04 de noviembre de 2019
DTIC-7021-2019

Máster
Robert Picado Mora, Subgerente a.i.
Dirección de Tecnologías de Información y Comunicaciones
Caja Costarricense de Seguro Social

Asunto: Análisis del Código Nacional de Tecnologías Digitales, propuesto por el Ministerio de Ciencia, Tecnologías y Telecomunicaciones, capitulo Ciberseguridad

Estimado señor:

Se ha recibido oficio DTIC-6476-2019, donde se traslada el documento "*Código Nacional de Tecnologías Digitales*", con el objetivo de realizar el análisis técnico del capítulo denominado "Ciberseguridad"

Al respecto, el equipo de trabajo desarrolló el documento adjunto a la presente donde se realiza un análisis desde la perspectiva de negocio y técnica referente al tema de ciberseguridad.

Quedamos en la mayor disposición para aclarar consultas o dudas que puedan presentarse sobre el tema.

Con mis atentos saludos, suscribe,

CAJA COSTARRICENSE DE SEGURO SOCIAL
Gerencia General
Dirección de Tecnologías de Información y Comunicaciones

MANUEL EMILIO MONTILLANO VIVAS (FIRMA)
Fecha: 2019.11.07 10:23:12 -06'00'

Manuel Montillano Vivas

Equipo de Trabajo
Archivo digital

CRITERIO DE ANÁLISIS DEL CÓDIGO NACIONAL DE TECNOLOGÍAS DIGITALES, PROPUESTO POR EL MINISTERIO DE CIENCIA, TECNOLOGÍAS Y TELECOMUNICACIONES

Antecedentes:

1. Es mediante correo electrónico del 17 de octubre de 2019 al ser las 15:05 p.m se nos convoca a reunión el 21 de octubre por parte del ingeniero Manuel Montillano Vivas representante de la Dirección de Tecnologías de Información y Comunicaciones, para el *"Análisis del Código Nacional de Tecnologías Digitales, propuesto por el Ministerio de Ciencia, Tecnologías y Telecomunicaciones"*, en el cual se adjunta los documentos denominados: DTIC-6476-2019 y Código Nacional de Tecnologías Digitales, propuesto por el Ministerio de Ciencia, Tecnologías y Telecomunicaciones.
2. El lunes 21 de octubre del año en curso se celebra la primera reunión para efectos de Analizar el Código Nacional de Tecnologías Digitales, propuesto por el Ministerio de Ciencia, Tecnologías y Telecomunicaciones, sita Sala 2, Dirección de Prestaciones Sociales, piso comercial, Edificio Jenaro Valverde "Anexo".
3. El 24 de octubre del año en curso se convoca la segunda reunión con el mismo fin.
4. En fecha del 31 de octubre 2019, se realiza sesión de trabajo final.

A continuación, producto de las reuniones llevadas a cabo se detallan las observaciones según el orden dado en este capítulo:

Observaciones Generales:

- **Apartado INTRODUCCIÓN AL TEMA:**

a. Se solicita ahondar más en la justificación con respecto a la creación y definición del capítulo.
b. Este capítulo de estar enfocado al uso de las tecnologías a través de la conectividad internet (internet-cosas). y en las amenazas de seguridad cibernética
c. Se debe tomar en cuenta que la Ciberseguridad debe, además, garantizar al titular de los datos el derecho de la autodeterminación informativa sobre el uso y destino con el fin de impedir su uso ilícito y lesivo para la dignidad y derechos, la protección del tratamiento de los datos personales, son aspectos fundamentales de los derechos y privacidades de las personas.
d. La confidencialidad, disponibilidad, integridad (CID) son definiciones propias de la Seguridad de la Información. además de los aspectos de seguridad y protección de los datos personales consignados en las bases de datos digitales.

- **Apartado DEL OBJETIVO Y ALCANCE:**

a. Se solicita ampliación en lo referente al alcance y objetivo para que exista congruencia entre los conceptos de Seguridad de la Información, Seguridad Informática y Ciberseguridad.

- **Apartado RELACIÓN CON OTROS CAPÍTULOS DEL CÓDIGO:**

a. No existe claridad conceptual entre los conceptos de Ciberseguridad, Seguridad Informática y Seguridad de la Información. aspecto fundamental para definir el alcance esperado de este código

- **Apartado PRINCIPIOS:**

a. Se solicita se realice la división de los principios por cada tema abordado, refiérase a Ciberseguridad, Seguridad Informática y Seguridad de la Información. los mismos con referencia a los documentos de buenas prácticas.
b. En el principio de confidencialidad debe ser visto u observado más un tema de derecho de protección de la información y no divulgación sin consentimiento informado.
c. El principio de Integridad es más orientado a la protección de la información y además a otros temas como las aplicaciones y configuraciones, ya que podrían en riesgo la confidencialidad de información (sensible, restringida y pública), la cual puede ser controlada por bitácoras, firma digital, hashes, encriptación y controles de accesos. Esta terminología o bien los principios ajustados deberían estar categorizada bajo el los principios de Arquitectura de Seguridad, ya que se dejan algunos elementos importantes de considerar como, por ejemplo: Firewalls, aislamiento y segmentación de los dispositivos de comunicación, monitoreo, detección y registro. Otro elemento que considerar sería la seguridad de redes, sistemas, aplicaciones y datos, dentro de esta se debe indicar la evaluación de riesgo, la gestión de vulnerabilidades, entre otras (pruebas de intrusión).
d. Disponibilidad elemento necesario definir la política conceptualizar los elementos para asegurar el acceso oportuno y confiable para el uso de la información y a su vez proteger los datos.

- **Apartado POLÍTICAS GENERALES Y POLÍTICAS ESPECÍFICAS:**

a) En este apartado se lee: *"Las siguientes políticas generales deben ser consideradas como punto de partida para la evaluación de la seguridad donde sea aplicable (...)"* y en el segundo apartado *"El objetivo principal de las políticas específicas es brindar un listado de lineamientos técnicos considerados como requerimientos de buenas prácticas destinadas a ser aplicados(...)"* solicitándose se aclaré porque se denomina a estos apartados política y políticas específicas, siendo que a lo interno de nuestra institución el término de Política difiere de lo consignado.
b) Falta de especificidad en las políticas específicas, así como tipificar cuales están dirigidas al usuario final o consumidor de los servicios digitales que se brindan. e indicar las fuentes

- **Apartado GLOSARIO:**

a) Se debe incorporar los términos de iniciativas y proyectos.
b) Las definiciones de algunos términos no corresponden a la bibliografía suministrada, se solicita revisar.
c) Incluir las definiciones de Seguridad de la Información, Seguridad Informática, Ciberseguridad y protección de datos.

Otros apartados distintos a lo solicitado:

a) Se hace mención del *"Sello de gobierno digital";* sin embargo, no se define claramente si este será vinculante o no para las instituciones meta. no indica una categorización de cuales proyectos son candidatos a este sello, cuál es la métrica? costo de inversión del proyecto impacto social, regulaciones de ley.
b) Valorar secuencia lógica entre los temas, a efectos de facilitar al lector ubicando mejor los beneficios y compromisos que adquiere con el establecimiento de este código, según el tipo de actor.
c) Referenciar las figuras de acuerdo con su realidad.
d) El documento en términos generales no cuenta con un proyecto de gobernanza con un proceso de gobernanza institucional
e) Aclarar la siguiente idea *"Gestión del riesgo de la cadena de suministro"*, siendo que este obedece a una definición de los procesos industriales.
f) Que cada apartado del documento cuente con ideales de protocolos para aplicarlos.
g) En relación con los estándares mencionados en el Código, se recomienda analizar la vinculación con el capítulo de Ciberseguridad.
h) Se recomienda, establecer un análisis previo por institución para la implementación o adaptación de los diferentes estándares sugeridos en el presente código. Con el objetivo que exista una definición nacional del concepto Gobernanza en TIC.

Finalmente, como equipo de trabajo concluimos con la tabla de validación lo siguiente: (esto se debe completar en conjunto).

CAPÍTULO 3: CIBERSEGURIDAD				
cod	ASPECTOS QUE EVALUAR	Si	No	OBSERVACIONES (en caso de indicar que No)
3.1	Las pautas establecidas cumplen el objetivo del capítulo. (Pertinencia)		X	Ver observaciones.
3.2	Claridad en la descripción pautas procedimental. (Aspecto de fondo)		X	Ver observaciones.
3.3	Las pautas se consideran suficientes para cumplir el objetivo. (cantidad)		X	Ver observaciones.
3.4	Correcta estructura del capítulo. (Aspecto de forma)		X	Ver observaciones.
3.5	Aspectos por mejorar.	Ver observaciones antes señaladas.		

Aprobación de Integrantes:

Nombre	Lugar de trabajo	Firma Digital
Manuel Montillano Vivas	Dirección de Tecnologías de Información y Comunicaciones	
Ronald Guzman Vásquez	Gerencia Médica	
Natalie C. Fonseca Loáiciga	Dirección de Planificación Institucional	
Manuel Eduardo Cerdas Velásquez	Gerencia General	

Róger Muñoz Díaz	Gerencia Administrativa	
José Solís Rodríguez	Área de Gestión Informática	
Alexánder Solís Abarca	CGI Gerencia Financiera	
Minor Zúñiga Sedó	Dirección SICERE	
Jeffry Monge Salmerón	Dirección de Inspección	
Jorge Abraham Porras Pacheco	Despacho Gerencia Infraestructura y Tecnologías	