organizativaasegura la coordinación y el alineamiento de los procedimientos administrativos que intervienen en la provisión de los servicios de Gobierno Electrónico. En la práctica, ello implica definir de manera colaborativa el por qué y el cuándo de los intercambios de información, las normas y reglas que garantizarán la seguridad en dichos intercambios o los planes que guiarán la implantación de las iniciativas (Criado, Gascó y Jiménez, 2010).

Interoperabilidad Semántica: Se ocupa del significado en el uso de los datos y la información y, en concreto, garantiza que el significado preciso de la información intercambiada pueda ser entendido por cualquier aplicación. Para ello, habilita a los sistemas para combinar la información proveniente de otras fuentes y para procesarla de una manera integrada y con el sentido adecuado. Algunas de las herramientas con las que cuenta son los sistemas de clasificación, los tesauros, los metadatos y las ontologías (Criado, Gascó y Jiménez, 2010).

Interoperabilidad Técnica: Se refiere a aquellas cuestiones técnicas que garantizan que los componentes tecnológicos de los sistemas de información de las entidades participantes estén preparados para colaborar con los demás. Permite, por tanto, proporcionar mecanismos comunes de transferencia de datos y de invocación de funciones, transparentes al sustrato de redes y sistemas informáticos existentes. Entre otras cuestiones, se refiere a interfaces, servicios de interconexión, integración de datos, *middleware*, presentación e intercambio de datos, accesibilidad o servicios de seguridad (Criado, Gascó y Jiménez, 2010).

Metadato: Información que caracteriza o describe a otro recurso de información, especialmente con el propósito de documentar, describir, preservar o administrar ese recurso.

Metadato de gestión de documentos: Información estructurada o semiestructurada que hace posible la creación, gestión y uso de documentos a lo largo del tiempo en el contexto de su creación. Los metadatos de gestión de documentos sirven para identificar, autenticar y contextualizar documentos, y del mismo modo con las personas, los procesos y los sistemas que los crean gestionan, mantienen y utilizan.

Neutralidad Tecnológica:

1. Las administraciones contrates deben garantizar la independencia en la elección de las alternativas tecnológicas escogidas por los oferentes e interesados, para lo cual se deben emplear estándares abiertos o de uso generalizado (v. gr. software libre o de código abierto). El artículo 143 RLCA, establece que el sistema empleado por la administración no debe contener exigencias propias de tecnologías propiedad de determinados fabricantes (Jinesta Lobo).

2. Posibilidad que tienen los operadores de redes y proveedores de servicios de telecomunicaciones para escoger las tecnologías por utilizar, siempre que estas dispongan de estándares comunes y garantizados, cumplan los requerimientos necesarios para satisfacer las metas y los objetivos de política sectorial y se garanticen, en forma adecuada, las condiciones de calidad y precio a que se refiere esta Ley (Ley N°8642 General de Telecomunicaciones, 4 de junio, 2008).

No repudio: Garantizar que el remitente de la información se proporciona con el comprobante de entrega y el destinatario se proporciona con el comprobante de la identidad del remitente, de manera que ninguno de los dos puede negar haber procesado la información. Fuente: CNSSI-4009; SP 800-60.

Ownership: Propiedad sobre activos virtuales.

Política: Es la orientación o directriz que es divulgada, entendida y acatada por todos los miembros de la organización, que relacionan normas y responsabilidades dentro de la organización.

Política de gestión de documentos electrónicos: Orientaciones o directrices que define una organización para la creación y gestión de documentos auténticos, fiables y disponibles a lo largo del tiempo, de acuerdo con las funciones y actividades que le son propias. La política se aprueba al más alto nivel dentro de la organización, y asigna responsabilidades en cuanto a la coordinación, aplicación, supervisión y gestión del programa de tratamiento de los documentos a través de su ciclo de vida, de acuerdo con las políticas establecidas por el Archivo Nacional.

Proceso gubernamental: Es un conjunto de actividades organizadas de manera sistemática para la generación de un producto o servicio. Esta estructura lógica y ordenada agiliza las actividades y facilita su control.

Protección de datos: “La protección de datos es el proceso de proteger la información importante de la corrupción y/o pérdida.

El término protección de datos se utiliza para describir tanto el respaldo operativo de datos y la recuperación de desastres/continuidad del negocio (BC/DR). Una estrategia de protección de datos debe incluir la gestión del ciclo de vida de datos (DLM), un proceso que automatiza el movimiento de datos críticos hacia el almacenamiento en línea y fuera de línea y la gestión del ciclo de vida de la información (ILM), una estrategia global para la valoración, catalogación y protección de los activos de información de errores de aplicación/usuario, ataques de malware/virus, fallo de la máquina o cortes de energía/interrupciones en las instalaciones.”

Phishing: Es un ataque cuyo objetivo principal es obtener de manera fraudulenta datos confidenciales de un usuario, aprovechando la confianza que este tiene en los servicios tecnológicos, el desconocimiento de la forma en que operan y la oferta de servicios, en algunos casos, con pobres medidas de seguridad. Para realizar este tipo de amenaza, se utilizan mensajes de correo electrónico y falsos sitios Web, que suplantan perfectamente a los sitios originales.

Ranking o Clasificación: Relación de un conjunto de elementos, con un orden dado por uno o varios criterios priorizados.

Redes de datos: Activos físicos que conforman los recursos computacionales.

Repositorio electrónico: Archivo centralizado donde se almacenan y administran datos y documentos electrónicos, junto con sus metadatos.

Seguridad de la Información: “La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.”

Seguridad Informática: “La seguridad informática es un conjunto de herramientas, procedimientos y estrategias que tienen como objetivo garantizar la integridad, disponibilidad y confidencialidad de la información de una entidad en un sistema.

La seguridad informática se caracteriza por la protección de datos y de comunicaciones en una red asegurando, en la medida de lo posible, los tres principios básicos:

La integridad de los datos: la modificación de cualquier tipo de información debe ser conocido y autorizado por el autor o entidad.

La disponibilidad del sistema: la operación continua para mantener la productividad y la credibilidad de la empresa.

La confidencialidad: la divulgación de datos debe ser autorizada y los datos protegidos contra ataques que violen este principio. La seguridad informática es una disciplina o rama de la Tecnología de la información, que estudia e implementa las amenazas y vulnerabilidades de los sistemas informáticos especialmente en la red como, por ejemplo, virus, gusanos, caballos de troya, ciber-ataques, ataques de invasión, robo de identidad, robo de datos, adivinación de contraseñas, intercepción de comunicaciones electrónicas, entre otros."

Service Delivery Capability Model o Modelo de Capacidades de Entrega de Servicios: Modelo para la medición de las capacidades de entrega de servicios por parte de las organizaciones. Es un modelo australiano que consiste en un marco de trabajo común para identificar los aspectos clave para la implementación de servicios en la industria.

Servicio: Un mecanismo para permitir el acceso a una o más capacidades, donde el acceso se proporciona mediante una interfaz prescrita y se ejerce de manera coherente con las restricciones y políticas especificadas en la descripción del servicio (Official Oasis Standard, 2006).

Sistemas críticos: se refiere a cualquier sistema de IA cuyo funcionamiento es esencial para el mantenimiento de actividades fundamentales en sectores clave, y donde su fallo o mal funcionamiento podría resultar en consecuencias graves, incluyendo daños significativos a la seguridad, salud, bienestar económico de las personas, o al ambiente. Estos sistemas son críticos debido a que su impacto trasciende la esfera operativa normal, afectando aspectos vitales como infraestructuras críticas, servicios de emergencia, seguridad, transporte, comunicaciones y sistemas financieros.

Sistema que utilicen Inteligencia Artificial (Sistemas de IA): Un sistema de IA es un sistema basado en máquinas que, con objetivos explícitos o implícitos, infiere, a partir de la entrada que recibe, cómo generar salidas como predicciones, contenido, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales. Los diferentes sistemas que utilicen IA varían en sus niveles de autonomía y adaptabilidad después de su implementación.

Sistema datacéntrico: Sistema basado en el uso de datos a través de sus relaciones. La información depende del sistema que lo creó.

Sistema docucéntrico: Sistema basado en el uso de documentos electrónicos, para su

gestión, clasificación, preservación.

Software Engineering Institute o Instituto de Ingeniería de Software: Instituto federal estadounidense para desarrollar modelos de evaluación y mejora del desarrollo de software.

Spam: Consiste en el recibo de mensajes no solicitados, principalmente por correo electrónico, cuyo propósito es difundir grandes cantidades de mensajes comerciales o propagandísticos.

Spyware: Conocidos como programas espías, son códigos maliciosos cuyo principal objetivo es recoger información sobre las actividades de un usuario en una computadora, para permitir el despliegue sin autorización en ventanas emergentes de propaganda de un producto o servicio, o, por ejemplo, para robar información personal como números de tarjetas de crédito.

Tecnologías de Información: Uso del cómputo y las telecomunicaciones para el almacenamiento, procesamiento y recuperación de datos.

Troyanos, Virus y gusanos: Son programas de código malicioso capaces de alojarse de diferentes maneras en las computadoras con el fin de permitir el acceso no autorizado a un atacante o a permitir el control de forma remota de los sistemas. Antes que la destrucción de archivos confidenciales, el principal objetivo de estos códigos maliciosos es robar información financiera, poniendo en riesgo los datos confidenciales y el dinero de las personas u organizaciones.

Actualmente existen unos nuevos virus, denominados criptovirus, los cuales cifran la información contenida en el disco del equipo y posteriormente se solicita una cantidad de dinero para que los autores del disco del equipo entreguen las claves para recuperar el contenido de los archivos cifrados.

User Experience o Experiencia de Usuario: Habitualmente referido a las interacciones humano-computadora, el término ahora se usa para referirse a cualquier interacción específica de diseño humano, desde dispositivos digitales a procesos de ventas o una conferencia completa (Knemeyer et al., s.f.).

Virtualización: Es la creación de una simulación por medio de software de algún recurso tecnológico, que puede ser una plataforma de hardware, un sistema operativo, un dispositivo de almacenamiento, aplicaciones de colaboración, etc.

World Wide Web o Mundo de hipertexto: Servicio de internet conformado por la colección de páginas de documentos con lenguaje de marcación de hipertexto.

REFERENCIAS

Agencia Europea para Necesidades Especiales y Educación Inclusiva. (2015). *Guidelines for Accessible Information*. ICT for Information Accessibility in Learning.

A. Naser (coord.), “Gobernanza digital e interoperabilidad gubernamental: una guía para su implementación”, Documentos de Proyectos (LC/TS.2021/80), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2021.

ANSI/NIST-ITL. (2000). *Data Format for the Interchange of Fingerprint, Facial, & Scar & Tattoo*.

ANSI/NIST-ITL. (2007). *Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information*.

Archivo Nacional. (2017). *Norma Nacional de Descripción Archivística*. Archivo Nacional. San José: Costa Rica.

BID (Banco Interamericano de Desarrollo) (2019), El ABC de la interoperabilidad de los servicios sociales: marco conceptual y metodológico. Recuperadode https://publications.iadb.org/es/el-abc-de-la-interoperabilidadde-los-servicios-sociales-marco-conceptual-y-metodologico.

Carreras, O. (2012). *Accesibilidad web y SEO*. La Gaceta. San José: Costa Rica.

Castillo Solano, M. y Umaña Alpízar, R. (2018). Modelo de Preservación de Documentos Digitales En La Administración Universitaria. Universidad Nacional de Costa Rica. Heredia: Costa Rica.

CGR. (2007). *Normas técnicas para la gestión y el control de las Tecnologías de Información*.

Criado, J. Gascó, M. y Jiménez, C. (2010). Bases para una Estrategia Iberoamericana de Interoperabilidad. Buenos Aires, Argentina: XII Conferencia Iberoamericana de Ministros de Administración Pública y Reforma del Estado.

Cruz, C. A., Gómez, M. J. M., Ceciliano, L. S., & Vargas, J. V. (2018). *Código Nacional de Tecnologías Digitales Capítulo 9â Uso de la nube*.

Directriz Nº 049-MICITT. (2013). Define fecha límite para la implementación del Protocolo de Internet IPv6 en el Sector Público Costarricense. Recuperado de https://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=74895&nValor3=92632&strTipM=TC

Directriz Nº 064 -MICITT. (2019). Lineamientos para el fortalecimiento y la escalabilidad de la infraestructura de red en el sector público costarricense. Recuperado de http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=90160&nValor3=118631&strTipM=TC

Espinoza Suarez, J. Meneses Gómez, V. Picado Valverde, F. Ramírez Cerdas, C. (2018). Código Nacional Gobierno Digital – Interoperabilidad y gestión de atributos ciudadanos. Instituto Tecnológico de Costa Rica. Cartago: Costa Rica.

Gobierno de Costa Rica. (2018). *Decreto Ejecutivo N° 41248-MP-MICITT-PLAN-MEIC-MC Creación de la Comisión de Alto Nivel de Gobierno Digital del Bicentenario*. La Gaceta. San José: Costa Rica.

Gobierno de Costa Rica. (2019). *Directriz N°019-MP-MICITT Desarrollo del Gobierno Digital del Bicentenario*. La Gaceta. San José: Costa Rica.

Gobierno de Costa Rica. (2014). *Directriz Nº036-MTSS-MICITT Implementación de accesibilidad de la red de los sitios del sector público*. La Gaceta. San José: Costa Rica.

Gobierno de Costa Rica. (2006). *Reglamento a la Ley de Contratación Administrativa*. La Gaceta. San José: Costa Rica.

GOV.UK (2018). *Accessible communication formats*. Recuperado de https://www.gov.uk/government/publications/inclusive-communication/accessible-communication-formats

IDF. (s.f. a). *Human-Computer Interaction (HCI)*. Interaction Design Foundation. Recuperado de https://www.interaction-design.org/literature/topics/human-computer- interaction

INEC. (2019). Enadis 2018. Población por situación de discapacidad, según el uso de lengua de señas. Recuperado de http://www.inec.go.cr/sites/default/files/documetos- biblioteca-virtual/resocialenadis2018-04.xls

ISO 9241-210:2010. *Ergonomics of human-system interaction - Part 210: Human-centred design for interactive systems*. Recuperado de https://www.iso.org/standard/52075.html

ISO/IEC. (2014a). *ISO/IEC 17788:2014*.

ISO/IEC. (2014b). *ISO/IEC 17789:2014*. ISO/IEC. (2016a). *ISO/IEC 19086-1:2016*. ISO/IEC.

(2016b). *ISO/IEC 27036-4:2016*. ISO/IEC. (2017). *ISO/IEC 19941:2017*.

ISO/IEC. (2018). *ISO/IEC 19086-2:2018*.

ISO/IEC. (2019). *ISO/IEC TR 22678:2019*.

Knemeyer, D. & Sbovoda, E. (s.f.). *User Experience - UX*. Recuperado de https://www.interaction-design.org/literature/book/the-glossary-of-human-computer-interaction/user-experience-ux

Ley N°7494 de Contratación Administrativa. La Gaceta, San José, Costa Rica, 2 de mayo de 1995.

Ley N°7948. Ratificación de la Convención Interamericana para la Eliminación de todas las Formas de Discriminación contra las PcD. La Gaceta, San José, Costa Rica, 18 de noviembre de 1999.

Ley N° 8454 de Certificados Firmas y Documento Electrónicos. La Gaceta, San José, Costa Rica, 13 de octubre de 2005.

Ley N°8642. Ley General de Telecomunicaciones. La Gaceta, San José, Costa Rica, 4 de junio de 2008.

Ley N° 8661 de Aprobación de la Convención sobre los Derechos de las Personas con Discapacidad y su Protocolo. La Gaceta, San José, Costa Rica, 19 de agosto de 2008.

Lueders, H. (2004), "'El marco europeo de interoperabilidad': recomendaciones de la industria de las tecnologías de la información y comunicación" Recuperado de https://administracionelectronica.gob.es/pae_Home/pae_Biblioteca/pae_Tecnimap/pae_T

ECNIMAP_2004_-_Murcia/pae_COM_2004-Integracion_de_servicios_publicos.html?currentPage=2&idioma=es.

Méndez Sanhueza, F. (2013), “An approach based on language ontology and serious

Makaton. (2017). The Makaton Charity. Recuperado de https://www.makaton.org/

Ministerio de Ciencia, Tecnología y Telecomunicaciones. (2013). *Directriz Nº46-H-MICITT*.

Ministerio de Ciencia, Tecnología y Telecomunicaciones. (2018). *Estrategia de Transformación Digital hacia la Costa Rica del Bicentenario 4.0*. Ministerio de Ciencia, Tecnología y Telecomunicaciones. San José: Costa Rica.

Ministerio de Ciencia, Tecnología y Telecomunicaciones. (2023). *Estrategia de Transformación Digital.* Ministerio de Ciencia, Tecnología y Telecomunicaciones. San José: Costa Rica.

Ministerio de Ciencia, Tecnología y Telecomunicaciones. (2022). *Plan Nacional de Desarrollo de las Telecomunicaciones 2022-2027*. Ministerio de Ciencia, Tecnología y Telecomunicaciones. San José: Costa Rica.

Ministerio de Hacienda y Administraciones Públicas. (2016). *Política de gestión de documentos electrónicos 2da Edición*. Ministerio de Hacienda y Administraciones Públicas. Madrid: España.

Ministerio de Planificación Nacional y Política Económica. (2016). *Guía para la Elaboración de Políticas Públicas*. Ministerio de Planificación Nacional y Política Económica. San José: Costa Rica.

Naciones Unidas. (2007). *Convención sobre los Derechos de las Personas con Discapacidad*. Recuperado de https://www.un.org/esa/socdev/enable/documents/tccconvs.pdf

NCSU. (1997). The Principles of Universal Design, Version 2.0. Recuperado de https://projects.ncsu.edu/ncsu/design/cud/about_ud/udprinciplestext.htm

Nielsen, J. The Definition of User Experience (UX). (s.f.). Recuperado de https://www.nngroup.com/articles/definition-user-experience/

Nielsen, J. Usability 101: Introduction to Usability. (2012). Recuperado de https://www.nngroup.com/articles/usability-101-introduction-to-usability/

NIST. (2004). *Fingerprint Image Quality*.

OASIS Reference Model for Service Oriented Architecture 1.0. Official OASIS Standard, 2006.

Oxford (2019). *Oxford Dictionaries*. Recuperado de https://en.oxforddictionaries.com/definition/interface

Papantoniou, B. (s.f.). *Cognitive ergonomics*. Recuperado de https://www.interaction-design.org/literature/book/the-glossary-of-human-computer-interaction/cognitive- ergonomics

Petrov, O. Gurin, J. y Manley, L. (2016). *Open Data for Sustainable Development*. World Bank Group.

Pérez-Castilla, L. (2010). Cambios en la Concepción de la Discapacidad y Nuevas Perspectivas. *En Seminario Clasificación Internacional del Funcionamiento, de la Discapacidad y de la Salud*. San José: Costa Rica.

Piedra, L. A., Solís, D. C., Garita, E. G., & Calderón, J. J. V. (2018). *Código Nacional de Gobierno Digital: Redes de Datos*.

Sala Constitucional. (2000). Resolución Nº11516. San José: Costa Rica. Sala Constitucional.

(1998). Resolución Nº00998. San José: Costa Rica.

Sui, H., & Dempsey, B. (2017). *Digital Accessibility Compliance Program*. Information Technology Services. Boston: EEUU.

Unión Internacional de Telecomunicaciones. (2016). *Buenas prácticas y logros en accesibilidad de las TIC en la región de las Américas*. Recuperado de https://www.itu.int/en/ITU-D/Regional- Presence/Americas/Documents/EVENTS/2016/15526-MX/AAIII-best-practices-and- guidelines-Accesible-SP.pdf

Vargas, A. M., Uribe, C. R., & Vargas, G. V. (2018). *Código Nacional de Tecnologías Digitales de Costa Rica, área de Centro de Datos*.

World Wide Web Consortium (W3C). (2018). *Web Content Accessibility Guidelines (WCAG) 2.1.* Recuperado de https://www.w3.org/TR/WCAG21/#later-versions-of-accessibility-guidelines