

MEMORIA

XXXI CONGRESO ARCHIVÍSTICO NACIONAL

LA INFORMACIÓN: EL ADN DE LA TRANSFORMACIÓN DIGITAL

22, 23 y 24 de julio del 2019, San José, Costa Rica



COLECCIÓN DE MEMORIAS

ISBN 978-9968-690-10-2



ISBN 978-9968-690-10-2

Ministerio de Cultura y Juventud
Dirección General del Archivo Nacional

MEMORIA
XXXI CONGRESO ARCHIVÍSTICO NACIONAL
"LA INFORMACIÓN: EL ADN DE LA TRANSFORMACIÓN DIGITAL"

Colección de Memorias

22, 23 y 24 de julio de 2019
San José - Costa Rica



027

C749c Congreso Archivístico Nacional (31 : 2019 : San José, C.R.)

La información: El ADN de la transformación digital : memoria. – Primera edición –
San José, Costa Rica : Junta Administrativa del Archivo Nacional, 2021.

1 recurso en línea (126 p.) il., digital, archivo PDF ; 3.71 MB (Colección de Memorias)

ISBN 978-9968-690-10-2

1. Archivística. 2. Congresos. 3. Archivos Costa Rica. 4. Administración de
archivos. I. Título

Ministerio de Cultura y Juventud
Dirección General del Archivo Nacional
San José - Costa Rica

Editorial
Junta Administrativa del Archivo Nacional

Director
Alexander Barquero Elizondo
Dirección General del Archivo Nacional

Unidad de Proyección Institucional
Maureen R. Herrera Brenes
Catalina Zúñiga Porras
Gabriela Soto Grant

Diseño gráfico
Gabriela Soto Grant

Dirección General del Archivo Nacional de Costa Rica. Curridabat,
San José, Costa Rica.
Apartado Postal: 41 2020 Zapote
Teléfono: (506) 2283-1400
Fax: (506) 2234-7312
Correo electrónico: archivonacional@dgan.go.cr
Página web: www.archivonacional.go.cr

Nota: los textos se editaron a partir de las conferencias impartidas.
Si bien se adaptaron lo mejor posible al registro escrito, es posible
que en algunos casos se encuentren vestigios de lenguaje oral y
coloquial.

Sylvie Durán Salvatierra

Ministra de Cultura y Juventud

Alexander Barquero Elizondo

Director General del Archivo Nacional

**JUNTA ADMINISTRATIVA DEL ARCHIVO
NACIONAL**

Dennis Portuguez Cascante
Presidente

David Bullón Patton
Vicepresidente

Ramsés Fernández Camacho
Secretario

Aarón Arguedas Zamora
Tesorero

Eduardo Bedoya Benítez
Primer Vocal

Nathalie Gómez Chinchilla
Segundo Vocal

María Teresa Bermúdez Muñoz
Fiscal

Alexander Barquero Elizondo
Director Ejecutivo

**COMITÉ ORGANIZADOR
XXX CONGRESO ARCHIVÍSTICO NACIONAL**

Carmen Campos Ramírez

Adolfo Barquero Picado

Ana Lucía Jiménez Monge

Graciela Chaves Ramírez

Ivannia Valverde Guevara

Javier Gómez Jiménez

Marco Calderón Delgado

COMISIÓN EDITORA

Alexander Barquero Elizondo
Archivo Nacional de Costa Rica

Carmen Campos Ramírez
Archivo Nacional de Costa Rica

Luz Alba Chacón León
*Academia de Geografía e Historia
de Costa Rica*

María Teresa Bermúdez Muñoz
*Sección de Archivística, Escuela de Historia, Universidad
de Costa Rica*

Roberto Morales Harley
*Escuela de Filología de la Universidad
de Costa Rica*

TABLA DE CONTENIDO

CONFERENCIA INAUGURAL: ¿Qué es la transformación digital?” Edwin Aguilar Sánchez	8
Legislación informática costarricense aplicada a la gestión de la información Alexander Astorga Monge	17
Política Nacional de Gestión y Conservación de Documentos Alexander Barquero Elizondo y Raquel Umaña Alpizar	32
Ciudades y Territorios Inteligentes: ¿Qué son realmente? Valeria Castro Obando	40
Cultura o cambio organizacional y las características del recurso humano Juan Miguel Castillo Fonseca	53
El valor público en la era digital Luis Antonio Román Hernández	60
El Archivo Digital Nacional (ADN) Natalia Cantillano Mora, Luis Carlo Rojas Mora, Mellany Otárola Sáenz, Evelyn Valerín Alvarado, Sofía Irola Rojas	67
MESA REDONDA: Gestión de riesgos en el entorno digital para la continuidad del negocio Roberto Lemaitre Picado, Randall Barnet Villalobos, Ricardo Villalón Fonseca Moderadora: Carmen Campos Ramírez	92
The Role of the Archivist in Digital Transformation James Doig	112

PRESENTACIÓN

El XXXI Congreso Archivístico Nacional titulado, *“La información: el ADN de la transformación digital”*, promovió la transformación digital en los procesos de trabajo en las instituciones donde laboran las personas participantes a este evento; donde se entiende que la materia prima es la información y el conocimiento tecnológico con un enfoque en las personas funcionarias de las instituciones y las usuarias de los servicios que se ofrecen.

Lo anterior implica considerar la premisa de que una institución inteligente es la consecuencia directa de la transformación digital de su organización, y el objetivo de la institución inteligente es hacer del cliente o usuario, una parte importante del ADN de la organización. Por esa razón, considero que los participantes lograron interiorizar los tres pilares clave de la transformación digital: las personas, la gestión de la información y la comunicación digital.

A lo largo de los tres días, se definió que la transformación digital es la aplicación de capacidades digitales a procesos, productos y servicios con el objetivo de mejorar la eficiencia, el valor para las personas usuarias, gestionar el riesgo y descubrir nuevas oportunidades de generación de ingresos o de potenciar el valor público, obligación permanente para las instituciones que pertenecen al Estado.

De igual manera, y tomando en cuenta las exposiciones, podemos decir que la transformación digital es la integración de tecnología digital en todas las áreas de una institución, cambiando fundamentalmente la forma en que opera y brinda valor a las personas usuarias. Esto, necesariamente supone un cambio cultural que requiere que las organizaciones desafíen constantemente su *“status quo”*, experimenten y se sientan cómodas con el fracaso; y a la vez puede implicar la reelaboración de los productos, servicios, procesos y estrategias mediante el aprovechamiento de las tecnologías.

Es importante destacar que la transformación digital ayuda a una organización a seguir el ritmo a las demandas emergentes de las personas usuarias, manteniéndolas en el futuro; y permite que las instituciones compitan mejor en un entorno económico que cambia constantemente a medida que la tecnología evoluciona; por lo que podemos decir que esta transformación es necesaria para cualquier empresa, organización sin fines de lucro o institución que busque mantener su relevancia y una de propuesta de valor adecuada en el futuro.

En este sentido, la tecnología impulsa la necesidad de la transformación digital y respalda la digitalización de una organización, pero no existe una sola aplicación o tecnología que permita la transformación digital, sino que existen múltiples oportunidades en los procesos clave que una organización debe tener en cuenta para afrontar esa oportunidad de transformación. La computación en la nube, por ejemplo, otorga un acceso más rápido al software y los datos que se necesitan, así como nuevas funcionalidades y actualizaciones para los servicios, y permite que las organizaciones sean lo suficientemente ágiles como para transformarse desde la esencia de su negocio o su propósito; pero es una solución tecnológica con características y costos que no necesariamente aplican para cualquier institución o cualquier producto o servicio.

Un concepto importante que se abordó durante el Congreso fue el tema de la seguridad informática, también conocida como “ciberseguridad”, definiéndose como el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta, muy especialmente la información contenida en las computadoras o que circula a través de las distintas redes de telecomunicaciones. Para su desarrollo, existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información, y las instituciones y las personas a cargo debemos tenerlo presente y aplicarlo a nuestros productos y servicios que dependen cada vez más de las plataformas electrónicas.

Es así como la ciberseguridad comprende software (herramientas y soluciones de todo tipo), hardware, redes de computadoras, y procedimientos de todo tipo que permitan proteger los activos que la organización valore, y que signifique un riesgo si la información que contienen llega a manos de otras personas.

En el contexto general del Congreso, quedó evidenciado que es necesario diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir sistemas informáticos que sean seguros y confiables. Por lo tanto, la seguridad informática está concebida para proteger los activos tecnológicos y de información, entre los que se encuentran: la infraestructura computacional; los usuarios; y la información propia, de clientes, socios y usuarios como principal activo de las organizaciones.

Finalmente, en el congreso se mostraron dos novedosos proyectos en los que trabaja la Dirección General del Archivo Nacional, a saber:

- A. Política Nacional de Archivos: esta propuesta de política se ha llevado a cabo desde el 2017, precisamente en un congreso archivístico, y su objetivo principal es proveer al país de una política nacional para la gestión y conservación de documentos que permita el desarrollo del Sistema Nacional de Archivos.
- B. Archivo Digital Nacional (ADN): servicio tecnológico cuyo objetivo es que Costa Rica en un mediano plazo, cuente con un portal que centralice el acceso y consulta de los documentos que genera la administración pública. Lo anterior, facilitará la toma de decisiones por parte de la administración; promoverá la rendición de cuentas y la transparencia administrativa al proveerle al ciudadano un punto de acceso único y normalizado a la información; y finalmente permitirá resguardar los documentos patrimoniales, fuente indiscutible para la construcción de la memoria histórica y cultural del país.

Para mí, es de gran satisfacción poder presentarles la presente memoria del XXXI Congreso Archivístico 2019, ya que cuenta con las ponencias de las diferentes personas que brindaron su aporte para que el programa diseñado se realizara exitosamente. Mi más sincero agradecimiento a esas personas que desinteresadamente transmitieron sus conocimientos y experiencias, para un público que sin duda alguna agradece y aprovecha su mensaje.

De igual forma, deseo agradecer a todo el equipo del Archivo Nacional, que con mística, compromiso y responsabilidad; organizan año con año tan importante actividad de actualización profesional dirigido a todas las personas que laboran dentro y fuera del Sistema Nacional y Archivos.

Alexander Barquero Elizondo
Director General
Archivo Nacional de Costa Rica





CONFERENCIA INAUGURAL ¿Qué es la transformación digital?"

Edwin Aguilar Sánchez

Máster en Ciencias de la Computación, Universidad de Essex, Inglaterra.

Buenas tardes estimada audiencia. Primero quiero felicitar al Archivo Nacional por estar celebrando este congreso tan importante para el desarrollo de la Archivística, no solo del país, sino que tengo entendido que hay también invitados de países centroamericanos, colegas, compañeros nuestros. En segundo lugar, quiero agradecer el honor que me hacen don Alexander, don Dennis y los miembros de la Junta Administrativa por haberme encomendado tratar esta tarde con ustedes el tema de la transformación digital, que muy acertadamente el lema del congreso pone a la información como el ADN de la transformación digital.

Hay muchas concepciones de la transformación digital. En la investigación que he hecho he encontrado muchísimas definiciones, con diversos enfoques, unos más complejos que otros. Recuerdo, y aquí don Giovanni del Instituto Costarricense de Electricidad (ICE) tal vez podrá confirmarlo, que la institución a principio de año hizo un requerimiento de información a consultores y a empresas de tecnología sobre servicios de transformación digital y entre las cosas que nos preguntaban estaba una: "¿qué es para usted la transformación digital?" Me gustaría conocer todas esas definiciones que los diferentes consultores y empresas de consultoría de Costa Rica le han de haber dado al ICE, porque son muchas las concepciones que hay.

Hoy les voy a presentar mi particular punto de vista y la concepción de este fenómeno que es la transformación digital. Me he basado en grandes teóricos de la administración y de la tecnología, que es como pararse en los hombros de gigantes para venir a hablar aquí de algo tan complejo. Primero, que la transformación digital es un fenómeno que se da dentro de la cuarta Revolución Industrial. Dicha revolución hace posible que lo físico de los procesos industriales, productivos y económicos se fundan con lo biológico, con lo mental y con lo cognitivo.

Esta fusión se da gracias a las potencialidades de la tecnología. Fíjense ustedes que el fenómeno de esta fusión biológico digital uno la puede observar en algo que ocurre en Guanacaste en una finca ganadera, donde a las reses les ponen unos chips en las orejas y esos chips dicen la temperatura, la presión arterial, todas las condiciones que se pueden detectar de su organismo. Por ejemplo: se descubrió que las reses cuando comen mueven las orejas de una forma y cuando toman agua las mueven de otra y cuando están descansando no las mueven.

Entonces de esa manera se puede detectar cuánto está comiendo cada res, cuánto está bebiendo y cómo está su salud. También se puede detectar a cualquiera que esté enferma y en el caso de las reses hembras, determinar en qué momento los cambios de temperatura indican que está en el proceso de ovulación, para inmediatamente localizarla y proceder a la inseminación artificial. Y como esas pajillas de inseminación artificial son muy caras, pues valen \$1,000 cada una, entonces antes se perdían muchos dólares por no saber en qué momento oportuno había que fertilizar a uno de estos animales. Podemos ver en ese ejemplo lo que es la cuarta Revolución Industrial que, como ya lo mencionamos anteriormente, trata de la fusión de lo físico, biológico y lo mental gracias a

las tecnologías digitales. El autor Klaus Schwab es el padre de esta concepción, él es el presidente del Foro Económico Mundial que se reúne en Suiza cada principio de año; esta es la organización económica y política más importante del mundo en términos de revolución tecnológica.

Como lo comenté, esta revolución es un fenómeno económico, social, cultural, político y tecnológico. Voy a hacer un símil para que ustedes vean frente a qué estamos. Esto se nos viene encima como un tsunami, pero en el país hay poca conciencia de eso, qué significa esta revolución que amenaza empresas, empleos, y amenaza la posición del país en la estructura mundial de la producción. Es decir, es como un tsunami que viene, pero que estamos muy ignorantes de eso, no hay mucha conciencia y en eso tienen la gran virtud el ministro Luis Adrián Salazar y Alexander Barquero de haber lanzado una alerta para tomar conciencia de esto: la estrategia de transformación digital del bicentenario 4.0 que necesitaba el país frente a la Cuarta Revolución Industrial.

La Primera Revolución Industrial se dio de la mano del vapor; previo a eso la producción era agropecuaria, minera, pesquera y un poco artesanal. Pero el vapor vino a transformar ese mundo rural y empezó la industria sobre todo textil y amplió el transporte terrestre y marítimo, que a su vez amplió las fronteras, favoreció el comercio y aparecieron las ciudades en sentido moderno.

La Segunda Revolución fue aún más allá con la electricidad. Fíjense que este nuevo elemento transformó la economía, las empresas, los empleos, el transporte y las ciudades. No se trabajaba de noche previo a la electricidad, a las cinco de la tarde terminaba la producción. Con la electricidad empezó la vida nocturna en todos los sentidos, no solo el económico sino también la vida social; las ciudades se transformaron, en eso Costa Rica fue avanzada ya que San José fue la segunda ciudad capital electrificada de América, antes que México, Lima, Santiago, Brasilia y Río de Janeiro.

Ahora ante la Cuarta Revolución Industrial, Costa Rica es el segundo exportador de software de América Latina, solo Brasil nos gana en este tipo de exportaciones. Aquí tenemos a todas las empresas multinacionales de tecnología. Cuando voy a los parques industriales me maravillo de que a pocos metros entro al *International Business Machines Corp.* (IBM), a Amazon o entro a *Hewlett Packard*; es como un *Silicon Valley* aquí en Costa Rica. ¿Por qué están todas esas empresas aquí? Porque aquí hay buenos ingenieros. Eso es lo que a Costa Rica la ha tenido siempre en buena posición frente a las revoluciones; el talento costarricense es de primera, muy capaz, innovador, trabajador, productivo y usa muy bien las tecnologías.

Desafortunadamente, en este momento tenemos una deficiencia de ocho mil ingenieros para mantener el ritmo de crecimiento de esta economía y se nos están yendo muchos negocios para Panamá, Ecuador y Colombia por falta de dichos profesionales. En eso el sistema educativo nuestro marcha atrás, hace falta impulsar mejoras en la enseñanza de matemática, enseñar mejor inglés e incentivar la enseñanza de las ciencias para que los muchachos opten por estudiar ingenierías. Solo el 13% de la población universitaria estudia este tipo de carreras y esa es ahorita la necesidad más grande que hay, que ese talento tico se desarrolle más cuantitativamente porque cualitativamente anda muy bien.

Entonces, así como la Segunda Revolución Industrial transformó realmente la civilización, la Cuarta Revolución también lo va a hacer. Va a transformarnos y hasta dice Klaus Schwab que va a cambiar la concepción del humano; va a empezar, o mejor dicho ya empezó a aparecer, la transhumanidad. Esto se refiere al humano que abandona la evolución natural darwinista (esa que tomó millones de años para generar el lóbulo frontal) y con tecnología e ingeniería genética pretende generar transformaciones ya no evolutivas sino de una generación

a otra y también por medio de tecnología incrementar el promedio de vida. Dicen que al final de este siglo se va a vivir 200 años, el tico ya está cerca de vivir 100 años. Si nosotros vemos, en el año 1950 la esperanza de vida eran 60 años y ahora son 80; con algunos médicos que hemos conversado de esto dicen que si comemos bien, bajamos la ingesta de alcohol y hacemos ejercicio, llegamos a los 100 años. La tecnología no solo va a transformar la civilización, sino hasta la misma humanidad.

Haciendo un breve repaso de lo que ha sido la tecnología, vemos que todo empezó entre los años 1960 y 1980, con los grandes computadores que valían millones de dólares. Aquí en Costa Rica, en los años 60, sólo el Banco Central tenía una, después la Universidad de Costa Rica adquirió otra y eran pocas las computadoras que había de ese tamaño y se dedicaban a automatizar todo lo que era la contabilidad, recursos humanos, planillas, pagos de los trabajadores y los inventarios, entre otros. Luego del año 1980 al 2000 aparecen en el mercado las microcomputadoras, ya no sólo son los grandes computadores que había.

Cuando en el año 1970 al gerente de la IBM le dijeron que si iban a producir una microcomputadora, noten cómo pensaba en ese tiempo que respondió: “¿para qué quiere una computadora la gente en su casa?”. No creyó siquiera que fuera posible tener una de esas en la casa y apareció. Pero entonces las microcomputadoras permitieron que la computación se metiera en la cadena de valor de las empresas, ya no solo en la administración sino que se metieran en el diseño, en las compras con toda la logística de aprovisionamiento que hay en las compras, la manufactura, la distribución, la logística de salida, el mercadeo, las ventas, los servicios post venta, atención al cliente. Ahí se introdujo porque aparecieron las redes (eso fue una maravilla) conectando todas esas microcomputadoras vinculadas con la producción de las empresas en procesos novedosos. Fue tanto así que en esos años apareció la metodología que se llamó “reingeniería de procesos”. Hay un libro de Hammer y Champy que decía “mire, todo lo que usted ha hecho no sirve, empiece de nuevo” y sabemos que eso no se puede en tecnología. Uno no puede decir en una organización “tiremos todo y empecemos de nuevo”; hay que hacer una transformación, conservar lo bueno que tenemos, posicionarnos sobre eso y evolucionar.

Después de esto, aparece a finales del siglo XX el internet y con su presencia se afirmó: “la computadora es la red, ya no es solo un aparato, son todas las comunicaciones”. Y así empezó el comercio electrónico y el internet se volvió una red de información. Con el inicio del siglo XXI aparecen tecnologías de comunicación 2G, pero sobre todo 3G y 4G que hacen que un celular inteligente sea un verdadero computador en la mano que permite el acceso en cualquier momento y lugar por cualquier dispositivo.

Ahora, además de los teléfonos tenemos las tabletas y otros dispositivos para estar con un acceso poderoso no solo a la información, sino a procesos industriales, comerciales y financieros. Internet y la movilidad vinieron a transformar la banca móvil. ¿A quién de ustedes le gusta ir a los bancos? A nadie, porque mejor hacemos la gestión desde el celular. Las transformaciones a las que me refiero vinieron no sólo en los bancos, sino también en las industrias, en las empresas y en el comercio. Se transformó la forma de producir, de comerciar y de relacionarse con los clientes.

Aparecen también los nuevos modelos de negocios digitales. El primero grande e importante fue Google, que con un algoritmo nos dio un servicio gratuito. Nosotros no nos dábamos cuenta de que éramos su producto; nos convertimos en producto de Google porque con su algoritmo nos reunió a todos, se dio cuenta como éramos y entonces se convirtió en una empresa que le vendía mercadeo a otras grandes empresas, que le hacía estudios de mercado y recomendaciones de comportamiento de los clientes.

Tenemos también el ejemplo de Apple. Es otro modelo de negocio exitoso porque aunque hay mejores teléfonos que el *iPhone*, y más baratos, todos queremos uno y pagamos hasta mil dólares por tenerlo y hoy esa empresa tiene un valor de mercado increíble. También está el fenómeno de Amazon. Vean cómo es el modelo de negocio que está causando el cierre de negocios físicos. En Estados Unidos han cerrado muchas cadenas comerciales porque ya no venden lo que vendían, pues Amazon está acaparando todo eso digitalmente. Se diversificó. Empezó con libros, después con música y ahora de todo; yo creo que lo único que no vende son ataúdes.

Por su parte, Facebook está haciendo cosas muy notables pero amenazantes; está alterando la democracia. Ahí hay muchas *fake news* (noticias falsas), intervenciones en procesos electorales; en Estados Unidos sucedió. En las redes sociales lo que hay son emociones y ahora hay algoritmos poderosos para analizar las emociones y se llaman *sentimental análisis*. Se hacen análisis con información que tienen las personas en Twitter, Facebook e Instagram, incluso en WhatsApp. Con estos datos se realizan análisis antropológicos de grupos humanos para saber cómo influir en ellos y eso trae estos grandes conglomerados. Fíjense ustedes que el valor de los datos es el nuevo petróleo, digámoslo así, de la economía digital, es la sangre de la economía digital (los datos y la información). De ahí que quede muy bien puesto el lema de este congreso “El ADN de la transformación digital”.

En la economía digital el valor se crea. Tomen nota en la parte industrial. Cuando estudiábamos economía nos decían que el valor se crea con recursos naturales, capital, trabajo y los factores de la producción. Ahora el valor se crea con datos, información y conocimiento aplicado con tecnología digital y por eso es que el talento costarricense puede crear mucho valor, porque es muy hábil para manejar la tecnología y sabe cómo generar la información o los sistemas de información, cómo obtener conocimiento. Es muy bueno en *videitac*, en *analytics*, en *business intelligence* y todas estas tecnologías que generan conocimiento.

Recién aparece en Alemania el concepto de industria 4.0, es decir la Cuarta Revolución Industrial. Aquí es donde entonces empezamos con que hay distintas concepciones sobre cómo llegar a esa industria 4.0, porque la transformación digital es el fenómeno de cambio de las empresas y es a su vez una estrategia de innovación de negocios. Hay quienes coinciden en que la transformación digital es algo que está en modo manual o analógico para pasar a digitalizar. Pero no es así porque sigue siendo el mismo negocio dentro de la Tercera Revolución Industrial.

Hay quienes dicen “bueno es la transformación de productos y servicios o de procesos y la más acertada para mí”. Es la visión que concibe la transformación digital como la innovación del modelo del negocio. Ya les voy a explicar qué es un modelo del negocio. También se transforman los mercados. Vean ustedes lo que hizo Uber con el mercado, lo que hizo Airbnb con otro mercado; Netflix, por ejemplo, amenaza a las televisoras, a las cableras, en realidad no sólo amenaza el mercado sino una industria completa. Fíjense en el poder que tienen las tecnologías para transformar empresas, mercados e industrias; esa es la Cuarta Revolución Industrial, la transformación de estos niveles y escalas económicas. Ahora se está hablando de “arenas”. El concepto me encanta porque antes se hablaba de industrias: por ejemplo la industria de telecomunicaciones, la bancaria o la del transporte. Ahora la tecnología está juntando todas esas industrias en arenas, ahí están todas interrelacionándose tecnológicamente, haciendo clusters de empresas pertenecientes a diferentes industrias que actúan en la misma arena.

Para caracterizar qué es la industria 4.0 puedo decir que es una organización robusta en investigación científica, que es la base de la innovación. Esta última no es una ocurrencia, es producto de una sólida investigación que nos descubre oportunidades para hacer cambios importantes y desarrollar nuevas cosas. Es una empresa dirigida por datos que son la base de la toma de decisiones en estas compañías. La cadena o red de valor está totalmente

integrada electrónicamente, allí los procesos de aprovisionamiento, de manufactura, de mercadeo y de ventas, están fuertemente integrados con aplicaciones, con comunicaciones y las personas y las cosas también.

Es una integración digital la que tienen, que garantiza una correcta toma de decisiones, detectar problemas en tiempo real. Lo que se busca no es ir viendo el desarrollo por el retrovisor sino determinar qué está pasando en este momento en la empresa en todas las transacciones, las operaciones y las actividades de todos los procesos. Se trata de gerencia en tiempo real, tomar decisiones de las cosas que en ese momento están ocurriendo, incluso algunas se hacen automáticamente, las que son estructuradas, aquellas que cuando se cumple un conjunto finito de condiciones, se dispara una y lo hace de forma automática, por ejemplo, otorgar vacaciones es un proceso administrativo, u otorgar un préstamo, o cambiar la programación de una máquina, entrar en operación una actividad, situaciones que dependen de condiciones finitas para que suceda un proceso. Esa es la parte de un concepto: la autonomía. Hemos oído de autonomía en los vehículos que no necesitan un chofer, pues aquí también la autonomía es eso: decisiones sin intervención humana.

Explicando un poco más a fondo lo que es la transformación digital, hay que aclarar varias cosas. Primero, no está centrada en la tecnología, no es automatizar. No es una planificación estratégica de tecnología, porque esto es controlar la maduración tecnológica de una organización para que alcance la estrategia del negocio. Todo esto es el pensamiento de Michael Porter, de la planificación, de la ventaja competitiva, de que el negocio tal y cómo está, en el mercado que está y a la industria a la que pertenece genera ventajas sobre sus competidores. Eso no es transformación digital.

La transformación digital es que el negocio que está actualmente se transforme en algo que no era, que con la capacidad de las tecnologías digitales pueda hacer mañana algo que no puede hacer hoy. Es un proceso donde desaparece lo obsoleto, la habilidad de descubrir que este negocio ya no va a sobrevivir, entonces vamos a cambiarlo y vamos a hacerlo de nuevo, esto que nos está dando mucha fortaleza vamos a hacerlo más fuerte todavía. Es transformar el negocio, cambiar, madurar; es un proceso de innovación que usa tecnologías disruptivas, tecnologías muy poderosas que fortalecen la propuesta de valor del negocio y mejoran las formas en que el negocio crea valor, entrega valor a sus usuarios y captura valor. Ese es el corazón de la transformación digital: la innovación que fortalece la propuesta de valor del negocio.

Todo negocio tiene una propuesta de valor hacia sus usuarios, hacia sus clientes, en virtud de la cual esos clientes nos dan su dinero o su aprobación y están satisfechos con nosotros porque les sabemos entregar valor. Esa es la propuesta, una innovación que establece y mejora la manera en que ese negocio crea, entrega y captura valor, ya vamos a hablar esto con más detalle para profundizar este concepto.

Esta es la frase que me gusta: “la transformación digital está dirigida por el negocio”, por la junta directiva, por las altas gerencias y está habilitada por las tecnologías digitales. Ahí es donde todos los que trabajamos en tecnología debemos de apoyar el proceso de transformación digital que propone la gente del negocio. Nosotros como gente de tecnología tenemos que saber interpretar y poderles informar de las capacidades de transformación que tienen las tecnologías que son relevantes para un negocio. Aquí vamos a caer en un concepto de esos que se llaman “operacionales” y es “modelo de negocio”. Ahora me voy a referir a él, es una metodología de análisis de un negocio y al mismo tiempo sirve para formular una estrategia de transformación digital. Por esta razón es un concepto operacional, sirve para el análisis y para formular una estrategia de transformación digital.

Como todo modelo es una estructura que representa un fenómeno, un objeto. Así como el modelo de átomo

que nosotros estudiamos en la escuela, ese modelo nos dice que hay un núcleo de protones y neutrones y hay niveles de energía en electrones y con eso nos hace entender un átomo. O, por ejemplo en economía tenemos muchos modelos que prescinden de una serie de detalles. El modelo lo que hace es quitarse los detalles y concentrarse en lo que es esencial. Es decir, los componentes del fenómeno, del objeto; las relaciones que hay entre los componentes, las propiedades de esos componentes para poder entender ese objeto.

Alex Osterwalder creó lo que conocemos como modelo de negocio y lo voy a explicar así: tenemos los componentes agrupados en dos partes, uno frontal y uno trasero. Aquí tenemos tres procesos: se crea, se entrega y se captura el valor. Veamos cómo funcionan estos componentes. Primero aquí tenemos la propuesta de valor y lo principal, dicha propuesta surge de considerar al cliente o al usuario y segmentarlo, no todos nuestros usuarios son iguales, los segmentamos y vemos qué necesitan, qué desean, qué los emociona, qué los incomoda, hasta el punto de abandonar una empresa o de amar a una empresa porque los emociona tanto. Fíjense que aquí vuelvo a Apple, que ha sido muy ingeniosa en manejar este aspecto emocional, esta relación. La gente hace filas desde la madrugada cuando aparece una nueva versión de teléfono, están felices con su aparato, aunque hay mejores; pero no, el *iPhone* emociona.

La propuesta de valor debe emocionar a los clientes, hacerlos sentirse satisfechos, contentos. Ese valor se entrega por canales físicos si se les atiende en una plataforma, o por canales digitales si se les atiende por la web o por el celular o por la radio y ahora se habla de “omnicanalidad”. Quiero explicar estos cuatro componentes del modelo de negocio y su interacción para crear valor.

Voy a referirme a la propuesta de valor de Uber, aquí estamos muy familiarizados con eso, ¿qué nos ofrece Uber? primero seguridad, porque el conductor está controlado por la empresa, pasa un proceso de autorización y evaluación. Yo sé su nombre, puedo ver su perfil y cuántos viajes ha hecho, cómo está calificado y todo eso me da seguridad; es más barato, sé la ruta que va a tomar, no me va a llevar por lugares que no conozco como pasa con un taxi, sé la ruta e incluso sé a qué hora voy a llegar y de antemano sé cuánto me va a costar. Además voy a ir en un auto que huele bien, hasta me preguntan qué música quiero escuchar. Esa es la propuesta de Uber que le permite, por medio de la red, entregarnos ese valor y establecer una relación de confort, una relación emocional favorable para su negocio. De esa manera se crea valor.

Para poder crear este valor dentro de mi empresa, tengo que tener recursos claves que lo van a crear, y en este caso esos recursos no son de la empresa. Fíjense ustedes como captura valor Uber. Los vehículos no les pertenecen, ni tienen necesidad de mantenimiento, ni de planillas, incluso los mapas no son de ellos ni tampoco el pago. Realmente esta es una plataforma tecnológica, cuyo principal recurso es la misma plataforma y el otro componente de acá son las actividades claves. Por ejemplo en el registro ustedes tienen usuarios, y hay que saber bien a qué segmentos pertenecen, si son ciudadanos o si son instituciones, etc.

¿Cuál es la entrega de valor y cómo generan esa entrega? ¿Con qué recursos y con qué actividades claves? Y aquí están los aliados que me ayudan a crear ese valor, los socios, los proveedores esenciales para esto. Aquí tenemos cuánto cuestan los recursos, las actividades, las relaciones con proveedores y tengo mi estructura de costos. Entonces tengo los costos y las ventas, aquí es donde ese valor que he creado se materializa en las ventas y tengo entonces la viabilidad financiera del negocio, entre costos e ingresos. Eso me da la viabilidad financiera, eso se llama capturar valor. En esta parte está la factibilidad del negocio, si el negocio es capaz de entregar este valor para crear valor y capturar valor.

Las tecnologías digitales que son disruptivas, y que hacen posible la transformación, son las siguientes: Inteligencia Artificial, Lenguaje Natural, Aprendizaje Automático y Robótica, Ciencia de Datos: “*Bigdata*”, “*Analytics*”, Minería de Datos, “*Business Intelligence*”, Computación en la Nube (*cloud*) y Virtualización, Movilidad (*mobility*), Redes 5G, Internet de las Cosas (IoT), Drones, PKI, Biométrica, *Cybersec*, *Blockchain*, *iBanking*, *FinTechs*, Redes Sociales y Análisis Antropológico de grupos humanos. Son las que los analistas han dicho que de aquí al 2025 van a ser las decisivas de la transformación digital.

Entre ellas hay integraciones poderosísimas. Por ejemplo lo que es que lo móvil, el internet de las cosas, se juntan en la nube y en la virtualización se genera analítica de datos, minería de datos y se usa inteligencia artificial o lenguaje natural o aprendizaje automático. Entonces toda esta integración es poderosa para la transformación digital de un negocio, y así también la biométrica. En el caso del archivo también es muy importante la tecnología PKI, la ciber seguridad desde luego, *Blockchain* e *Internet Banking* o las *Fin Techs*, o el uso de redes sociales en mercadeo o lo que mencionaba del análisis antropológico en grupos humanos.

Estas otras son más especializadas: Supercomputación, Genómica, Biotecnología, Impresión 3D, Autonomía (vehículos, toma de decisiones, procesos mecánicos), Realidad Virtual y Realidad Aumentada, Imágenes satelitales y Escaneo Topológico LiDAR (*light detection and ranging*). Esta última se refiere a escaneo con aviones para ver qué está pasando en el subsuelo, qué hay ahí y qué se ha descubierto. En Guatemala han descubierto todas las ruinas mayas que hay debajo de la selva y que no se veían.

Sobre todas estas tecnologías recomiendo el artículo “El *software* se está comiendo al mundo”, de Marc Andreessen. Es una muy buena lectura y es cierto, con el *software* se está haciendo de todo. Entonces llegamos a la estrategia. Viendo el análisis del negocio y el concepto de modelo de negocio, puedo establecer una estrategia de transformación digital y digo primero modelar, entender y evaluar mi modelo de negocio actual.

¿Qué valor entrego? ¿Cuál es mi propuesta de valor actual? Esta debería ser una buena estrategia. Lo primero es modelar mi negocio de acuerdo con ese modelo que les he presentado, de componentes, dimensiones y procesos. Posteriormente hay que conocer las potencialidades de las tecnologías digitales que acabo de presentar, ver cuáles de esas tecnologías son relevantes para mi negocio, determinar cuáles de esas me ayudarán a hacer cosas que no puedo hacer ahora y que me van a permitir transformar mi negocio.

Con estas tecnologías hay un ejemplo de concepto de negocio exponencial: Airbnb. Si la empresa se hubiera dedicado a construir hoteles tendría un alcance decimal, crecería con el tiempo a una escala decimal. Pero basados solo en información lograron un alcance exponencial, a nivel global; cada vez hay más ofertas de hospedajes y de gente que quiere rentabilizar una habitación o su casa, solo basado en información. A esto me refiero cuando digo que hay que pensar con las tecnologías y valorar qué transformaciones exponenciales puedo hacer de mi modelo de negocio actual.

Diseñar y evaluar. Voy a diseñar mi modelo de negocio. Digo, por ejemplo: “voy a transformar mi propuesta de valor o voy a incluir mejor a mis usuarios, o las relaciones, los canales o las actividades claves, los recursos claves o mis aliados, con tecnología. Voy a transformar estas cosas para lo que decía Osterwalder: “la transformación digital fortalece la propuesta de valor y mejora las formas de crear valor, de entregar valor, o de capturar valor”.

Puedo tener estas nueve áreas de innovación, empezar con el diseño y el *marketing* que está aquí en la creación de valor, o los productos y servicios que están en mi propuesta de valor, los mercados y los canales que están

en el *frontend*, o la tecnología que está en mis recursos clave, los procesos que están en mis actividades claves, la gestión que es una actividad clave, o el modelo de negocio o la industria. Esas transformaciones se dividen en 3 categorías, porque el tiempo para hacerlas es diferente. Por ejemplo: estas tres se llaman innovación incremental (diseño & *marketing*, productos y servicios) porque el negocio queda un poco mejor y eso se obtiene en un horizonte de dos años.

Hay unas empresas que pueden lograr en un año o dos años la innovación incremental, pero cuando me meto a la innovación de mercados, tecnología y procesos eso es innovación arquitectónica. Incluso la gestión es parte de la arquitectura, eso toma más tiempo, alrededor de cinco años, y cuando hago una transformación disruptiva es cuando estoy cambiando el modelo del negocio, estoy haciendo cambios fundamentales, exponenciales, transformación exponencial y eso puede durar diez años para la transformación digital. Desde luego que esto de un año, dos, cinco o diez es muy relativo al negocio que se está transformando. Habrá algunos en los que se podrá hacer una innovación disruptiva en cinco años.

Después de haber diseñado y evaluado las innovaciones se formula una visión estratégica, su horizonte en el tiempo, la hoja de ruta que van a tener esos cambios, las etapas y los resultados en cada etapa y métricas para ir controlando la transformación. Una vez listos los cambios, hay que ver qué impacto tiene esa transformación en la arquitectura empresarial, es decir, en los procesos, en las aplicaciones, en la infraestructura tecnológica, en los flujos de trabajo y en el apoyo administrativo. Porque eso va a cambiar, y sobre todo en el talento; voy a necesitar talento nuevo, nuevas capacidades organizacionales, tecnológicas de talento y también cambio en la cultura tradicional de la organización.

Esto se toma en cuenta a la hora de evaluar el impacto en la arquitectura empresarial, el talento en la cultura y luego en la gestión del cambio porque hay que saber manejar el cambio, muchas empresas han terminado mal en los procesos pues no los asimilan. Hay que conocer bien las etapas porque el cambio tiene problemas y riesgos empresariales que son los más graves y de mayor impacto, riesgos en la producción, en las operaciones, riesgos tecnológicos, riesgos del ambiente de trabajo, lo emocional, lo cultural, ahí hay muchos riesgos.

El cambio tiene que tener un equipo ejecutivo bien seleccionado, multidisciplinario, con poder. Un equipo ejecutivo que dirige el cambio debe conocer bien de qué trata la transformación que está realizando; deben de tener liderazgo para poder impulsar el cambio, control de riesgos y la incertidumbre. Esta última va a estar ahí en el trasfondo de todo el proceso y se debe combatir con información, con una buena comunicación, porque hay problemas cuando a las personas les dicen “vamos a cambiar”, pero no les explican bien cuál es el cambio.

La incertidumbre les genera miedo, empieza a haber reacciones de oposición al cambio por temor, entonces ese equipo ejecutivo debe ser muy eficiente para saber comunicar de manera efectiva y asertiva. La experiencia dice que nadie apoya lo que no entiende. Si uno no entiende de lo que le están hablando se queda a la expectativa, para ver que se aclaren los nublados del día y ver qué pasa. La comunicación es un elemento muy importante en la gestión del cambio.

Los factores que influyen en la transformación digital son estos: formular una buena estrategia, que exista un fuerte liderazgo, equipo ejecutivo bien seleccionado, bien armado, multidisciplinario, con poder, contar con el talento, enfocarnos en el usuario. La transformación digital debe ser para entregarles valor, para fortalecer nuestra propuesta de valor, para crear en él emociones buenas que afiancen su relación con nosotros, utilizar los canales adecuados, es decir, el *frontend* que veíamos en el modelo de negocio y sus cuatro elementos muy

importantes centrados en el usuario y la cultura, los elementos culturales de la organización, cómo se cuecen las habas en la organización, cómo se matan las pulgas. Todo eso va a cambiar y cuando eso sucede se produce inestabilidad emocional, incertidumbre e inseguridad. Por este motivo la gestión del cambio tiene que tener en la cultura un problema central.

Con esta presentación espero haber contribuido a esclarecer una de las concepciones de la transformación digital, porque hay muchas, pero esta es la mía. Esta es la que me gusta porque tiene una metodología y es el modelo del negocio: desarrollar la transformación sobre la base de un modelo de negocio para fortalecer la propuesta de valor y las formas en que creo, entrego y capturo valor. Es muy importante tener una metodología porque decide las herramientas, los procesos y las etapas. Todo lo decide la metodología y en ciencias se le llama así a una teoría que sirve para la investigación y este es el objeto, que sirva para formular estrategias para crear.

Veamos un último ejemplo. Si pienso que la luz son rayos de luz, esa teoría me va a llevar a investigar la luz con lentes, la refracción y todo viéndolo como tal. Mis instrumentos van a ser apropiados para rayos, porque mi metodología es basada en una teoría de rayos. Pero si pienso que la luz son ondas, son vibraciones, entonces mis herramientas van a ser otras para investigar la luz y los procesos van a ser diferentes y la investigación va a tomar por otro camino.

Por eso es importante establecer bien la metodología de una investigación, para que oriente el camino a seguir y si yo creo que la luz es corpuscular, como dijo Albert Einstein que era, mi metodología va a ser diferente, debido a la teoría planteada. Entonces cuando ustedes escuchen hablar de metodología es eso, una teoría que guía la investigación. Porque a veces se confunde con método, que es diferente porque es un conjunto de pasos; sin embargo, metodología es una teoría para la investigación o para la formulación de estrategias. Entonces mi metodología en transformación digital es el modelo de negocio.

Muchas gracias a todos por la atención que me han brindado y les deseo mucho éxito en este XXXI Congreso del Archivo Nacional.





Legislación informática costarricense aplicada a la gestión de la información

Alexander Astorga Monge

Asesor de la Presidencia Ejecutiva del Instituto Nacional de Aprendizaje (INA)

Buenos días. Mientras corre la presentación, les comento que me alegra mucho estar acá frente a ustedes. Sé que la mayoría de las personas acá son profesionales en el tema de un archivo y que tienen muchísima experiencia en la administración pública. Entonces realmente es todo un honor estar por acá frente a todos ustedes y esperamos que disfruten la presentación.

Como dice el título, la charla trata sobre legislación en materia de informática, pero aplicada a la gestión de información. Entonces en esta presentación no me voy a abocar mucho a repasar temas muy relacionados a archivo puesto que, entiendo, más bien ustedes podrían dar cátedra sobre ese tema. Más bien nos vamos a enfocar en los temas que tienen que ver con una gestión de la información pública; entiendo también que quienes estamos acá, al menos en su mayoría, estamos a diario relacionados con la administración pública. Es así como más que hablar de información a nivel general vamos a hablar de información pública.

Entonces sin más, vamos a comenzar, que no tenemos mucho tiempo y el tema resulta un poco amplio. Tal vez para iniciar, algo que es importante. Debemos tener en cuenta algunos conceptos que son claves en materia de gestión de información; vale decir que en nuestro país dichos conceptos se encuentran tutelados desde la Constitución Política. Esto es un hecho bastante importante porque hacen que en materia de gestión de la información, nuestro país ha tratado el tema de la información como un derecho humano, siguiendo la tendencia internacional. Tanto el acceso como la tutela de la información pertenecen a las personas, lo que se entiende más como el derecho a la intimidad, a la libertad, a la privacidad de las comunicaciones.

Eso es muy importante y valioso puesto que en algunos otros países no se tiene este rango a nivel de la tutela de estos derechos. Ha sido más bien a través de leyes ordinarias y del control de convencionalidad que se ha ido incorporando este tipo de tutela de derechos al ordenamiento jurídico. Control de convencionalidad, para quien no lo tenga claro, es como el ordenamiento jurídico interno de un país, que va cambiando conforme la legislación internacional lo va haciendo. Muchos países han ido incorporando la tutela a estos temas que están acá a través de la vía jurisprudencial; en Costa Rica ya se incorporó desde la Constitución Política. Esto nos dice mucho acerca del enfoque garantista que ha venido manteniendo nuestra constitución y nuestro ordenamiento jurídico.

En materia de jurisprudencia, que en su mayoría es lo relacionado con la Sala Constitucional (aunque también hay otras Salas que se han pronunciado), tenemos jurisprudencia de avanzada en materia de gestión de la información. Esto hace que si tomamos en cuenta todo nuestro ordenamiento jurídico en su conjunto y que somos un país muy respetuoso, tenemos un sistema que es bastante robusto en lo que es el amparo que se da a

la información y también a lo que les decía de la privacidad al derecho, tener privacidad en las conversaciones y comunicaciones. Tomemos en cuenta que en Costa Rica, inclusive, vamos más allá con el tema de los derechos humanos al considerar supra constitucional los derechos humanos cuando están regulados por derecho internacional.

Entre los primeros conceptos para ver está el tema del acceso a la información pública. Nuestro artículo 30, y también el artículo 11. Tradicionalmente cuando se habla de acceso a la información pública está explícitamente regulado en el artículo 30 que dice: “todas las personas tienen libre acceso a los departamentos administrativos para obtener información”. Sin embargo, el artículo 11 incorpora un principio muy interesante que es el de rendición de cuentas y eso hace que de alguna manera el acceso a la información no solamente tiene que ser un derecho reactivo, sino también un derecho que es activo. Las personas deben recibir la información a través de mecanismos de revisión de cuentas y no que sea necesario pedir la información para obtenerla.

Cuando se combinan ambos artículos, 11 y 30, se hace una interpretación más amplia sobre el derecho de acceso a la información que no es meramente que yo tengo derecho a ir y solicitar información con lo que el artículo 30 dice, sino que también la puedo recibir de verdad. Eso es bien importante. Tenemos el secreto de Estado, que es una excepción que se mantiene en el artículo 30 que dice que todas las personas tienen derecho a tener información administrativa de los diferentes departamentos, salvo los secretos de Estado. Analizar esto es bastante complejo, de hecho les puedo compartir luego un artículo que escribí hace un tiempo sobre el secreto de Estado porque resulta ser lo que llamamos un concepto jurídico indeterminado.

Si buscan en la Constitución Política qué es el secreto de Estado no lo van a encontrar y es bastante importante entender qué es porque es lo que nos protege en un Estado democrático como el nuestro de decisiones arbitrarias para ocultarnos información. La jurisprudencia de la Sala Constitucional ha sido bastante esclarecedora para definir qué es. Básicamente es información administrativa que no se puede revelar por motivos ya sea de seguridad nacional o de seguridad de Estado, o bien por temas de relaciones internacionales que afecten estas. Es decir, no son todos los temas, si no los que de alguna manera puedan afectar la seguridad nacional o la seguridad del Estado.

Esto es bastante importante porque han habido casos en donde se le pide información a la Cancillería y se declara secreto de Estado. Y eso es porque de alguna manera se interpreta que esa información podía afectar la seguridad del país en un sentido amplio. Es decir, si pudiéramos entrar en algún tipo de conflicto económico o comercial con un país, esto también podría contar como materia de seguridad. Ahora, la información administrativa que tenga que ver, por ejemplo, con la Cancillería, esa no es secreto de Estado (como el salario de un canciller o de algún embajador). Lo que se considera como tal es lo que pueda poner en detrimento las buenas relaciones del país con otros países o la seguridad como tal del Estado. Eso lo menciono para entender el concepto. Van a ver más adelante que es importante y por qué se relaciona con todo el tema informático y demás. Lo que tenemos es el tema de la privacidad.

La privacidad tiene un sentido bastante amplio en nuestra constitución, en el artículo 23 que inicialmente define “la propiedad privada y la inviolabilidad de esta, salvo por órdenes judiciales la propiedad privada es inviolable”. O sea, nosotros no podemos meternos a la casa de alguien a menos que haya una orden de un juez y que se haga un procedimiento correcto, porque incluso hay allanamientos ilegales; o sea, se tiene que dar de una forma correcta de acuerdo a nuestro Código Procesal Penal, eso es en cuanto a la propiedad privada. Sin embargo, hablamos de que el legislador puede ser ordinario constituyente cuando hace una reforma constitucional.

Nuestro legislador constituyente fue más allá y en el artículo 24, además de hablar de la propiedad privada, incorporó el elemento de privacidad, que es más importante porque la privacidad no solamente habla del ámbito privado sobre bienes materiales como lo es la propiedad, sino también incorpora a lo que llamamos el fuero interno, que es lo que compete más a la persona. Ahí también metemos todo el tema de nuestras comunicaciones, incluso de nuestros pensamientos, hay libertad de pensamiento. Habla también del derecho a tener intimidad y eso está incorporado de forma muy clara en el artículo 24 y si lo ven es bastante largo, son varios párrafos, lo cual nos da un marco bastante robusto en materia de privacidad.

Otra cosa importante es el tema del orden público que resulta ser otro concepto jurídico indeterminado, es bastante difícil definir el orden público y ustedes se podrán encontrar tesis de tesis que tratan de hacerlo; pero el orden público resulta ser la potestad más importante que tiene el Estado para con sus habitantes. Porque si analizamos el artículo 28 que es donde se indica esto, básicamente lo que dice es que todas las acciones que estén fuera del orden público, la moral y las buenas costumbres, están fuera del alcance de la ley.

Y ni nos pongamos a hablar de la moral y las buenas costumbres porque ahí eso es más indeterminado aún. Pero sí podemos hablar del orden público, que realmente está muy relacionado con el tema de la seguridad y de las garantías que se tienen que dar de un Estado de estabilidad a nivel social, que el Estado debe proteger, eso para hablarlo en una forma fácil. Ya les dije que podemos hablar horas sobre el orden público. Para que tengan en cuenta lo que se dice de que todas las acciones que estén fuera del orden público, están fuera del ámbito de la ley. Entonces el Estado tiene como competencia a través de la ley, de alguna manera, propiciar el orden público. Así el Estado, a lo largo de la historia, ha ido generando diversas leyes que amparan el orden público.

Esas leyes son de diversa índole, pero si algo tienen en común es que no se meten en el ámbito privado de las personas, a menos que haya una afectación al orden público. En este punto les doy un ejemplo: en la vida privada uno puede ver televisión, ir al cine, puede hacer lo que sea, la ley no te puede decir cómo ir al cine o cómo ver televisión, eso está fuera del ámbito de la ley, porque es la vida privada y si saliera una ley mañana que dice: “ahora las personas solo pueden ver películas cómicas en los cines”, esa ley sería inconstitucional porque esa acción que es privada, está fuera del ámbito de la ley, a menos que se vaya al cine a causar un estrago. Ahí ya estaría afectando el orden público y eso sí estaría en el ámbito de la ley.

Ahora bien, ¿qué es lo que pasa cuando hay alguna acción que es privada en esencia? como por ejemplo la forma en que yo manejo mi correo electrónico, para ya irnos metiendo un poco más en la información que tiene que ver con el derecho informático y con el tema de gestión de la información. Imaginemos nuestro correo electrónico que es sumamente privado, inclusive en Costa Rica, y por eso les decía que hay jurisprudencia de otras Salas que también tienen que ver, no solo la Sala Constitucional.

El correo es tan privado que ni siquiera en materia laboral se puede acceder al de una persona, aunque diga el empresario “el correo lo costeo yo, yo pago el servidor de correo electrónico a mi funcionario, entonces, ¿por qué me dicen que es privado?”. Bueno, lo es porque la Sala Segunda ha ratificado votos de la Sala Constitucional donde indican que eso pertenece al ámbito privado de la persona. Ya mencionamos que el correo electrónico es privado, pero recordemos que la ley sí tiene dentro de su ámbito todo aquello que pueda ir en contra del orden público. Qué pasa si en mi correo electrónico a través de un procedimiento judicial penal, hay un caso formulado, donde posiblemente yo he mantenido comunicaciones y he utilizado mi correo para actividades fraudulentas, para cometer algún delito o pagué una cosa. Ahí entra el ámbito de acción del Estado que de alguna manera tiene la potestad de intervenir en el ámbito privado para salvaguardar el orden público.

No sé si les queda claro o estoy siendo un poco enredado con esto. Es decir, con una orden de un juez se podría intervenir el correo electrónico de una persona, pese a que sea del ámbito privado, para salvaguardar el orden público. Eso más que todo para tenerlo claro. Estos conceptos son básicos, pero muy importantes porque todo el derecho informático que hay en este país está montado sobre estos pilares; por eso quería repasarlos.

Ahora vamos a hablar un poco más del tema de acceso a información pública. En este hay un primer aspecto a tomar en cuenta y es que no me explica a nivel general qué es información pública. En eso, ya que ustedes son los expertos en la ley de Archivo, el artículo 8 de la Ley del Sistema Nacional de Archivos define cuáles son los documentos que son considerados documentos administrativos. Así que cuando hablamos de información pública es básicamente toda aquella información que de alguna manera compete al interés público, a la administración, y tiene que ver con el quehacer estatal. No es lo mismo información a nivel general donde se incluye la información, todas las bases de datos que hay en todo lado, en los foros de internet todo tipo de cosas que tienen bases de datos... No es lo mismo esa información a nivel general que la información pública que es gestionada por el Estado.

Eso nos lleva a esa información administrativa. Es como me gusta llamarle porque tiene que ver con toda la información que se produce en el quehacer institucional. Ahí sí la Ley de Archivo habla de documentos; no habla de información. Entonces es una actualización interesante hablar de información para estar un poquito más a la vanguardia y con lo que estamos viviendo hoy. Sin embargo, el tratamiento que se le da a nivel de archivo y todo, sí es de información pública más que de documentación pública. Eso es bien importante. Más adelante hablamos del interés público; que es también importante en la información, que haya un interés público en lo que está ahí.

Ahora bien, ¿qué pasa con los borradores? Hay un tema también de que muchas veces se filtran borradores y llegan funcionarios y dicen: “sí, pero es que eso no estaba terminado, alguien me lo quitó o se fue y no sé cómo salió y se filtró y eso no era correcto”. Entonces alguien podría decir “sí pero todo lo que usted hace es público”. No es tan cierto; no existe un derecho de acceso a los borradores porque de alguna manera se entiende que estos son parte de ese proceso en el que estamos llegando a un producto que al final sí va a ser de interés administrativo y de interés público. Pero que esté en proceso es parte del fuero interno de la persona, eso es un pensamiento que lo está plasmando y está tratando de crear algo que a la postre sí va a crear intereses.

Hay una ley que es la que regula el derecho de petición. Se hace una solicitud formal de un borrador y esos normalmente la Sala no los acepta; el tema es que los borradores siguen estando en el ámbito privado. Luego viene el derecho de petición, como decía. Hay una ley que regula ese derecho, esa ley establece los plazos en que la información se debe dar. Esto es bastante importante en materia de la gestión de la información, porque de alguna manera la buena práctica en esta materia tiene que permitir la realización de consultas, el poder tener la información en forma rápida para poder así realmente proteger o amparar el derecho de acceso a la información que tiene la gente.

Sí, tenemos un sistema de gestión de información que es híper ortodoxo, que no podemos realmente ni nosotros mismos, como funcionarios, obtener información rápida. Entonces si una persona, necesita información para una gestión o porque es su derecho y nosotros duramos dos años en darle la información. Realmente no estamos garantizando de la mejor manera el derecho de acceso a la información que tienen las personas. De ahí que la ley que regula el derecho de petición sea una buena guía para determinar cuáles son los plazos que se tienen que respetar para otorgar la información y que nuestros sistemas de gestión de información puedan responder

a sus plazos.

Luego hablamos sobre qué es privacidad, que ya vimos que está tutelada en el artículo 24 de nuestra constitución. Acá hablamos de un concepto que es el fuero interno; es decir, que todavía está en nuestro pensamiento. Es de alguna manera lo que utilizamos para poder llegar a expresar a futuro una voluntad y una vez que expresamos una idea ya eso es el fuero externo. El interno está completamente amparado en nuestra constitución y aunque ustedes digan “bueno no, ¿cómo se van a meter con el pensamiento de uno?”. El pensamiento son nuestras ideas políticas o religiosas, lo que pensamos sobre determinados temas eso es parte de nuestro fuero interno y hasta que no las expresemos están fuera del ámbito de protección.

Puedo tener algunas ideas que son muy mías, pero que cuando las expreso estoy ofendiendo a mucha gente, ahí entra el ámbito de la ley. Estamos hablando de que podríamos estar difamando a una persona o estar causando alguna otra ofensa, incluso peor. Hasta podríamos incitar a que se cometa un delito o una cosa así, ahí está dentro del ámbito de la ley; pero mientras esté dentro de, nadie se va a meter con eso.

Aunque suene extraño, hay tendencias totalitarias que en un pasado han buscado meterse hasta con estos temas y por esto es importante que nuestra constitución lo ampare. Este tipo de cosas, aunque parezcan básicas, son las que nos protegen de no caer en Estados totalitarios como en la Edad Media o en algunas otras épocas. Esto es un avance muy importante y por eso es válido hacer hincapié en conquistas de este tipo.

¿Cuándo puede el Estado meterse en la privacidad de las personas? Eso ya se los había adelantado. Básicamente, puede hacerlo cuando de alguna manera se pueda ver en riesgo el orden público. Esa es como la respuesta fácil, una orden judicial de que alguna persona pudo cometer algún delito, entonces hay un allanamiento, se interviene la privacidad de la persona para poder avanzar con un caso y demás, pero siempre con una orden judicial. Luego, también hay que tomar en cuenta el artículo 24 (que sería bueno que se lo lean o puede ser que ya lo conozcan). Sin embargo, existen ciertas reservas; hay una reserva de ley que se hace a Hacienda y a la Contraloría General de la República para que en materia de auditoría puedan obtener cierta información que puede ser del ámbito privado de la persona. Por ejemplo: algunos funcionarios tienen que rendir una declaración a la Contraloría General de la República.

Por ley eso está amparado en la Constitución Política en que existe esa reserva y por la Ley contra la Corrupción y Enriquecimiento Ilícito se genera un artículo que dice que los funcionarios tienen que rendir una declaración ante la Contraloría. Es por esto, porque la Constitución Política le otorgó esa reserva. Eso en cuanto a leyes que tengan que ver con el Ministerio de Hacienda y con la Contraloría.

También está el caso de la reserva de ley mediante leyes especiales, que es bastante valioso que lo tomen en cuenta. Como les dije, el orden público está dentro del ámbito de la ley y es lo que al Estado le corresponde regular a través de las leyes ordinarias. ¿Puede un legislador, o sea la Asamblea Legislativa, hacer cualquier cosa que afecte el orden público y entonces el Estado puede invadir la privacidad de las personas? En realidad no es así, porque tienen que ser leyes especiales y tiene que estar bien fundamentado el por qué en ciertas situaciones el Estado puede llegar y entrar en la privacidad de la persona.

Por eso en la Constitución Política hay un requisito especial para estas leyes y es que se tienen que aprobar por mayoría calificada. No es una ley que se aprueba por una simple mayoría sino que tiene que haber mayoría calificada para que esas leyes se pueden aprobar. Ahí es cuando se puede de alguna manera entrar a solicitar

información, inclusive obtener información por la fuerza de ser necesario, cuando el orden público se vea en riesgo.

También el mismo artículo 24 habla de que cualquier información que sea obtenida por mecanismos ilegales, va a ser una prueba espuria; es decir no va a ser información que se puede utilizar en un proceso judicial. Esto es bastante valioso, porque hay muchos casos que se caen por esto: si en una investigación penal y por alguna razón el fiscal logró grabar una conversación, llegó y presentó la conversación y el juez le dice “esa prueba no fue obtenida por los mecanismos correctos, no se la acepto”.

Esas son las famosas pruebas espurias y están con amparo constitucional. Puede haber una ley que diga que no, que ahora cualquier información que se obtenga va a servir para un juicio, no sería constitucional, tendrían que reformar la constitución y esto es súper importante para el país. Lo digo de nuevo, suena muy lógico, muy común para nosotros; pero no todos los países lo tienen. Por ejemplo, en Estados Unidos hay leyes antiterrorismo que se brincan cualquier proceso y sin orden judicial ni nada llegaban y le se metían en una conversación privada. Este fue el famoso caso de ya hace unos años que se dio en el gobierno de Barack Obama y que lo denunció Edward Snowden. Algo como eso sería completamente inconstitucional en este país y es un logro importante en nuestro sistema democrático, para que lo tengan en cuenta.

Luego, llegamos a tener la Ley 8968, que es la de protección de la persona frente al tratamiento de sus datos personales. Esta ley realmente es un avance bastante importante, no solo por el hecho de que nos permite de alguna manera sancionar a quien no hace una correcta gestión de datos personales; también nos ayuda a contar con una serie de definiciones que hasta la entrada en vigencia de esa ley no se tenían tan claras o estaba en una forma muy dispersa en otras leyes o en otros decretos, o en un montón de normativas por ahí que estaba atomizada.

La ley sí nos da un marco de referencia bastante importante para poder entender qué son los datos personales: es cualquier dato que pueda ser atribuible a una persona. Los hay de diferentes categorías, están los datos que son de acceso irrestricto, son datos que se pueden obtener libremente. Por ejemplo, está la base de datos del Tribunal Supremo de Elecciones, uno puede entrar a la página descarga el padrón y ahí están los números de cédula, los nombres y los distritos electorales de las personas. Son datos que de acceso libre, de acceso irrestricto.

Ahora hablemos de los datos de acceso restringido. Son ciertos datos de carácter privado que se otorgan cuando hacemos un trámite y damos información de nuestra dirección, número de teléfono, número de cédula (aunque sea irrestricto pero lo damos ahí). En esos casos facilitamos una serie de información que es privada y de acceso restringido; uno no la puede obtener así como así. Luego está otro concepto que es bien valioso y que no se maneja; es el tema del dato sensible. Este es bastante importante porque es un dato que por algún motivo en específico yo como persona tengo el derecho de no darlo, ya que es muy íntimo. Aquí puedo incluir mi preferencia sexual, mi religión, mi filiación política, mis opiniones políticas o cualquier otra información que de alguna manera yo sienta que darla conllevaría un detrimento de mi dignidad; eso es un dato sensible.

Aquí se incluye también toda aquella información que tiene que ver con la salud de la persona, como ciertos aspectos que son sumamente íntimos. Eso representa un avance porque hay cierta información que se solía pedir y que la persona se sentía incómoda cuando se la solicitaban y no había nada que la protegiera de eso; no al menos en una ley y no de forma tan específica. Por ejemplo, ciertas preguntas en una entrevista de trabajo como: si tiene algún tipo de enfermedad de transmisión sexual, si tiene una pareja estable, si mantiene relaciones

sexuales. Esas preguntas en algún momento en este país se hicieron y son datos sensibles, no se pueden pedir.

Estas se pueden llegar a solicitar cuando por algún motivo se necesite para dar un servicio o para alguna gestión legal y que sea requisito, no es lo mismo preguntarle a una persona si padece alguna enfermedad en una entrevista de trabajo, que preguntárselo en una ventanilla de la Caja Costarricense del Seguro Social (CCSS). Obviamente la Caja necesita esa información, para su quehacer diario; ahí se puede preguntar este tipo de información sensible.

Tiene que haber una sana crítica y un sentido común que se tiene que aplicar de cuándo se requiere la información y también una justificación técnica de por qué se requiere y cuándo. Puede ser que al momento de ir a sacar la cita no tenga que darle todo mi historial clínico a una persona, mis padecimientos y si tomo o no tomo alcohol, si consumo drogas o no. Eso no se lo tengo que dar a la persona de la ventanilla pero sí se lo tengo que dar a la persona que me está atendiendo, al doctor o a la doctora. También eso aplica en materia de datos sensibles y por qué son importantes esos datos; porque si bien es información que la persona puede reservarse cuando darla, es información que sí se acumula en bases de datos y eso conlleva a un manejo muy estricto. A la postre podría llegar al archivo; es decir, podría estar en registros de la institución.

Es verdad que pasa. Si, por ejemplo, hubiera una filtración de la base de datos de la CCSS que no solamente es de números de cédula, direcciones y datos por el estilo, sino también una filtración del historial clínico de las personas. En eso habría una completa invasión a la privacidad de las personas. Además, el tema se puede prestar para comercio ilícito, que entra en materia de derecho informático, las famosas listas o bases de datos que se venden en el mercado negro. Todo ese tipo de cosas se puede evitar si hay una gestión correcta de la información, veraz, que ampare estos derechos que estamos viendo. Estos no son los derechos, pero son mecanismos por los que se tutelan derechos.

Tenemos otro principio que está en la ley 8968 que es la auto determinación informativa. Es fácil entenderlo; básicamente es lo siguiente: doy la información que yo quiero dar. Si me preguntan el número de teléfono y no lo quiero dar, pues no lo hago, ya que tengo el derecho de auto determinar qué información doy y cuál no. Pueda ser que el número de teléfono sea requisito para realizar un trámite, obviamente si yo entiendo las consecuencias de que al no darlo no se puede proceder con el trámite, estoy en todo el derecho a hacerlo y no me pueden obligar. En un caso así, obviamente no podría hacer el trámite, pero puedo expresar mi voluntad en ese sentido.

La auto determinación informativa es bien importante porque no solo es para decidir sobre qué datos entrego, sino también para decidir qué información mantengo en una base de datos. Puede ser que hoy fui al banco y di el número de teléfono mío, o el de mi casa o trabajo, el de todo lado; pero resulta que en el banco me llaman cada cinco minutos para ofrecirme tarjetas de crédito y todo lo demás y ya estoy cansado. Entonces tengo mi derecho de ir y decir al banco y expresar que quiero que dejen solo el número celular, que es realmente el personal. Puedo hacerlo, a eso se le llama derecho de revocatoria; puedo revocar los datos que ya tengo en una base de datos determinada.

Para que se entienda que el hecho de haber dado un dato una vez, no quiere decir que sea perpetuo y que ya el dueño del dato es a quien se lo di. El dueño sigo siendo yo como persona; es mi dato y está asociado a mí y tengo el derecho de hacer lo que yo quiera con él. Eso es bien necesario entenderlo, porque muchas veces se cree que el hecho de que una institución sea dueña de la información implica que es dueña de los datos contenidos en ella.

En materia de gestión pública manejamos muchas bases de datos y se dice que la institución es dueña de esa información, ya sea la CCSS, el Ministerio de Trabajo o la Presidencia de la República, quien sea. Pero la institución no es dueña de cada dato que está ahí, esos datos le pertenecen a la persona y esta puede llegar a decir “no ya no quiero que me almacenen ese dato” y las instituciones tienen que estar en la capacidad de poder hacer valer ese derecho.

Hablemos de las excepciones; muchas de ellas ya las comenté antes. Está todo el tema de seguridad. Es importante que vean esas excepciones incluso por la auto determinación informativa; o sea, si por motivo de seguridad se requiere tener un dato, este se va a almacenar y hay un permiso legal que se da para poder tener información, porque es una excepción.

Hablemos de la prestación adecuada de servicios, puede ser que la persona llega y dice: “no quiero que mi registro esté ahí”. Y entonces se le explica que si no lo está, no se le puede dar un servicio que es público y es necesario y esto puede afectar a su familia.

En la prestación adecuada de servicios, caso de ejemplo Sistema Nacional de Información y Registro Único de Beneficiarios del Estado (Sinirube), es una base de datos que acumula información de carácter social de las personas. Ahí está todo el registro de beneficiarios y sobre esa información Sinirube tiene la potestad, primero de poderla consumir, de determinadas bases de datos. Ahí está la CCSS, el Ministerio de Trabajo, el Instituto Mixto de Ayuda Social (Imas) y el Instituto Nacional de Aprendizaje (INA). Doy este ejemplo en parte porque forma parte del sector social, que es donde he trabajado.

Eso tiene que ver mucho con el quehacer de ustedes de la información que se acumula con fines estadísticos, históricos o de investigación científica y acá es donde hablamos de los datos anonimizados o la información no individualizada. Es la información en bloque que se tiene ahí, que de alguna manera se puede gestionar, se puede compartir, pero siempre y cuando sea en estas condiciones. Por ejemplo el Instituto Nacional de Estadística y Censos, la información que acumula la Universidad de Costa Rica en los estudios que hace, esto es información científica que se acumula y se mantiene de forma anónima no individualizada.

En el campo de la autodeterminación informativa se manejan ciertas excepciones. Imagínense participar en un estudio de opinión que hace la UCR y mañana decir “no quiero que mi dato esté ahí, ni mi opinión”. Eso conllevaría a un detrimento de un estudio científico que se estaba haciendo, máxime si ya el estudio estaba publicado. Entonces es bastante lógico mantener esta excepción.

Les hablaba del interés público. Ahí me disculparán el texto en las presentaciones, no me gusta usar mucho texto, pero sí me pareció necesario poder leerles algunos datos de acá. Cuando se pone en una balanza el ámbito privado versus cualquier otra cosa, entonces el ámbito privado pierde. Hay situaciones muy específicas y de nuevo surge la pregunta ¿qué es el interés público? Entonces esta jurisprudencia que tengo acá, nos ayuda bastante a entender en materia de gestión de información cuando prevalece el interés público.

Esto es una sentencia sobre una información que se le solicitó al Banco Hipotecario de la Vivienda y esa información se negó por razones de que había datos privados ahí. Se interpuso un Recurso de Amparo y la Sala Constitucional le dio la razón a la persona de que esos datos se tenían que dar por un tema de interés público.

Dice lo siguiente: *“Si bien el Gerente de la entidad bancaria recurrida, indica en su informe que la solicitud realizada por*

la co-recurrente (...) se rechazó en forma parcial, debido a que parte de la información solicitada se encuentra protegida por el artículo 24 de la Constitución Política, al contener datos personales de aquellas personas beneficiadas con el bono de la vivienda, para este tribunal la información solicitada es de interés público, al tratarse de información concerniente a la forma en que son invertidos gran parte de los fondos que aporta el Fondo de Desarrollo Social y Asignaciones Familiares (FODESAF) – 33% de todos sus ingresos anuales ordinarios y extraordinarios - ,al Fondo de Subsidios para la Vivienda (FOSUVI) que administra el Banco Hipotecario de la Vivienda. Tal y como apuntan los co-recurrentes, parte de los recursos de FODESAF provienen del recargo de cinco por ciento aplicado sobre el total de sueldos y salarios que los patronos públicos y privados pagan mensualmente a sus trabajadores. Por ello, siendo que los fondos del programa que administra el Banco Hipotecario de la Vivienda constituyen fondos públicos, existe un interés de la colectividad de conocer sobre la forma en que los mismos son utilizados y la forma en que son desarrollados los planes y programas de contenido social que con ellos se financian. Por todo lo anterior se procede a declarar con lugar el presente recurso...”

Creo que queda bastante claro. Si hay información que estamos administrando que es de interés colectivo y que hay una justificante de ese interés, esa información es pública, incluidas listas de beneficiarios que se financian con fondos público. Dicha lista es de interés público porque yo podría querer comprobar como ciudadano que si a una persona se le está dando un bono o se le está dando una beca o cualquier ayuda económica de los programas sociales, que esa persona efectivamente sea merecedora de este beneficio. Según la ley, digamos la ley del Fondo de Desarrollo y Asignaciones Familiares (Fodesaf), los recursos son para población en condición de pobreza o pobreza extrema.

Como ciudadanos tenemos el derecho de verificar que efectivamente la persona que recibe un subsidio está en pobreza o en pobreza extrema. De lo contrario se estarían utilizando recursos que se financian de mi plata para algo que no debe ser. Es un derecho, hay un interés público en esa información y por ende se puede dar. Este dato no está exento de polémica. Muchas veces se indica que no, que esa información no se puede facilitar y solo se podría dar anonimizado, lo cual no es cierto puesto que la Sala Constitucional se ha pronunciado. Aunque no lo crean, esto es una polémica de todos los días, realmente cuesta que se interiorice y se acepte.

Es un poco más sencillo cuando hablan de los salarios de nosotros los funcionarios. Ahí todo el mundo quiere que los den y sí los pueden dar y no tienen que estar anonimizados ni nada porque también es derecho de una persona ciudadana poder verificar que el salario que recibe un funcionario o funcionaria realmente sea acorde a sus atestados, a su conocimiento, a la experiencia que tiene, que no sea que le estén pagando un plus. Todo eso es verificable y es de libre acceso si la persona solicita esa información. Eso es para tener claro todo el tema del acceso a la información, interés público y demás.

Ahora ustedes me dirán “¿Qué tiene que ver todo que está hablando Alex con el derecho informático? y ¿qué tiene que ver con la gestión de la información?” Preparé este gráfico acá porque de alguna manera explica cómo nosotros tenemos que gestionar la información.

Primero hablamos de información a nivel general. Como estamos hablando de gestión de la información pública, entonces toda la información que no tenga que ver con eso, básicamente no tenemos por qué guardarla; no tenemos que gestionarla, a menos que de alguna manera sea relevante para alguna cuestión. Primero tenemos la información general, luego viene la información administrativa que es la que gestionamos día con día, luego tenemos que cuando nos hacen una solicitud o cuando algo pasa, hay que tener mucho cuidado con la información privada que es administrada por entes públicos. Es información que nosotros administramos así que no la podemos dar así como así; tenemos que resguardarla, que cuidarla. También hablamos del secreto de

Estado, que es otro anillo que protege esa información, hay prohibiciones legales para darla.

Por último, tenemos la información que ya es pública. Esa no es que la tenemos que cuidar menos pero sabemos que es de libre acceso, que nosotros inclusive para propiciar la transparencia en nuestros sistemas de información y podríamos tenerla ahí libremente para que pueda ser consultada. Es importante tener eso claro, ya que es muy común que como funcionarios nos soliciten información. Podemos recibir una solicitud que diga: “en apego al artículo 30 de la Constitución Política le solicito que me de todos los registros de los proyectos que se han manejado”. Está bien, tenemos que dar la información; pero al suministrar lo que probablemente esté en sistemas informáticos, tenemos que cuidar el no dar información de datos personales, secreto de las comunicaciones, intimidad, velo societario o secreto comercial.

Es importante cuidarnos de no estar dando información privada de las personas, o de empresas. De lo contrario, nos meteremos un problema porque todo esto, vamos a ver después, tiene consecuencias. La ley sobre delitos informáticos, que se aprobó hace algunos años, lo que hizo fue incorporar algunas modificaciones en el Código Penal, disponer de un título de delitos informáticos y también hacer algunas modificaciones en el título de delitos contra la intimidad. El bien jurídico de esos delitos son estos temas que hemos estado analizando: la intimidad, el secreto comercial y algunas otras cosas que están por ahí. Como funcionarios, es bien importante tener esto claro para que no nos metamos en un problema.

Me permití acuñar un pequeño párrafo de lo que es una adecuada gestión de la información (esto es a nivel legal, porque a nivel informático hay una serie de criterios técnicos de cómo se tiene que administrar correctamente una base de datos para resguardar la información). El párrafo es el siguiente: *“Una gestión adecuada de la información por parte del Estado es aquella que resguarda adecuadamente la información y permite su uso de forma eficiente y eficaz para los fines por los cuales se recabó y para mejorar los servicios que se ofrecen y la seguridad del país, al tiempo que se garantizan los derechos de las personas”*.

Ahí está de alguna manera acuñado todo lo que hemos visto, porque hablar de resguardar adecuadamente la información, que no permita filtraciones, que tenga los controles adecuados para que no roben la información, que esté blindada lo más posible y eso habla de un resguardo. A nivel legal se habla mucho de un concepto que no me gusta, que es el de cuidar como buen padre de familia. Se oye mucho; es un concepto que viene desde el derecho romano, que es un derecho súper patriarcal.

No es cuidarlo como buen padre sino cuidarlo como si fuera nuestros ojos, o si es como padre, que sea también como madre de familia, de hecho las mamás cuidan mejor a los hijos y eso porque no hay una corresponsabilidad del cuido como debería ser. Pero el tema es que sí tenemos que resguardar y proteger la información ante cualquier eventualidad que pueda poner en detrimento ya sea la seguridad del país, los derechos de las personas, el orden público y todos los conceptos que hemos venido hablando. Eso es el resguardo, es una palabra gigantesca que de verdad conlleva muchísima responsabilidad de parte del Estado. El hecho de no resguardar correctamente la información conlleva responsabilidad civil, penal y administrativa, entonces es todo un tema, no es una palabra menor.

Ahora pues, hablamos de permitir el uso eficiente y es que muchas veces caemos por todos esos temas legales en toda una contradicción de que queremos resguardar tanto la información, protegerla tanto que no la utilizamos. Tampoco es eso, tiene que haber un balance entre ese resguardo adecuado; pero también que la información se utilice. Esto aplica, por ejemplo, para tomar decisiones inteligentes en materia política pública. Ahí hablamos

de conceptos como Big data, como minería de datos (que están tan en boga el día de hoy). Incluso, me parece que ayer conversaron un poco de eso con todo el tema de transformación digital.

Y no es que por resguardar la información vamos a hacer el nudo para que se dé la transformación digital. Todo lo contrario; más bien es poder tener los controles adecuados y más ahora con los avances tecnológicos para que esa información se puede utilizar de forma eficaz. Por ejemplo, unificar bases de datos, la interoperabilidad. Todo eso, siempre y cuando se respeten los conceptos que vimos acá, se puede hacer sin ningún problema. Muchas veces cuesta cambiar ese chip, no es que la información no la podemos dar porque es privada y si no me ponen una demanda, me hacen un problema y no quiero estar en la cárcel. No es eso, es realmente saber usarla de forma eficiente.

Con interoperabilidad se puede lograr mucho de eso. Si son bases de datos que están seguras, que tienen los controles que resguardan bien la información, que están interoperando entre sí, se pueden tomar decisiones muchísimo más inteligentes. Un claro ejemplo, de nuevo, es Sinirube. Todavía lo estamos implementando, pero lo que busca es que exista una única base de datos que integre todas las que tienen instituciones del sector social para que se tomen decisiones más inteligentes y para eliminar duplicidad.

Antes pasaba que una persona quería un bono de vivienda, iba por el bono y le hacían un estudio socioeconómico; la familia quería una beca para los hijos entonces iba al IMAS y le hacían otro estudio socioeconómico. Después pasaban unos tres o cuatro años y van al Ministerio de Trabajo por un programa como Empléate y les hacían otro estudio socioeconómico. Así en un lapso de cinco o seis años les hacían cuatro estudios socioeconómicos, cuando se pudo haber hecho solo uno. Juzguen si no es eficiente unificar las bases de datos, hacer un único estudio socioeconómico y no estar pasando a las personas por ese trámite engorroso a cada rato.

¿Qué es lo que se hace? el Imas hace una ficha de estudio socioeconómico (FIS), que tiene vigencia por siete años. Esa información queda integrada dentro de Sinirube como un registro único y de esa manera eliminamos tanta duplicidad y somos más eficientes. Eso se puede hacer, resguardar la información correctamente, proteger la privacidad de la gente, proteger temas importantes que pueden afectar la seguridad del Estado. Todo eso se hace pero también somos eficientes, que una cosa no excluya a la otra. Por eso hablo acá de ese tema, de cumplir para los fines para los cuales se recabó o para mejorar los servicios.

También tenemos el tema de garantizar los derechos. De alguna manera en estas tres líneas traté de incluir todo lo que vimos hasta este momento. Ya estamos finalizando, pero hay un par de cositas más, también en el ámbito del derecho privado. Tiene que haber gestión adecuada de la información, máxime que la ley de protección de la persona frente al tratamiento de sus datos, no es solamente para el ámbito público, es también para el ámbito privado.

En algunos temas la información es general. Digo general porque no es solo pública, también puede ser restringida o sensible. Nos vamos a topar con ella todos los días; tanto como funcionarios como en nuestra vida privada nos la van a pedir. Si vamos al banco, lo que sea. Un ejemplo, soy tan “*freaky*” con este tema que no lleno rifas en las estaciones de servicio, porque sé que esos datos que uno llena terminan en el mercado negro de bases de datos y ese tipo de cosas, aunque no lo digo como una aseveración.

Eso es un riesgo que se tiene. Yo no firmo ahí por mis datos si no hay un consentimiento informado. No me están diciendo cómo se van a usar los datos, cómo se van a almacenar, qué va a pasar con ellos, es completamente

inseguro, más allá de que terminen o no ahí. Lo que sí es un hecho es que si no se está cumpliendo con todos los requisitos para pedirme esa información, entonces no la doy. No sé si ustedes la darán, les aconsejo que no lo hagan... de por sí difícilmente me pego una rifa yo.

Cuando hablamos de datos personales, hablamos de que hay un amparo constitucional al secreto de las comunicaciones y también a la intimidad. Eso siempre lo tenemos que tener clarísimo. Aquí estamos haciendo un repaso de esa parte, pero luego, del lado de las empresas hay un tema, y es que mucha de esta información tiene un valor comercial. Nos referimos al famoso velo societario que es otro concepto jurídico indeterminado. Ya he hablado como de cinco, pero este es otro que está ahí y que a través de la jurisprudencia y la doctrina se ha ido desarrollando; se ampara en el Código de Comercio. Se refiere a que cuando hay una sociedad anónima o una sociedad de responsabilidad limitada, quien responde es la persona jurídica no la física.

Se entiende que las personas que forman parte de esa sociedad están protegidas y eso es el velo societario, esa es información privada. Entonces ¿qué pasaría si el Registro Nacional tiene una filtración y se revelan todos los socios de todas las sociedades del país? Bueno, como esa información es de carácter privado, eso conllevaría a una filtración bastante importante e ilegal y habría que esperar todas las acciones legales de esas empresas contra el Registro. Eso es el velo societario información privada que una sociedad no está obligada a dar; lo que está obligada a facilitar es su representante legal y ciertas características, pero no el tema de la totalidad de sus socios.

Está también el secreto comercial, que lo que hace es amparar toda la información que no se ha divulgado, que la empresa todavía no ha hecho pública y que tiene un valor comercial, entonces aquí entran un montón de cosas y lo vamos a ver seguidamente. Cuando hablamos del secreto comercial, hablamos de que es información no divulgada que tiene un valor comercial por su condición. No es la receta secreta del coronel de Kentucky Fried Chicken (KFC). Un ejemplo puede ser que consideremos que podemos brindar toda la información nutricional de los productos comestibles, porque es pública y se la tenemos que dar al consumidor; pero no así. Toda la técnica que se utilizar para producir este comestible es información que si la empresa quiere se la puede reservar.

Si todo fuera tan fácil como simplemente agarrar una lista de ingredientes y llegar y hacerlo, yo haría Coca Cola en mi casa. Obviamente hay una técnica, que la empresa tiene la potestad de reservarse, para llegar a obtener el producto. Pero es una receta, no son solamente ingredientes; una receta también es metodología y eso se puede resguardar. Esto es importante porque muchas veces tienen un valor comercial.

Es importante notar que el secreto comercial entra tanto en relaciones comerciales como laborales. También si nosotros somos funcionarios y conocemos información que es secreto de Estado, a nosotros eso casi que nos cubre igual. Ahora vayámonos al ámbito privado que nos cuesta un poquito a veces. En este ámbito, si uno entra a una empresa y conoce algún tipo de metodología, algún tipo de información, tiene el deber de resguardarla aunque el contrato de trabajo no lo diga específicamente. Esto se debe a que hay una ley que dice que la información que uno conoce en el ámbito laboral, si no ha sido divulgada, tiene que resguardarse. Esto es bien necesario entenderlo.

En el tema público también es bien importante. Puede pasar que por temas registrales nosotros como funcionarios tengamos acceso a información que está cubierta por el secreto comercial. Por ejemplo una patente. Si alguien quiere certificar una patente tiene que dar toda la información del producto. Y está bien, la entrega; pero como Estado esa información tenemos que resguardarla porque tiene un valor económico para la

empresa y está cubierta por el secreto comercial también.

Otro tema aparte, porque es muy amplio, es el secreto bancario, que también se refiere a información que no se puede divulgar. Hablamos del velo societario que ya expliqué.

Y con esto termino (me va a dar apenas el tiempo), los delitos informáticos o el ámbito de la intimidad. Hace unos años se aprobó la ley contra los delitos informáticos que hizo algunas modificaciones y menciono aquí los principales. Es una lista amplia; estamos hablando de:

- Violación de correspondencia, de llegar e intervenir correspondencia. Luego hablamos de violación de datos personales. Antes tenía un nombre más bonito, se llamaba violación de correspondencia electrónica. Ahora, con una reforma, se le cambió el nombre a este delito. Pero básicamente la violación de datos personales nos tiene que importar mucho porque se da cuando por mecanismos ilegales se accede a información de una persona que incluye la correspondencia. Entonces todos los temas de hackeo entran acá.
- Sustracción, desvío o supresión de correspondencia. Para los funcionarios esto también es vital. O sea, ¿qué pasa si nosotros recibimos una solicitud de información muy incómoda y llega el funcionario y dice: “¡Ay qué pereza responder esta solicitud! voy a borrar el correo y así no lo respondo”? Sin embargo, la persona va a tener copia. Entonces no solamente sería un tema inconstitucional y vendría recurso de amparo de fijo, sino además se estaría cometiendo un delito porque estaríamos suprimiendo información, máxime si esa información entró a un sistema y la borramos. Es importante saber que eso es un delito.
- La captación indebida de manifestaciones verbales, este creo que es el más importante. ¿Cuántos hemos estado en reuniones y muchas veces pasa que alguien dice que para mayor seguridad va a grabar la reunión? Eso es ilegal y es un delito, a menos que le preguntemos a las personas si podemos grabar la reunión.
- El uso indebido de correspondencia y publicación.
- Divulgación de secretos que es donde entra el tema del secreto de Estado.
- El sabotaje informático se da cuando llegamos y por algún mecanismo violentamos algún sistema informático, alguna red para que se caiga y algo pase. Digamos que soy funcionario y estoy en el Ministerio de Obras Públicas y Transportes (MOPT) y ya no quiero dar más licencias, voy a decir que se cayó el sistema. El tema de esto es que si esa caída de sistema fue intencional es un delito.
- Espionaje informático.
- Facilitación de delito informático. Este es muy importante. ¿Qué pasa, por ejemplo, si algún ente privado de alguna manera aparece con una base de datos pública que por algún mecanismo ilegal la sustrajo y resulta que fue que un funcionario le ayudó, que le dio un acceso o le dijo “te voy a dejar tal puerto a tal hora”? Ahí estaríamos hablando de una facilitación de un delito informático, lo cual también es un delito.
- Difusión de información falsa.

Esos son los delitos más importantes, les aconsejo que revisen esos dos títulos, que son el de propiamente delitos informáticos y el capítulo de delitos contra el ámbito de la intimidad, donde van a poder ver un recordatorio. Del 202 para arriba todos son delitos agravados en casos de ser funcionarios públicos. O sea, se duplican las penas si quien comete el delito es funcionario público; para que lo tengamos en cuenta nada más. En resumen,

una adecuada gestión de la información que ampara los derechos de las personas a la intimidad y también protege la seguridad de esa información.

Todo eso tiene muchísimo que ver con el tema informático porque son consideraciones que a la hora de desarrollar un sistema va a dar información. Tenemos que velar porque esté lo necesario; que si uno se puede saltar el login cuando inicia sesión en una página y con eso obtiene información, saber que hay una brecha de seguridad importante, que podría acarrear muchas de estas situaciones que hemos mencionado.

Otro aspecto valioso es que no se necesita una ley específica. Esto es bien importante porque muchas veces se quieren generar leyes para todo; pero resulta que ya tenemos un marco jurídico bastante robusto que sirve tanto para el informático, como para lo que es analógico. Algunas leyes nuestras sí han sido bastante visionarias en dejar sentadas las bases para cualquier tipo de medio en que se gestiona la información. Y este es el caso, me parece, salvo ciertas cuestiones que van más allá del tema de la gestión de la información.

Finalmente, en la última diapositiva dejé una lista de leyes y normativas distintas que les pueden ser muy útiles para estudiar y tener en cuenta cómo se debe gestionar la información en materia de informática. Vale decir que, por ejemplo, el manual sobre normas técnicas de control interno relativo a los sistemas de información computarizado de la Contraloría General de la República lo que hace es basarse muchísimo en estos conceptos y llevarlos a la práctica. Por eso quise más bien enfocarme en los conceptos básicos, porque son los que dan pie para que a la hora de que operativicemos las cosas a nivel informático, no cometamos errores que nos puedan hacer caer en algún tipo de responsabilidad legal.

Estoy disponible si hay preguntas. Muchas gracias.

NORMAS RELEVANTES

Constitución Política.

Ley Protección de la Persona frente al tratamiento de sus datos personales (8968) y su reglamento.

Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones (7425).

Manual sobre Normas Técnicas de Control Interno Relativas a los Sistemas de Información Computarizados (GCR).

Código Penal.

Ley de Información No Divulgada (7975).

Reglamento sobre Medidas de Protección de la Privacidad de las Comunicaciones (35205-MINAE).





Política Nacional de Gestión y Conservación de Documentos

Alexander Barquero Elizondo

Director general del Archivo Nacional de Costa Rica

Raquel Umaña Alpízar

Profesora de la carrera de Archivística de la Universidad de Costa Rica

Alexander Barquero Elizondo

El tema de la transformación digital tiene que ver con una reconversión de los modelos de negocios en las instituciones. En el caso de la administración pública, nuestro modelo está definido por todo el marco normativo, es decir el cumplimiento de los objetivos que establece la misma administración para poder brindar adecuadamente los productos, los servicios y los procesos que los ciudadanos requieren para su buen vivir.

Cuando hablamos de transformación digital en lo público, nos referimos a todos esos esfuerzos que vamos a desarrollar de aquí en adelante para que verdaderamente la administración pública aproveche las oportunidades de incorporar mecanismos de tecnología y nuevas destrezas en sus profesionales para brindar cada vez mejor estos servicios y productos en función del valor público.

Cuando pensamos que los documentos se van a preservar en herramientas tecnológicas, es inevitable almacenar una serie de datos alrededor de la documentación que nos permita ubicarlos fácilmente y sacarle más provecho.

A estos datos que contextualizan un documento, los podemos llamar metadatos. Tenemos que cuidarlos con responsabilidad porque posiblemente explican los temas que están incorporados y también tienen un tratamiento dentro del marco normativo que recién nos explicaba el expositor. Estamos acostumbrados a gestionar documentos en soporte físico como una unidad de información.

Cuando nos referimos a documentos electrónicos existe una serie de información alrededor de los mismos. Por esa razón, es importante tener claro cuál es la ruta a transitar para resolver esos inconvenientes y generar resultados. En ese sentido, se aprovechó la consulta pública en la que muchos de ustedes participaron en un congreso anterior, con la finalidad de crear una política de gestión y conservación de documentos.

Ahora dimos un paso más allá a toda esa instrumentación. Nos referimos a una Política Nacional de Archivos, un marco común que establezca la ruta 2020-2030. Es un esfuerzo que se construye entre todos, con tareas y responsabilidades para todos, pero que también servirá como herramienta de trabajo para generar capacidades y buscar recursos de cara a un mundo completamente distinto, donde las tecnologías nos permean en todo lo que hacemos.

Con la intención de reflejar un esfuerzo de concreción, solicité a la sección de Archivística de la Universidad de Costa Rica por medio de la señora Raquel Umaña, una síntesis de todo el proceso realizado en congresos anteriores y el excelente trabajo del equipo designado dentro del Archivo Nacional.

Muchas tareas retadoras vendrán a futuro, con una visión y aspiración política a diez años que trascienda en donde estamos hoy. Queremos posicionar los archivos y brindar desde los archivos todos los beneficios para la administración.

Raquel Umaña Alpizar

En primer lugar, felicitar al Archivo Nacional, realmente estoy muy motivada y me parece excelente el tema de este congreso. Felicito a don Alexander Barquero y a todo su equipo por el arduo trabajo en relación con el documento electrónico. Como archivistas, este es un tema que tiende a asustarnos porque sabemos qué nos corresponde. Sin embargo, es un reto que tenemos que enfrentar en conjunto y de manera interdisciplinaria.

¿A qué nos referimos con la Política? El Archivo Nacional está trazando una ruta de diez años en los cuales se brindarán los instrumentos y herramientas necesarios para abordar el tema del documento electrónico. Habrá un instrumento guía enfocado hacia los encargados de los Archivos y en general a todos los usuarios que necesitan la información. La Política se trabajó desde el año 2017 y está en su última fase, esperando que al final de año pueda ser publicada.

En el año 2011, se realizó un diagnóstico para saber cómo estamos trabajando. Todavía hoy, casi treinta años después de la aprobación de la Ley 7202, seguimos detectando los mismos errores: no hacemos cuadros de clasificación, no tenemos tablas de plazos, siempre nos quejamos por el espacio, entre otros aspectos. La idea ahora es que ustedes no se sientan solos.

Todas las instituciones están migrando del papel a lo electrónico y se compran sistemas que no siempre responden. La ruta a seguir como país y las necesidades a solventar en la sociedad actual, es el trabajo que realiza el Archivo Nacional y que se ha discutido en varios congresos.

Esta política es importante porque fue a consulta pública, se analizó en un congreso anterior, se trabajó en el Ministerio de Planificación (Mideplan), con grupos focales, con la sección de Archivística de la Universidad de Costa Rica y ahora se encuentra en fase final, por lo que estamos presentando un panorama más claro de hacia dónde se encamina el Archivo Nacional.

Alexander Barquero Elizondo

Esto es un esfuerzo del que hace tiempo se viene hablando, cuál es la ruta que debemos definir en la gestión de los documentos, sin importar el soporte.

Con los diagnósticos de la situación archivística, entendemos un poco por donde tenemos que ir, pero no

todos lo estamos haciendo al pie de la letra, tal y como se establece, por muchas razones: los recursos no son suficientes, el tiempo no alcanza o no se recibe apoyo de la administración.

Estos factores influyen en qué tanto hemos podido impulsar los esfuerzos de la gestión, desde la emisión de normativa interna, la gestión de las políticas de los documentos en las instituciones y el adecuado uso y trasiego del ciclo de vida de los documentos dentro de la misma administración pública.

La Política los contempla, pero no podemos obviar que hay un reto todavía mucho más fuerte que es el tema de los documentos electrónicos.

Estoy seguro que todos ustedes están al tanto de la directriz 019-MP-MICITT que se emitió el año pasado. Lo que busca es poner en sintonía el desarrollo del gobierno digital en el país con una serie de disposiciones para las instituciones.

Una de ellas, se refiere a la emisión de documentos electrónicos. El inciso c) del artículo 3, indica que al finalizar el 2020 las instituciones del Gobierno Central y las instituciones descentralizadas deberán realizar los esfuerzos necesarios para que la producción y la preservación de sus documentos sea en soporte electrónico, al menos en un 75% de la producción documental total.

En algunos casos no se avanzará mucho, hay instituciones que no sabrán cómo hacerlo, no cuentan con recursos o con gente capacitada para resolverlo. En otros casos, conozco entidades que están analizando el potencial y no quieren quedarse rezagadas.

Ustedes tienen que estar ahí. Tienen una responsabilidad, una obligación y además el potencial de ayudar a dirigir esos esfuerzos para que el resultado sea acorde con la expectativa de lograr la adecuada gestión de nuestros archivos. El negocio de los documentos les pertenece a ustedes, a los encargados de los archivos.

La temática que han desarrollado los diferentes congresos archivísticos, responde a las oportunidades de mejora y a la brecha que se detectó desde el 2011 con ese primer diagnóstico. Entonces, la Política Nacional de Archivos es un producto de estrategia país. La emitió la Junta Administrativa del Archivo Nacional quien tiene las competencias para definir rectoría en la materia y es articulada por la Dirección General del Archivo Nacional. Está pensada del 2020 al 2030 porque es un marco de trabajo, una serie de lineamientos que establecen la ruta y esfuerzos de las diferentes instituciones que pertenecen al entorno archivístico nacional.

La Política cuenta con planes de acción que indican cómo resolver las tareas, desarrollar proyectos, mejorar servicios, responsables, corresponsables, expectativa de instrumentación, entregables, métricas y fechas en las que esperamos un cumplimiento. La Política es el primer nivel y tiene el guion de hacia dónde queremos ir, pero son los planes de acción enmarcados en esos cinco años, los que dirán cuáles son las acciones, los indicadores, las metas y los responsables.

Como resultado se tendrán dos grandes instrumentos. Por un lado, tenemos proyectos que terminan desarrollando un producto, un servicio en particular, generan capacidades, alguna nueva certificación, un programa de formación continua o bien un nuevo diseño de una carrera. También tenemos los instrumentos técnicos que son los que dirigen la actividad de los archivos de nuestro país. Hay normas, lineamientos, directrices, circulares y otros, todos muy diversos, que no siguen un estándar en particular, pero que generan

obligatoriedad y disposiciones para los archivos.

La idea es estandarizarlos en un instrumento único que será la Norma Técnica Nacional, la cual permitirá la normalización en la gestión de documentos electrónicos, siguiendo el marco jurídico, con el fin de normalizar la producción de documentos en las diferentes unidades de una institución.

El día de mañana en vez de que cada uno de ustedes haga un ejercicio de ingeniería de requerimientos ajustado a sus necesidades de negocio, vamos a contar con un instrumento único con lo mínimo que el país necesita, sin importar cuál sea la institución.

Hay una frase que todos la hemos escuchado en algún momento que es “Lo perfecto es enemigo de lo bueno, o lo perfecto es enemigo de lo posible”, esa es la base detrás de lo que estamos persiguiendo con la construcción de la Norma Técnica Nacional. Será minimalista, solo tendrá lo necesario, no más, lo cual no significa que será estática, sino un instrumento vivo en constante revisión y mejora continua.

En el tema de gestión de documentos electrónicos podemos subir la barra un poco más, inclusive manejar modelos de madurez. Yo podría pensar en establecer un nivel tres, dos y uno para cada institución según sus recursos y capacidades. Sería una forma evolutiva muy orgánica y ajustada a la realidad, por eso la Política está pensada para diez años plazo.

Igualmente sucede con los requerimientos para sistemas de preservación de documentos electrónicos. El Archivo Nacional está dando pasos importantes en esta materia y mañana presentaremos una solución para ustedes. También existe un instrumento que define algunas reglas con respecto a la descripción archivística y lineamientos para la elaboración del tipo documental carta, ambos eventualmente se incorporarán al estándar para la Norma Técnica Nacional.

Y finalmente un esquema de metadatos para los sistemas de documentos electrónicos y protocolos de comunicación entre un sistema y otro. Probablemente no es una cuestión archivística, pero es de interés de los archivos que se desarrollen adecuadamente. Contando con una Norma Técnica Nacional podemos definir este esquema de metadatos o ese protocolo de comunicación que nos permitirá ir viendo donde están las brechas, las cosas que hay que resolver y cómo podemos hacerlo, sea con un proyecto que termine generando un producto o un servicio, o una generación de capacidades.

En la Política Nacional de Archivos no se establecen responsables, pero si es muy importante tener claro quiénes sacarán provecho. Esa lista de beneficiarios y responsables la bautizamos como el *Entorno Archivístico Nacional* que involucra a los actores relacionados con los archivos.

Nos referimos en primera instancia al Archivo Nacional de Costa Rica con todos sus elementos: Junta Administrativa, Comisión Nacional de Selección y Eliminación de Documentos y la Dirección General. También se incluye el Sistema Nacional de Archivos que agrupa todos los archivos de las instituciones públicas, la Academia, gremios profesionales usuarios de los servicios de los archivos, asociaciones y grupos organizados de investigadores, docentes, profesionales, y/o encargados de archivos. Así como la Comisión de Archivos Institucionales del Sector Público (CIAP), las empresas privadas que brindan productos o servicios para los archivos, entes superiores de planificación, hacienda, tecnología, fiscalización, seguimiento y/o control, entre otros.

Todo el Entorno Archivístico Nacional se beneficiará con la concreción de los objetivos de la Política Nacional de Archivos y en los planes de acción se sentarán los responsables para cumplir esas metas.

¿Qué incluye la Política Nacional de Archivos? Tiene dos enfoques orientadores, siete principios guía, objetivo general, diez objetivos específicos, tres ejes de acción y veinticinco lineamientos.

Los enfoques orientadores tienen que ver con Derechos Humanos y la contribución al derecho de acceso a la información, así como la gestión por resultados, una política como esta tiene sentido cuando tiene una estrategia que garantiza una evaluación periódica del cumplimiento. Es una visión de diez años y las cosas pueden cambiar de un día para otro, entonces esta política tiene que ser capaz de mantener su vigencia y por eso está planteada la posibilidad de evaluarla desde el inicio. Sólo podemos mejorar lo que medimos porque tenemos que saber dónde estamos para entender claramente hacia dónde vamos y qué acciones podemos tomar.

Los siete principios guía involucran: acceso a la información y la transparencia; eficacia y eficiencia; ética; innovación y adaptación al cambio; talento humano; valor público y visión sistémica.

Con relación a la eficacia y eficiencia, es importante concientizar que hoy estamos en una realidad de limitación en acceso a los recursos mucho mayor que en el resto de la historia del país. Tenemos que tomar cada colón y estirarlo todo lo que se pueda para poder hacer lo máximo posible. Implica que tenemos que pensar en un tema de economía y en absolutamente todas las disposiciones y proyectos que se desarrollen de aquí en adelante en el marco de la Política.

La ética no tengo que explicarla, pero si no hay un ejercicio ético en lo que hacemos, estamos perdidos. Esto permea absolutamente todo.

Innovación como bien lo comentaba ayer el profesor don Edwin, es algo que se busca, que se persigue, que se diseña metodológicamente para ir logrando nuevos resultados; y la adaptación al cambio lamentablemente es un tema más reactivo. Estos aspectos estarán presentes en el desarrollo de la Política porque no tenemos idea con qué tipo de tecnologías nos vamos a enfrentar en estos años ni qué están haciendo los altos investigadores en Alemania, Corea, Estados Unidos o en otros países que podrían darle completamente la vuelta a una propuesta como esta y tenemos que ser capaces de acomodarnos y de sacarle provecho.

El talento humano es un pilar fundamental de toda la Política Nacional de Archivos. Nada caminará si no se generan las capacidades, se crean las competencias o si el Entorno Archivístico Nacional no diseña los modelos de formación continua que permitan los conocimientos y destrezas para hacerle frente a estos retos.

El valor público nos permite cumplir con los objetivos que la administración persigue en relación al servicio que se entrega a los ciudadanos.

Finalmente, la visión sistémica se refiere a los ejercicios de planificación nacional, de inversiones públicas, el Plan Nacional de Desarrollo, la Estrategia de transformación digital hacia la Costa Rica del Bicentenario, los objetivos de desarrollo sostenible, entre otros.

El objetivo general de la Política es aportar al Estado una ruta de desarrollo al 2030 que promueva y contribuya al acceso a la información pública y a la transparencia en la gestión, por medio del fortalecimiento y mejora

continúa del Entorno Archivístico Nacional, la superación de las brechas que existen en los productos y servicios existentes, y el aprovechamiento de las tecnologías para mejorar la gestión y preservación de los documentos; teniendo siempre como pilar fundamental el talento humano que labora en los archivos.

Los tres ejes de acción de la Política son el fortalecimiento del Sistema Nacional de Archivos, la gestión de los documentos y la preservación de los documentos. Estos ejes se reflejarán en los lineamientos y en los objetivos de la Política Nacional de Archivos.

Para el primer eje de la Política podemos mencionar cuatro objetivos específicos: la modernización y transformación digital del Archivo Nacional de Costa Rica; el desarrollo del Sistema Nacional de Archivos; el mejoramiento de la formación profesional, la capacitación continua y el liderazgo de los archivistas; así como el desarrollo adecuado de los productos y servicios del entorno archivístico nacional.

Los objetivos del segundo eje, se relacionan con la normalización de los procesos archivísticos; la gestión de los documentos electrónicos y la digitalización de los documentos. Para el tercer eje podemos mencionar la preservación de documentos electrónicos, la mejora continua de los procesos de selección, eliminación y transferencia de documentos, así como la divulgación de los documentos electrónicos.

Cada uno de los tres ejes atiende una serie de lineamientos, 25 en total. La idea es que el día de mañana cualquiera de nosotros pueda hacer referencia al lineamiento que está atendiendo y entender que es lo que persigue y cuál es el objetivo que podrá lograr.

Para tener claridad de cómo se estructuran los lineamientos, vamos a detenernos sólo en uno de ellos: revisar regularmente el marco jurídico archivístico nacional con el fin de identificar y aplicar las reformas necesarias para que respondan a los retos de nuestro país, frente al desarrollo de la sociedad de la información y el conocimiento y generando los cambios que permitan enfrentar con mayores capacidades y conocimiento los procesos de transformación digital del Estado.

Me permito comentarles una anécdota al respecto. Durante una reunión del Consejo Europeo en Bélgica sobre la firma digital, conversamos con los encargados de los procesos de transformación digital del gobierno de Bélgica (la Agencia de Tecnologías de Información y Comunicación Federal). Ante un comentario muy interesante yo les dije: ¿qué pasa cuando hay una ley que no les permite hacer algo? Todos se miraron y respondieron: se cambia la ley.

Me quedó muy claro que eso no puede ser una excusa. Si algo hoy está expreso en una norma que no es correcto o que no es vigente, podemos proyectar su modificación en una política de diez años plazo, la cual establece claramente los objetivos, incluso se pueden buscar patrocinadores dentro de la Asamblea Legislativa y realizar los cambios pertinentes. Es parte de los esfuerzos que toca hacer.

Otros de los lineamientos son la solvencia financiera y capacidad desarrolladora del ente rector; la articulación institucional e internacional; la transformación digital, innovación y eficiencia. Además, podemos mencionar el cumplimiento de la legislación archivística y de la normativa técnica; la formación continua de la profesión archivística, la profesionalización y promoción del ejercicio archivístico nacional y la incorporación de los

productos y servicios de los archivos al Sistema Nacional de Calidad.

Contamos con más lineamientos: la mejora continua, implementación y fiscalización de cumplimiento de la normativa sobre los procesos archivísticos; transformación digital de la gestión de los documentos en el Sistema Nacional de Archivos; implementación de sistemas de gestión de documentos electrónicos; interoperabilidad en la gestión de los documentos electrónicos; respuesta de incidentes en la gestión de documentos electrónicos e implementación de proyectos de digitalización, digitalización certificada y eliminación por sustitución.

Con respecto al tercer eje sobre preservación a largo plazo de los documentos electrónicos en el Sistema Nacional de Archivos; podemos mencionar los siguientes lineamientos:

actualización permanente y mejora continua de las soluciones para la preservación de documentos electrónicos; implementación de tecnologías disruptivas para la toma de decisiones; transferencias de documentos con valor científico y cultural; mapeo del estado de conservación del entorno archivístico nacional; descongestionamiento de los archivos; y consulta centralizada de los documentos de archivo.

Para que esta Política Nacional de Archivos tenga sentido, debe estar acompañada por un plan de acción, que incluirá todas esas acciones estratégicas, indicadores, metas, coordinador y responsables. Será la hoja de ruta para los productos, proyectos y servicios que tienen que desarrollarse en el corto, mediano y largo plazo.

Algunas de las iniciativas que ya se están desarrollando involucran el Archivo Digital Nacional y la Norma Técnica Nacional. Ambos son temas urgentes de los requerimientos para los sistemas de gestión de documentos electrónicos y de los sistemas de preservación de documentos electrónicos. ¿Por qué nos precisa esto? porque la mayoría de ustedes son parte de estos esfuerzos en sus instituciones y si nosotros no definimos estas reglas, vamos a tener un manejo diferente entre una institución y otra y eso no nos conviene. También es un instrumento para la empresa privada para que logremos hasta cierto punto una normalización de los productos.

Tenemos que pensar en neutralidad tecnológica, en el desarrollo de los productos y servicios tecnológicos que vamos a incluir en los archivos. Hoy podríamos necesitar una herramienta y mañana otra completamente diferente y esa transición no nos debería de doler porque así es como se diseña adecuadamente un aparato que funciona en el tiempo.

Raquel Umaña Alpizar

Lo que debemos tener claro los archivistas, son los requisitos básicos y mínimos que tiene que tener un sistema de gestión de documentos.

Por ejemplo, la normalización de formatos, que está muy ligado a la gestión y la preservación. ¿Cuál es el reto que tenemos con documentos electrónicos? la obsolescencia. No podemos garantizar la información contenida en los documentos que se conservan a través del tiempo.

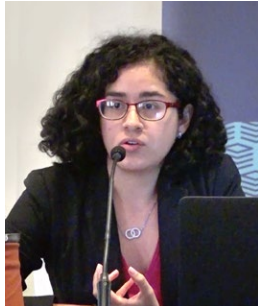
Otro elemento básico son los identificadores únicos. No se trata de un solo sistema de gestión para arreglar la gestión administrativa, se necesita un conjunto de sistemas que interoperen.

En la prospectiva archivística estamos obligados en las instituciones a colaborar con la normalización de los procesos, entender el negocio que tiene cada organización y la diferencia. Que también nos quede claro qué es un repositorio de preservación digital, porque no es posible que ni siquiera nosotros que somos los expertos, no lo sepamos ni las funcionalidades que tiene. Tenemos, además, que aplicar la norma OAICE sobre preservación, que tiene más de cuarenta años y que apenas la estamos empezando a conocer.

Para finalizar, agradecer este esfuerzo del Archivo Nacional y ofrecerle nuestro apoyo. Este es un trabajo conjunto con los profesionales, archivistas de las instituciones, la academia, los grupos organizados y el Archivo Nacional. Es nuestro momento y tenemos que tomar las riendas que nos corresponden.

Muchas gracias.





Ciudades y Territorios Inteligentes: ¿Qué son realmente?

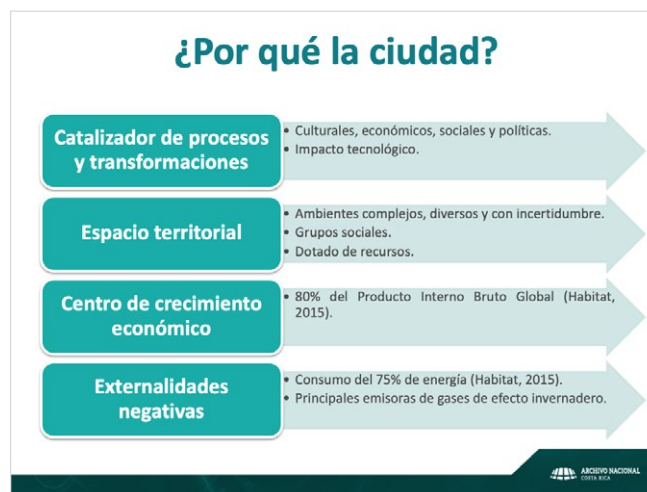
Valeria Castro Obando

Investigadora del Programa Institucional Sociedad de la Información
y el Conocimiento (PROSIC) de la Universidad de Costa Rica

Muy buenos días, es un gusto poder acompañarles en esta actividad que está realizando este día el Archivo Nacional. Les voy a hablar sobre las Ciudades y Territorios Inteligentes. La idea es ofrecerles un panorama general de ambos conceptos, introducirlos al tema y precisar la evolución socio-histórica de estos términos. También me interesa brindarles un par de definiciones básicas de la noción de ciudad inteligente, hablar sobre las características más relevantes y el tipo de beneficios que pueden generar este tipo de urbes.

De igual modo, voy a presentarles algunas de las críticas, vacíos y debilidades que ciertas teorizaciones han hecho al término. Finalmente voy a referirme a las diferencias específicas de la ciudad inteligente con respecto a otros conceptos que pueden ser considerados como similares, pero que no precisamente corresponden a ciudad inteligente.

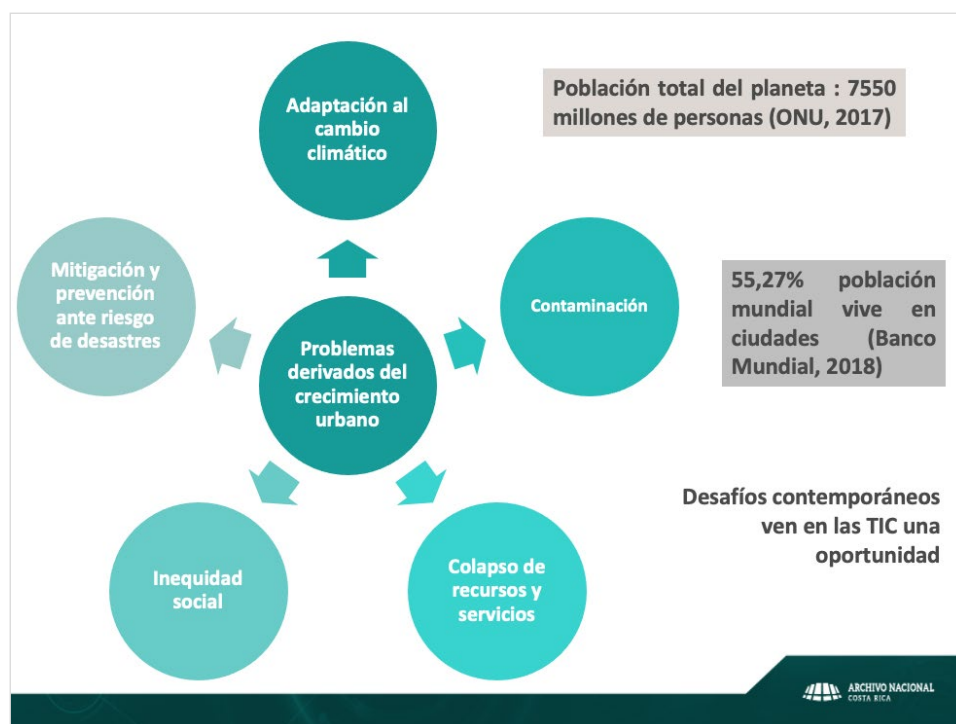
Me gustaría iniciar la conferencia, centrando la reflexión en torno al espacio urbano, ¿por qué estamos hablando de ciudad en general? y ¿por qué es importante situar la mirada en este escenario? Como muchos de ustedes sabrán, algunas de las principales transformaciones económicas, culturales, políticas y sociales más trascendentales que se han dado a lo largo de la historia de la humanidad, han ocurrido en centros urbanos. Esto hace que las ciudades deban ser vistas como catalizadores de procesos y transformaciones de esta índole y por tanto, siempre han sido el bastión de importantes cambios que se expresan en términos de innovación y de transformaciones que se dan dentro de nuestras sociedades.



Pensar en la ciudad, implica enfocarse en el ámbito de lo urbano y conlleva pensar en espacios territoriales que tienen cierto tipo de características específicas. ¿Cuál sería la primera? Bueno, es un territorio en el cual convergen una serie de recursos, tanto económicos como de infraestructura y de los servicios que la ciudad le provee a la población que reside en ella. Los centros urbanos se caracterizan por la presencia de diversos actores sociales que interaccionan dentro de estos y que por tanto, constituyen espacios complejos en los que se tejen dinámicas entre los distintos actores presentes en las ciudades.

De igual modo, las ciudades son muy importantes porque estas suelen ser el motor del crecimiento económico de muchísimas sociedades. Datos del Programa de Naciones Unidas para los Asentamientos Humanos (ONU Hábitat), estimaban que en el 2015 cerca del 80% del producto interno bruto (PIB) global era producido en centros urbanos, lo cual nos indica que sin lugar a dudas las ciudades son bastiones de desarrollo. Sin embargo, esto también nos permite ver que si bien las ciudades son muy importantes por esas razones; igualmente generan una serie de problemas o desafíos específicos que están vinculados con la gestión urbana. Entonces se puede decir que las ciudades producto del crecimiento urbano, no solo enfrentan problemas vinculados con el medio ambiente sino también con el desgaste de recursos y el consumo energético.

En este contexto y considerando que más de la mitad de la población mundial actual vive en ciudades, se hace muy necesario que se empiece a centrar la atención justamente en los desafíos que enfrentan. Algunos de esos problemas están asociados con el crecimiento urbano y el incremento en la cantidad de población que reside en centros urbanos. En primer lugar, habría que hablar de la adaptación al cambio climático, que para nadie es un secreto que esto es un gran reto al que tienen que hacerle frente nuestras sociedades. Asimismo, se puede mencionar la contaminación, no solo de las fuentes de agua y el aire, sino también contaminación sonora y visual.



La utilización y desgaste de los recursos de los centros urbanos contribuye al colapso de los servicios que ofrece la ciudad, lo que se expresa en problemas relacionados a la incapacidad de los servicios urbanos para dar abasto con las demandas ciudadanas (por ejemplo; falencias con la movilidad urbana).

Otra de las implicaciones del crecimiento urbano son las externalidades negativas derivadas de la inequidad social, el acrecentamiento de brechas sociales a lo interno de las ciudades, la pobreza, la violencia y otros fenómenos vinculados como por ejemplo, el aumento de la criminalidad. Estos problemas junto con la necesidad de planificar las ciudades y el desarrollo humano en términos de la adaptación al cambio climático y bajo estándares de prevención y adaptación ante el riesgo de desastres, hace que los centros urbanos hoy se encuentren ante grandes desafíos.

Pero, ¿por qué es esto tan importante? Y ¿por qué les hablo de algo que pareciera que no tiene tanta relación con la ciudad inteligente? Esto es porque justamente cuando se empieza a hablar del tema se comienza a ver a las tecnologías de la información y la comunicación (TIC) como un medio para ayudar a gestionar los espacios urbanos. Lo anterior implica pensar en la ciudad como un escenario que puede ser planificado, organizado y en el cual las tecnologías podrían convertirse en una ayuda para poder resolver ciertas problemáticas urbanas.

Cuando hablamos sobre el origen de la expresión “ciudad inteligente”, es importante mencionar que la misma está vinculada con la intensificación del proceso urbanizador que enfrentan nuestras ciudades actualmente. En ello, las TIC se ven como una oportunidad para ofrecer soluciones integrales a los desafíos que en estos momentos enfrentan las ciudades.

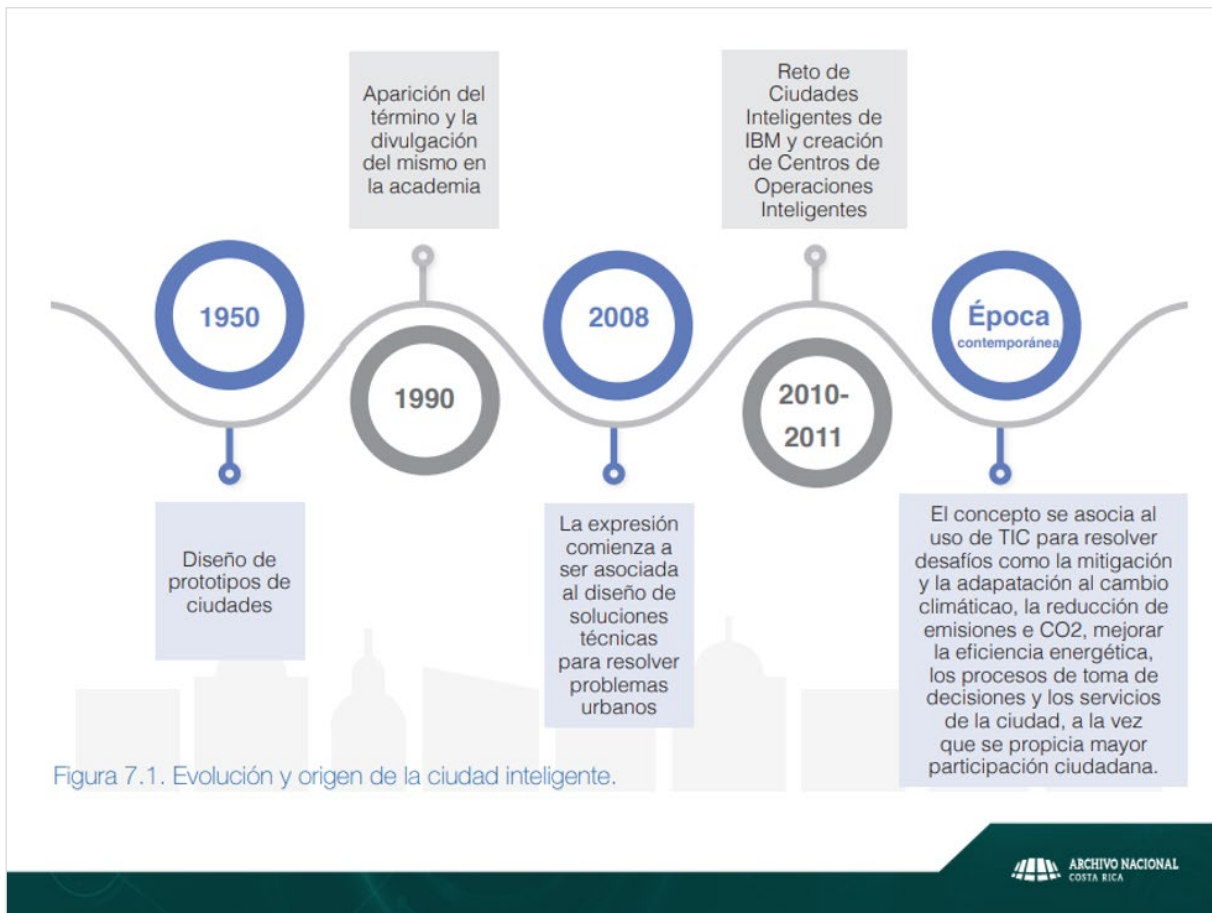
Se considera que las ciudades inteligentes vienen a modificar el rol tradicional de las ciudades porque estas deben ser pensadas como espacios para residir y los cuales me dotan de cierto tipo de recursos de los que puedo obtener cierto tipo de servicios. En ese sentido, tratar de integrar la tecnología en espacios urbanos y pensarla desde este paradigma, implica introducir una serie de cambios que están destinados no solo a la gestión urbana, sino también a entender que esto trae aparejado una serie de transformaciones vinculadas a las formas como se trabaja y como se comunica, produciendo un impacto en las relaciones sociales que se tejen a lo interno de las ciudades y por supuesto también en la manera como se producen bienes y servicios.

En términos de la evolución socio-histórico que ha tenido este concepto, es importante señalar que este apareció y/o al menos se empieza a hacer mención del mismo en el ámbito académico, a partir de la década de 1990. Sin embargo, es posible encontrar una serie de antecedentes previos a esta fecha, en los que si bien es cierto, aún no se utilizaba esa denominación, ya se empezaba a considerar la posibilidad de que las tecnologías fungieran como herramientas para mejorar la gestión urbana.

Algunos de los primeros ensayos que se empezaron a dar en esta línea, fueron prototipos muy específicos desarrollados en 1950 con la idea de unir la ciberfísica con la gestión urbana y el urbanismo. A partir de esto, se hicieron algunos prototipos para las ciudades de Pittsburgh y New York, no obstante, los resultados obtenidos con su implementación no fueron los más idóneos, lo que llevó a una especie de divorcio entre urbanistas y técnicos. Es, hasta muchos años después, que se empieza a plantear nuevamente la posibilidad de que tecnología y urbanismo empiecen a colaborar conjuntamente.

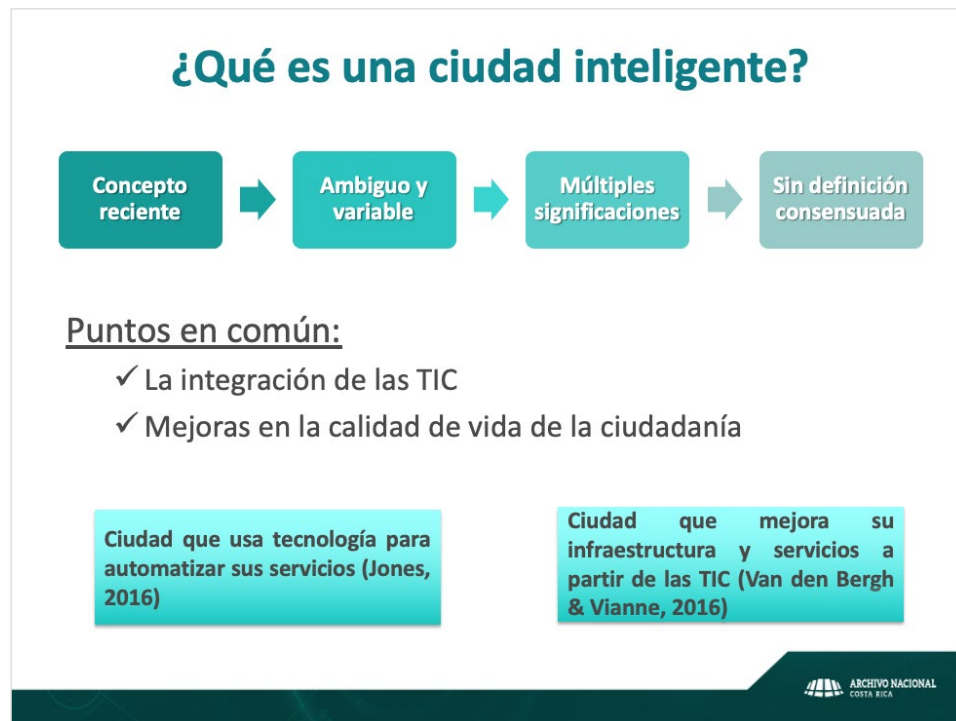
Posteriormente, se da un punto de disrupción importante en 2008 cuando el término es mencionado por primera vez fuera del ámbito académico, pero también empieza a ser apropiado por el sector empresarial. Es así

como la noción comienza a ser asociada con un conjunto de soluciones tecnológicas para resolver problemas urbanos y de ahí en adelante adquiere una resonancia importante. Con ello, advino un *boom* con respecto al tema, sobre todo por parte de grandes consorcios empresariales.



Por esto no es de extrañar que en años siguientes, por ejemplo entre 2010 y 2011, la transnacional IBM promocionara el reto de las ciudades inteligentes en el que la empresa dispuso a un grupo de consultores para que ayudaran a ciudades alrededor del mundo a participar en un concurso en el que se desarrollaron soluciones tecnológicas para problemas puntuales que estas enfrentaban en dicho momento. De igual modo, tampoco es casual que un año después de dicho concurso, aparecieran los centros de operaciones inteligentes, los cuales vienen a ser una plataforma creada con el fin de recopilar y gestionar información que contribuyera a los procesos de toma de decisión.

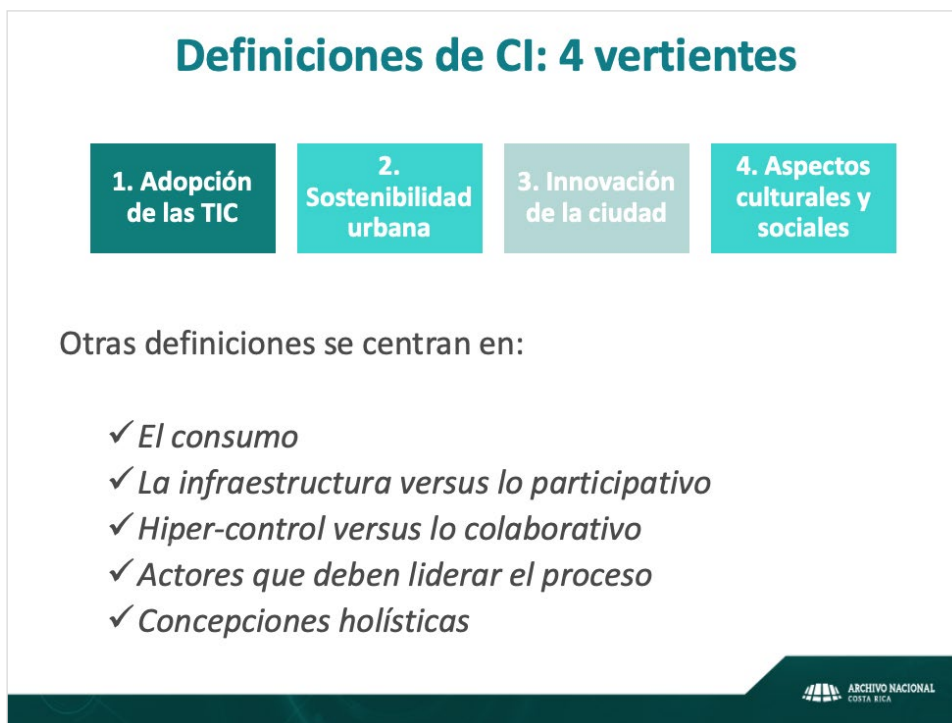
Si situamos el panorama en la época actual, se puede considerar que hoy el concepto de ciudad inteligente está vinculado al uso de las TIC, pero no en un uso de las TIC solo por usarlas. Esto me lleva a precisar el tema sobre cómo podemos entender la ciudad inteligente. Como les venía mencionando previamente, hablar de ciudad inteligente significa referirse a un concepto sumamente reciente. Como les decía, es hasta 1990 cuando se empieza a hablar del término tal y como lo entendemos actualmente.



Como es muy reciente el concepto, abundan las definiciones y significaciones, las cuales además de ser sumamente variables no sólo en lo que se refiere a los rasgos que caracterizan a las ciudades inteligentes sino que también con respecto al emisor de esa definición. En muchas de estas definiciones, se terminan plasmando las visiones de los actores que las brindan, entonces varía mucho si es una conceptualización que proviene de la academia y/o del sector empresarial.

A la fecha no se cuenta con una definición consensuada sobre el término de ciudad inteligente. Entonces si ustedes revisan un libro o literatura sobre este tema, van a encontrar múltiples definiciones que se van a referir a cuestiones diversas; sin embargo, a pesar de esta variedad, es posible encontrar un tema central: la integración de las TIC con el fin de impactar positivamente la calidad de vida de la población, ya sea de una ciudad o territorio en específico.

Hay dos definiciones básicas y muy escuetas de cómo se puede entender la ciudad inteligente, en las que pueden ver que el tema de la integración tecnológica es muy importante. En las definiciones sobre ciudad inteligente es posible identificar cuatro vertientes de dichas definiciones, las cuales se pueden clasificar ya sea que estas enfaticen las TIC, que se refieren más a la sostenibilidad urbana, que mencionen aspectos vinculados a la innovación de la ciudad o que enfaticen aspectos culturales y sociales.



En la primera vertiente, la ciudad inteligente es vista como aquella que no solo genera desarrollo en infraestructura de telecomunicaciones, sino que también es la que cuenta con servicios automatizados y aboga por la digitalización de los mismos. Asimismo, es una ciudad en la que se busca producir información y datos y se vela por la gestión de estos a través de medios digitales.

Las conceptualizaciones que enfatizan la sostenibilidad urbana, están vinculadas con objetivos como la reducción de la huella ambiental, la mitigación y adaptación al cambio climático y las energías limpias, entre muchos otros. Por otro lado, cuando se habla de definiciones asociadas a la capacidad de innovación de la ciudad, entonces estamos aludiendo a ciudades capaces de generar atracción o de invertir y atraer inversión, en las que su estructura productiva se ha diversificado, es decir que ha logrado la inserción de empresas no tradicionales en la ciudad (por ejemplo industria creativa, incubadoras, empresas de alta tecnología, entre otras) a la vez que se fomentan los emprendimientos y se crea un clima de negocios propicio a estos.

Por último, en las definiciones basadas en aspectos más culturales-sociales de la ciudad se le presta especial atención al rol que juegan las TIC para potenciar la participación ciudadana y la coproducción entre ciudadanía, autoridades gubernamentales y demás actores que están presentes en el escenario urbano e inciden en los procesos de toma de decisión y en la agenda de generación de política pública.

De manera paralela y por la gran variabilidad de definiciones que existen, hay otras teorizaciones que enfatizan otros rasgos. Por ejemplo, están las que se centran en el estímulo al consumo como elemento central de la ciudad inteligente, que son promovidas por el sector empresarial y que buscan la creación de soluciones TIC para brindar servicios a la ciudad. Por otro lado, se encuentran las definiciones que enfatizan el despliegue de infraestructura TIC y de telecomunicaciones como el rasgo más importante de la ciudad inteligente, versus

aquellas definiciones que lo que hacen es enfatizar de manera similar a la vertiente cuarta donde se habla de los aspectos culturales y sociales donde lo importante es justamente propiciar la participación ciudadana.

Luego podemos hablar de aquellas definiciones que están vinculadas a la noción de hipercontrol. Esto último debe ser entendido como la creación de mecanismos que permiten no solo generar y capturar, sino también gestionarla y utilizarla como un insumo que incida en la toma de decisiones. Otras definiciones se relacionan con los actores que lideran el proceso. En estas lo que se dice en primer lugar es que los procesos de ciudad inteligente, deben ser asumidos o liderados por gobiernos locales o administraciones municipales de manera conjunta con otros actores importantes.

También están las concepciones que tienen un carácter mucho más holístico, lo que hacen básicamente es recoger elementos previos de las otras vertientes en un afán por reflejar la complejidad del sistema urbano.

Ahora bien, con respecto a las principales características de una ciudad inteligente, como les mencionaba, la integración de las TIC es un aspecto fundamental porque eso permite generar soluciones tecnológicas, pero ¿de qué tipo?, ¿cuáles áreas deben impactar? y ¿para qué me deben servir este tipo de soluciones tecnológicas?

En términos generales podemos decir que, este tipo de soluciones deben tratar de generar algún tipo de efecto o estar destinadas a incidir en cinco áreas específicas: la dinámica urbana, la gestión pública, el análisis de recursos urbanos, la adaptación a cambios medio ambientales y el impacto en servicios públicos.



Por ejemplo, en el área de la dinámica urbana las soluciones TIC deben partir de la adaptación y la integración de las TIC para monitorear y conocer lo que ocurre a lo interno de una ciudad. En términos de gestión pública la introducción tecnológica debe permitir generar información, ordenarla y producir cierto tipo de efecto positivo en términos de la transparencia y la rendición de cuentas de las administraciones locales.

Con respecto al análisis de los recursos urbanos, las soluciones tecnológicas deben tratar de identificar y sobre todo valorar los requerimientos y las necesidades, en infraestructura, servicios, infraestructura TIC y de telecomunicaciones- de un centro urbano. Asimismo esas soluciones deben estar enfocadas hacia la adaptación a cambios del medio ambiente, básicamente con esto a lo que me refiero es que deben responder de manera efectiva al cambio climático, puedan ayudar a gestionar la seguridad y mitiguen el riesgo ante un desastre natural que pueda impactar la infraestructura y servicios de una ciudad. Una solución tecnológica de esta índole me permite incidir no solo analizando la oferta y demanda de servicios, sino también creando nuevos servicios.

Un aspecto fundamental que debe estar en el corazón de la ciudad inteligente es el hecho que todas estas intervenciones deben estar destinadas a impactar positivamente las condiciones de vida de la población. Sin embargo, para que esta condición pueda cumplirse es necesario generar un clima de coproducción en el que la ciudadanía más que ser un actor pasivo y beneficiario, se integre de manera activa en la identificación de soluciones que pueden ser útiles para su vida a lo interno de la ciudad.

Junto con estas condiciones, tampoco se debe perder de vista la necesidad de producir *inteligencia e innovación territorial*. La primera de estas está vinculada con la capacidad de planificar en función de la sostenibilidad ambiental dentro de la ciudad, mientras que la innovación territorial contempla un cambio de paradigma y/o de mentalidad que guarda relación con los valores y la cultura, y que no solamente busca generar adaptación y apropiación tecnológica sino también innovación, elevar la productividad y la competitividad del territorio.

Esto nos hace pensar hacia dónde deben estar destinadas las soluciones tecnológicas que se ponen en práctica dentro de una ciudad inteligente. Esto nos da ciertas pistas de cuáles deben ser los componentes centrales que debe tener este tipo de espacios, que como les mencionaba por la variabilidad de definiciones existentes, pueden variar, aunque al final vienen a ser básicamente las mismas áreas (gobierno inteligente, medio ambiente inteligente, economía inteligente, movilidad inteligente, ciudadanía inteligente, modo de vida inteligente).



Por ejemplo, en términos de gobierno inteligente estamos hablando de procesos de digitalización y de la introducción de elementos que caracterizan iniciativas de gobierno abierto. Por su parte, el medio ambiente refiere a la creación de soluciones tecnológicas que ayuden a combatir el cambio climático, reduzcan el consumo energético y prevengan el riesgo de desastres, entre otras.

La economía inteligente busca potenciar la innovación, diversificar la estructura productiva y potenciar la productividad y la competitividad del territorio. En áreas como la movilidad inteligente se pretende introducir mejoras dentro de los sistemas de transporte público existentes o crearlos. Los últimos elementos que son el de ciudadanía inteligente y el modo de vida inteligente, el primero engloba las condiciones que permiten la participación efectiva de la ciudadanía, mientras que el segundo significa llevar las tecnologías más allá de los servicios tradicionales, es decir procurando que estas incidan en otras áreas (por ejemplo al utilizar una solución tecnológica para el turismo a lo interno de la ciudad).

Con respecto a los beneficios de la ciudad inteligente se pueden mencionar los siguientes: la capacidad para mejorar el trabajo que realizan las administraciones públicas (mejoras que se manifiestan en la digitalización y simplificación de trámites, la reducción en el uso de papel y la implementación de servicios más eficientes y eficaces), facilitar el análisis de lo que ocurre en la ciudad a partir de la integración de las TIC (por ejemplo para crear plataformas especializadas, colocar sensores ambientales o identificar el tipo de usuarios y calidad de servicios que se brindan en la ciudad) y puede propiciar la participación ciudadana creando canales especiales para ello, entre otros. Gracias a esto no solo sé que ocurre en la ciudad, sino que también puedo producir datos e información que al fin y al cabo termina por ser utilizada en procesos decisorios, en rendición de cuentas y para canalizar mejor ciertas demandas ciudadanas.

Si bien es cierto que varios de estos beneficios vienen a ser grandes promesas para potenciar este tipo de iniciativas en centros urbanos o en otro tipo de territorios, hay importantes vacíos y debilidades con respecto al concepto de ciudad inteligente. De igual modo, se han hecho múltiples críticas en relación a lo que pregona este concepto.



Una de las críticas más notorias considera que, la noción trata de posicionar o plantear una serie de objetivos que a simple vista no parecen ser compatibles y que en términos prácticos no siempre aparecen como los más alcanzables en la realidad. Asimismo, hay poca referencia a experiencias prácticas que hayan sido exitosas y tampoco se habla de cómo deberían llevarse a cabo procesos de ciudad inteligentes.

También existe un gran vacío en cuanto a la gestión y temas administrativos, pues no se dice qué implica organizar un proceso de esta índole ni qué clase de decisiones o cambios específicos deben realizarse, aparte de todo el tema que está vinculado con la infraestructura. Si bien es cierto que se habla de los múltiples beneficios que traerá la producción de datos y como puede eso potencialmente mejorar los procesos y decisiones –al ser más informadas–, son pocas las referencias al manejo de dichos datos. Tampoco se precisa a quiénes pertenece la información o como debería gestionarse.

Otro de los aspectos no abordados es el hecho de que al automatizar los servicios a lo interno de las ciudades, queda por fuera el tema sobre cómo hacer o gestionar la seguridad en estos espacios, sobre todo si se considera que hay una gran cantidad de información que está circulando a lo interno de la ciudad y la cual se debe gestionar adecuadamente. Asimismo, a pesar de que se habla de la participación ciudadana y la coproducción, no se enfatizan las condiciones que deben darse para que eso se pueda llevar a cabo.

Por otro lado, se considera que el excesivo protagonismo que se le da a las TIC puede dar la falsa impresión de que algunos de los problemas que se pueden dar a lo interno de las ciudades son algo meramente técnico, despolitizándolos y minimizando la complejidad de estos para verlos como problemas que solo requiere de la aplicación de TIC para su resolución. En esa línea también queda el cuestionamiento de si las ciudades podrían estarse convirtiendo en sitios que no sean adecuados o deseables para vivir, sobre todo si pensamos en aplicaciones como la bioanalítica facial con propósito de mejorar la seguridad ciudadana en estos espacios, lo cual plantea todo un dilema ético.

La ciudad inteligente puede ser confundida con otras nociones como las de *comunidades inteligentes* y *campus inteligentes*, los cuales se registran a espacios muchísimo más controlados y reducidos. Con el término de comunidades inteligentes la principal diferencia es que la tecnología está destinada a introducir cambios en estilo de vida de una población, pero se pierden de vista aspectos como la participación ciudadana, el manejo de datos o la producción de datos o servicios y en ese sentido, es un concepto más vinculado a la dotación de infraestructura TIC al espacio urbano.

El campus inteligente se distingue de la ciudad inteligente por la escala territorial y porque implica un proceso de digitalización de los servicios y gestión que se ofrecen a lo interno de un campus universitario. Otro término hermano es de *Ciudad Conectada* o la *Data City* que vienen a ser casi lo mismo y en los que se enfatiza es la generación de grandes cantidades de datos.

De todos los conceptos similares a los de ciudad inteligente, el más relacionado sería el de *ciudad digital* el cual recoge algunos elementos de ciudad inteligente, pero con la principal diferencia de que la ciudad digital se centra más en la digitalización y la creación de servicios digitales. Por ello, pierde de vista elementos más sistémicos que sí aborda la ciudad inteligente. Además, no necesariamente en una ciudad digital deben buscarse otros objetivos que vayan más allá de la digitalización.

Para hablar propiamente del *territorio inteligente*, es importante mencionar que este término se plantea como

una respuesta crítica al hecho de que solo los espacios urbanos puedan ser considerados como inteligentes. Esto plantea la pregunta de ¿qué sucede con los espacios que no concuerdan con los criterios de lo que se considera como urbano? Es así como surge el concepto de territorio inteligente el cual es muy similar al de ciudad inteligente pero que está vinculado con la interacción entre ciudades, ecosistemas y espacios rurales, lo que hace que pueda ser considerado como una interacción entre estos distintos espacios los cuales además tratan de responder a los desafíos de la globalización.



A partir de esto, los territorios inteligentes empiezan a ser pensados como un espacio en donde lo que se busca es aprovechar las ventajas competitivas de ese territorio y de establecerlas o tratar de asegurarlas a través de una serie de políticas específicas, legislación o estrategias para hacer más atractivo el territorio. Así tienen la particularidad de que son planificados por las personas que habitan estos espacios, lo que supone una planificación no solo pensada en función del mercado sino también un esfuerzo por integrar las necesidades y requerimientos de la población y otros actores relevantes dentro de ese escenario, implicando un diálogo multisectorial entre esos intereses y necesidades.

La innovación es sumamente importante dentro de ese territorio, por lo que se busca establecer ciertos mecanismos político-administrativos eficientes así como medios de cooperación interinstitucional con el fin de fomentar el planeamiento conjunto entre actores, potenciar el desarrollo de infraestructura de telecomunicaciones e infraestructura TIC y un diálogo con el entorno que implica pensar el territorio en función de recursos y necesidades ambientales.

Existe otro concepto que está relacionado y que ha sido denominado como *smart region* (región inteligente) que es similar al de territorio inteligente, pero que está pensado únicamente para espacios rurales o al establecimiento de redes intermunicipales que desarrollan iniciativas de ciudad inteligente, generando interconexión entre las mismas.

Para finalizar, me gustaría hablar un poco sobre ciertas iniciativas vinculadas con proyectos de ciudad inteligente que han sido puestos en práctica en el país y de cómo justamente el tema de la digitalización viene a ser el paso número uno para potenciar este tipo de procesos. Estos hallazgos derivan de una investigación que se realizó en 2018 e inicios de 2019 en el tema de ciudades inteligentes y la cual pueden revisar con mayor profundidad en el sitio web www.prosic.ucr.ac.cr. Con respecto a estos casos, debo mencionarles en primer lugar a la Municipalidad de Cartago.

Esta tiene un amplio desarrollo en términos de digitalización y ha generado una serie de iniciativas muy específicas en distintos ámbitos. Yo solo voy a hablar del sistema de información geográfica (SIG) que han implementado. Desde 2008, la Municipalidad de Cartago ha planteado un proyecto llamado *Cartago Ciudad Histórica Digital* el cual pretende convertir al municipio en una de las primeras ciudades inteligentes del país. Este es un proyecto al que cada año, se le agrega más proyectos en más áreas. Como parte de este proceso de digitalización se estableció la *Agenda Digital*, que es una cartera de proyectos con acciones específicas y en las que se estableció como prioritario un SIG. Poco a poco se comenzó a trabajar en dicho proyecto de tal modo que a la fecha el SIG tiene más de trescientas capas de información actualizada, geo-referenciada en donde las y los usuarios pueden acceder a esta plataforma y consultar un sinnúmero de datos distintos sobre el cantón y la municipalidad.

A partir de la introducción de este sistema se desarrollaron aplicaciones específicas para la institución. Por ejemplo, la Policía Municipal cuenta con un app para el levantamiento o la identificación de infracciones y además permite que el usuario revise esta información en línea (cuánto debe, qué tiene, pendientes de cobro). Desde la implementación del SIG no sólo ha mejorado la detección de infracciones sino también la recaudación de ingresos por concepto de multas.

La digitalización o implementación de elementos de gobierno electrónico/digital en las municipalidades del país ha permitido que en algunos casos como la Municipalidad de Belén, la Municipalidad de Montes de Oca más recientemente y la Municipalidad de Palmares, cuenten con más datos e información y mejoren su recaudación. Este último aspecto produce una gran diferencia, un antes y un después a partir del momento en el que se empiezan a utilizar este tipo de soluciones y se empieza a utilizar internamente.

En el caso de la Municipalidad de Palmares, el visor cartográfico tiene multiplicidad de capas de información que son alimentadas internamente por una persona de la municipalidad que está destinada a realizar esta tarea. La disposición de esta herramienta ha sido tan exitosa que ha llegado a convertirse en una herramienta importante para los topógrafos que trabajan en este cantón, porque el visor no solo despliega la información sino también permite hacer análisis o mediciones específicas.

Finalmente, el caso de la Municipalidad de Curridabat destaca porque desde el 2015 ha adoptado una aplicación móvil que se llama “*Yo alcalde*”, lo que permite que la población mediante sus celulares pueda notificar problemas específicos que ha detectado en su comunidad. La aplicación cuenta con una serie de categorías específicas que están conectadas a un tablero informativo que tiene la municipalidad a nivel interno. Las personas usuarias

pueden verificar el estado de la solicitud, el tipo de trámite que se está haciendo, cuánto va a durar y quién lo tiene. Con esto se hace cierto control cruzado de modo que no solo a nivel interno se puede ver el estado de la solicitud sino que también lo puede ver la persona usuaria. Esto ha servido para generar estadísticas internas que al fin y al cabo han alimentado los procesos de toma de decisiones de la municipalidad.

Estos son sólo algunos ejemplos de esfuerzos que se han realizado en esta línea y que quería traer a colación sobre todo por el tema de la digitalización, que viene a ser un elemento central para propiciar este tipo de procesos, así como un escalón previo para alcanzar la ciudad inteligente. Estos ejemplos muestran algunos de los beneficios que puede traer la adopción de iniciativas de ciudad inteligente y que si bien refieren a casos municipales, imaginen las posibilidades que podrían traer a otras instituciones de acuerdo a las necesidades que estas tengan.

Muchas gracias.





Cultura o cambio organizacional y las características del recurso humano

Juan Miguel Castillo Fonseca

Universidad Autónoma de San Luis Potosí. México. Facultad de Ciencias de la Información

Para iniciar este tema un poco complicado voy a tratar de explicar un poco en lo que me basé para construir esta idea pues son varios los temas que se entrelazan en esta conferencia.

Si vemos el título de la conferencias, notaremos que hay tres temas inmersos: la cultura organizacional, el cambio organizacional y las características del recurso humano. Siguiendo el índice, voy a dar una introducción. Luego, hablaremos de lo que es la cultura organizacional, el cambio organizacional, las consideraciones para el cambio organizacional. Esto último lo trabajo desde un enfoque de sistemas y desde la tecnología suave o «*Soft Technology*». Para concluir, veremos las características del recurso humano, liderazgo, motivación.

Lo que hemos visto es que en la actualidad las organizaciones se ven obligadas a estar en constante cambio. Sin embargo; dichos cambios que estamos viviendo son demasiado rápidos y muy pocas organizaciones logran adaptarse a ellos para poder competir y para poder solucionar sus problemas. Entonces se van perdiendo en el camino por no tener las capacidades para poder sobrevivir. Igual veíamos que la información es uno de los ejemplos; la gente del siglo XVII, con un periódico del domingo prácticamente tenía toda la información que podía recibir.

También vamos a ver que la cultura organizacional nos está representando un conjunto de valores, creencias, rutinas y comportamientos generalizados mientras que el cambio organizacional es un conjunto de cambios estructurados y definidos, visiones nuevas y escenarios prospectivos. Por lo tanto, si pensamos en un cambio nuevo, el recurso humano es fundamental, principalmente para el manejo de la información y la tecnología. Es decir, las personas y los nuevos perfiles de capital humano se deben ajustar a la exigencias de la globalización.

Las organizaciones que pervivan serán solo aquellas que entiendan la necesidad de una adecuación rápida, a veces vertiginosa, a nuevos entornos económicos, nuevas técnicas y tecnologías aplicadas a los procesos. Comenzamos por el informativo y la toma de decisiones, por lo que las características del recurso humano representan ese valor agregado que puede marcar la diferencia.

Si se quiere llegar a un clima organizacional adecuado, se debe tener un equilibrio entre la cultura y el cambio organizacional. Esto es simple si consideramos a la organización como un sistema y tenemos en cuenta lo que significa la entropía (teoría del caos) y la homeostasis (equilibrio). Por lo anterior el recurso humano es trascendental para lograr dicho balance.

Manuel Castells lo vaticinaba y en una de sus publicaciones, “La aldea global”, decía que estos cambios representan en las organizaciones “un proceso de reestructuración profundo, caracterizado por una mayor flexibilidad de la gestión; la descentralización e interconexión de las empresas, tanto interna como en su relación con otras, aumento de poder considerable del capital frente al trabajo.” Asimismo, indicaba que “las redes informáticas interactivas crecen de modo exponencial, generando nuevas formas y canales de comunicación, y dando forma a la vida a la vez que esta les da forma a ellas.” Esto tiene que ver con estos cambios sobre las cuestiones digitales, sobre las nuevas tecnologías que se han desarrollado y cómo las organizaciones tienen que operar o ajustarse para poder sobrevivir a dichos cambios.

Para entrar en el tema y no tener tanto texto, voy a ir a la parte de imágenes para poder entender más rápidamente este tema. Estuve revisando por qué están fracasando las pequeñas y medianas empresas, en el caso de Costa Rica principalmente. Hoy vamos a ver un poquito como está esa situación en el país.

Aquí podemos ver en una publicación que generalmente el noventa por ciento de las pequeñas y medianas empresas truenan entre los tres y cinco años, es como el máximo que tienen muchas de ellas. Es lo que duran en el negocio y generalmente tiene que ver con la falta de profesionalización; es decir, inician con buenas intenciones, con muchas ganas, pero en el camino se dan cuenta que les hacen falta recursos humanos o gente profesional que impulse a la empresa de verdad. Entonces a veces no todas las empresas familiares duran, también terminan hasta peleados por estas cuestiones; pero sí tiene que ver la falta de profesionalización en estos casos.

También podemos ver en el caso de Costa Rica que han estado cerrando varias empresas. Podemos ver que el 29 de mayo existe un ejemplo de una textilera que cerró operaciones. También en Nicaragua y en toda Centroamérica han estado cerrando empresas. Una aerolínea también tiene suspendida una flotilla y desde el 2015 existen algunos indicios de empresas de comidas rápidas que han estado cerrando. No es para menos tener el caso de “Sears” que también está teniendo problemas y está a punto de cerrar, a pesar de ser una empresa grande. Entonces esto está afectando a todas las empresas y a muchas instituciones. Generalmente tienen problemas en varios de los puntos que voy a considerar, para que los podamos revisar.

Entre los factores de riesgo que existen se encuentra, en algunas ocasiones, el propio liderazgo. La dirección no tiene una visión completa de la organización o no logra tener el alcance adecuado y el equipo a veces no está bien armado, con personas profesionales o con gente que debe estar en el puesto adecuado. Eso produce que, obviamente, no se lleve a cabo bien el trabajo, además de una estructura salarial que no es tan buena. Y en el mercado en ocasiones no se estudia al cliente que es el que les indica sobre la mala atención que tienen, sobre los servicios que reciben y no existen estudios en esos casos, no se tienen planes de negocios, no se determinan objetivos ni se genera una planeación estratégica mayor a futuro. Y es así como ignoran que si no planifican o no estudian algunas consideraciones, hasta vender más es riesgoso, porque no se tiene la capacidad para vender tanto.

Entonces ahí se tienen que tener consideraciones, como en la operación. A veces no tienen controles en los procesos productivos y en los servicios que se ofrecen, entonces hay altos costos por desperdicio, en insumos que se compran y no se utilizan y no existe una dosificación de todo esto. En ocasiones no se evalúan los proveedores y se tienen más por amistad o por recomendación de otros que por análisis propio de las empresas. Los resultados: no se tienen indicadores reales sino que se dice “vamos más o menos”. Sin embargo, no se sabe realmente con estadísticas y la mejora continua no existe porque solo van sacando el día a día y se atienden los

problemas cuando van saliendo en la organización. Este sería como el preámbulo de lo que esporádicamente sucede en las organizaciones.

En relación con la cultura organizacional, algunos autores la definen precisamente como estas creencias, valores, hábitos, tradiciones, actitudes y experiencias que tienen en la organización y generalmente es tratar de controlar el modo en el que las personas interactúan entre ellas y con el exterior para relacionarse. En otras palabras, es el alma de la empresa; esta cultura organizacional está formada por personas. Entonces los empleados y los proveedores, tanto desde la parte interna como de la parte externa, son los que de alguna manera se tienen que cuidar o vigilar.

La importancia de la cultura organizacional es que tiene dos grandes ejes. Principalmente uno interno que es la relación del personal con los directivos y el clima laboral, entre otros. El segundo es su relación con la sociedad, con la parte externa: el medio ambiente, las actividades sociales de caridad, gubernamentales. Es decir, es la cara o la imagen que da una empresa, como aquellas empresas que colaboran en la parte social, en la parte ecológica, en la parte humanitaria. Es una imagen de colaboración que a veces muchas empresas tienen en su cultura organizacional.

Dentro de la cultura organizacional existen diferentes elementos que la constituyen y que los empleados de alguna manera tienen que identificarse. Debe de haber una identidad de organización; es decir, qué tipo de empresa es, a qué se dedica, qué hace, que yo conozca precisamente la empresa en que trabajo. Es necesario que existan sistemas de control para poder manejar las conductas, los reglamentos, la normativa que existe. Igualmente se necesita una estructura de poder que también se tiene que definir: quiénes son los jefes, los gerentes, la gente que está al frente. Debe haber ciertos símbolos que identifican a la empresa o a la institución, logos o imágenes en particular, rituales y rutinas de la vida en la organización; algunas acostumbran hacer juegos cada año, por ejemplo. Entonces estas cuestiones se convierten en ciertos rituales o rutinas que en un momento dado los empleados utilizan.

También tenemos las historias, los mitos, las anécdotas de cómo creció esa empresa: que nació en un carrito en la calle, en la esquina, y luego hubo tres y cuatro hasta que fueron creciendo. Estos son elementos que constituyen precisamente parte de esa cultura organizacional y que los empleados deben de conocer o la gente que labora en ellas.

Hasta ahí vamos bien todavía, es la parte bonita. Sin embargo, vamos a ver más adelante las resistencias que a veces se encuentran ante el cambio. ¿Cómo pasar de una cultura organizacional a un cambio organizacional? Este cambio organizacional es la capacidad de adaptación de la organización a las diferentes transformaciones que sufre el medio ambiente interno o externo mediante el aprendizaje. Otra definición indica que es un conjunto de variaciones de orden estructural que sufren las organizaciones y que se traducen en un nuevo comportamiento organizacional. El cambio organizacional es aquella estrategia ^{uw} se basa en la visión de la organización para que exista un mejor desempeño administrativo, social, técnico y de evolución de mejoras. Forzosamente tenemos que estar cambiando, no podemos quedarnos con una cultura organizacional que algunas veces se corrompe, se daña y que lleva a las empresas incluso al fracaso o a quebrar.

Este cambio organizacional tiene algunos modelos que se han propuesto: diagnosticar cuál es la cultura actual que tienen, definir los cambios culturales que existen, identificar comportamientos deseados, desarrollar programas para generar compromisos de la gente, modelar roles de los líderes, alinear sistemas y procesos. Generalmente

los cambios se originan por interacción de fuerzas que generalmente son internas y externas. Por un lado las internas son aquellas que provienen dentro de la organización y las externas son las que generalmente vienen por el medio ambiente o los cambios que existen alrededor de la empresa, económicos, sociales.

Cuando hablamos del cambio organizacional vamos a notar que también existe mucha resistencia porque es muy fácil decir “bueno, vamos a hacer un cambio en la organización, vamos a hacer mil cosas y vamos a vivir en el mundo feliz”. Pero esa es la parte difícil, cómo lograr un cambio organizacional efectivo y que realmente la gente quiera participar.

Generalmente encontramos muchas causas, como el miedo a lo desconocido, la falta de información o desinformación, algunos factores históricos, amenazas al estatus, a los expertos o al poder. También hay amenazas al pago y otros beneficios, clima de baja confianza organizativa, miedo al fracaso, resistencia a experimentar, poca sensibilidad organizativa, aumento en las responsabilidades laborales, temor a no poder aprender las nuevas destrezas requeridas o nuevas tecnologías. Generalmente todo esto sucede cuando nos dicen que va a haber un cambio organizacional o incluso llegan nuevos jefes o llegan nuevos personajes, siempre existen miedos, dudas y ciertas cuestiones que hacen que a veces la organización quede con incógnitas.

Un autor que leí menciona cuatro aspectos para lograr este cambio organizacional. Estos puntos me parecieron interesantes y creo que se pueden adaptar muy fácilmente a las organizaciones. Jay A. Conger ha hecho algunos experimentos con Dow Chemical y Toyota. Él dice que se tiene que hacer atractivo el cambio para el personal; es decir, convencerlos de que vale la pena cambiar y los beneficios que van a tener con dichos cambios. Es necesario generar seguidores al cambio.

La organización debe de alinearse desde la parte directiva, con las partes de la estructura jerárquica que se tiene para poder todos buscar el mismo objetivo y las mismas metas, que cada uno conozca lo que tiene que hacer para lograr conseguir el objetivo y de alguna manera enfrentar la parte de la resistencia. Es decir, es necesario tratar de hacer entender a las personas que tienen esa resistencia que tienen que cambiar porque si no se hace, de alguna manera la empresa no va a poder sobrevivir o va a tener problemas más adelante.

Algunas consideraciones que tuve para el cambio organizacional, es principalmente el enfoque de sistemas. También se debe tener en cuenta que todos conocemos la parte de un sistema que es un conjunto de elementos que interactúan entre sí para tener un objetivo común, un conjunto ordenado de procedimientos relacionados que contribuyen a realizar una serie de funciones, pasos o procedimientos que permiten obtener un resultado predeterminado, un conjunto de partes, elementos, componentes con funciones interrelacionados que conducen a un fin específico. El autor Peter Checkland dice “que un sistema engloba un grupo de elementos conectados entre sí que forman un todo que muestra propiedades que son propiedades del todo y no propiedades de sus partes que son componentes”.

En el caso de los sistemas de gestión o gestión de información en la parte de las empresas -esto tiene que ver con archivos-, son acciones y procedimientos planificados y organizados por medio de los cuales se busca conseguir el mejoramiento de productos y servicios. La gestión de documentos ha sido definida como un proceso-programa de acción que pretende normalizar el ciclo de vida de los documentos en las organizaciones desde su planificación hasta su eliminación o conservación permanente sin importar el medio.

Michelle Duchein dice que desde el punto de vista de los archivos administrativos, la empresa es como un sistema que pretende organizar y racionalizar la gestión de los fondos desde el mismo momento de la producción de los documentos hasta su ingreso a los Archivos Nacionales, interviniendo en el trabajo de las oficinas y los servicios administrativos en las distintas etapas del tratamiento de los fondos.

Actualmente, por lo menos en la práctica, todas las empresas deben contar con un sistema de gestión de archivos, un sistema de gestión documental y deben de caminar hacia los sistemas de preservación documental. Entonces, en la parte de sistema de gestión de archivos, los especialistas en archivos o en información deben de considerar lo siguiente: siempre diagnosticar primero como está la parte de los archivos, como una unidad de información, es decir, qué funciones, actividades, programas y manuales existen. Deben de atender las políticas nacionales o internacionales para poder aplicarlas de forma precisa. Además, deben de tener la capacitación –volvemos a esta parte del recurso humano-, estar profesionalizados o de alguna manera se debe contar con los elementos mínimos para entender estos cambios. Por último, se deben generar programas de gestión de archivos en su empresa o institución, en este caso considerando mínimamente estas unidades.

El otro sistema que podemos tener es el sistema de gestión documental que va a detectar varias cosas. Por ejemplo, cómo está la parte de la documentación, cómo está la parte de los espacios físicos donde se guardan los archivos, los servicios que se ofrecen, los recursos humanos, materiales con los que cuenta. Igualmente tiene que analizar la normativa, las políticas que se deben visualizar, la capacitación del personal, la sensibilización, mandos medios, personal en general y personal especializado y desarrollar todo un programa de gestión documental para la empresa o la institución. Generalmente, dicho programa tiene los elementos básicos que son: considerar la producción documental, la recepción, la distribución, el trámite, organización y consulta de los documentos, la conservación de documentos físicos y digitales y la disposición final de los mismos.

Hasta ahí es la parte física. Ahora, ¿cómo está la parte de las tecnologías? que es donde estamos varios. En la parte de la preservación digital tenemos que analizar otras cosas también, por ejemplo el *hardware* y el *software*, los recursos humanos, financieros, técnicos y también detectar las fallas que existen en los sistemas de gestión de documentos y de archivos porque estos nos van a dar las bases para desarrollar este sistema de preservación digital. Igual tendríamos que aplicar normativas, normas en relación a documentos electrónicos o digitales como la norma 30300, la norma 30301, la familia del ISO 300, considerar la norma 15489 y volver a capacitar nuevamente a la gente en un sistema de preservación digital. Con esto vamos a poder desarrollar un programa de preservación digital con el que vamos a dar mantenimiento, actualización, migración, estimulación, preservación de la tecnología y la arqueología digital.

Estos términos, por lo menos la arqueología digital, ahora se constituyen como un elemento para los discos que teníamos de 3 1/2. Para esos discos que de alguna forma teníamos dañados ahora existen especialistas que se encargan de rescatar la poca información que pudiera existir todavía en ellos o en estas tecnologías obsoletas. Pero aun así tenemos situaciones que debemos resolver: al tener una interoperabilidad sistémica, tenemos los sistemas (de gestión de archivos, de gestión documental y de preservación documental). Sin embargo, todos los sistemas en las mismas organizaciones tienen ciertas problemáticas y generalmente tienen que ver con la entropía y la homeóstasis.

En este caso, la entropía es la teoría del caos. Los sistemas siempre tienden a fallar o a descomponerse, a fallar en algunos puntos. Por esta razón es importante tener la homeóstasis, o la teoría del equilibrio, que que nos ayuda a autorregular que los sistemas no fallen, que exista control y mejoras. En estos dos puntos de esta

interoperabilidad sigue prevaleciendo el recurso humano; es decir, no se logra sin las personas trabajando para que estos sistemas se mantengan y para que esta organización mantenga tanto cultura y quiera lograr sus cambios organizacionales.

Actualmente se está trabajando (se está retomando una idea aparentemente nueva, aunque no lo es) porque se habla de la tecnología suave o «*Soft Technology*». En realidad siempre hemos vivido con ella. El tema habla de tecnologías duras y de tecnología blanda o suave. Mientras la tecnología dura son todos aquellos elementos tangibles, la tecnología suave son todos los elementos intangibles. Entre estos últimos están los recursos humanos. Entonces el mismo recurso se convierte en una tecnología suave que aporta conocimiento a las organizaciones para desarrollar nuevos esquemas.

Ahora vamos a ver un poquito de esta parte de la tecnología suave y es lo que les comentaba. Es un conjunto de conocimientos tecnológicos o de naturaleza administrativa, comercial y organizativa y la tecnología abarca conocimientos, procedimientos, metodologías, disciplinas, habilidades que permiten el desarrollo posterior de productos y servicios. Por esta razón el concepto equivale en el saber hacer o «*Know how to do*» prácticamente que tienen las personas por sus características. Como les comentaba, este concepto surge a la par de la idea de las tecnologías duras, aunque ambos tienen en común su relación con el campo científico, el desarrollo de bienes y servicios. Esta tecnología blanda o suave es la parte intangible; gracias a ellas las personas poseen las habilidades necesarias para adaptarse al entorno tecnológico o a las organizaciones de manera efectiva.

Como es razonable, sin la tecnología suave (es decir, sin el conocimiento) la tecnología dura no sería posible. Es necesario poseer las habilidades cognitivas anteriores que hacen realidad las creaciones y los avances de liderazgo. Está el líder que es coercitivo (“haz lo que te digo”), el que es orientativo (“ven conmigo”), el afiliativo (“crea armonía o trata de llevarse bien con las personas”), el que es democrático porque busca los acuerdos, el que es ejemplar y el que es formativo. Entonces existen varios tipos de líderes. Las personas que van a trabajar en las empresas o que actualmente trabajan en ellas de alguna manera deben de tener estos elementos, que les han ayudado a sobresalir y desarrollar cosas importantes.

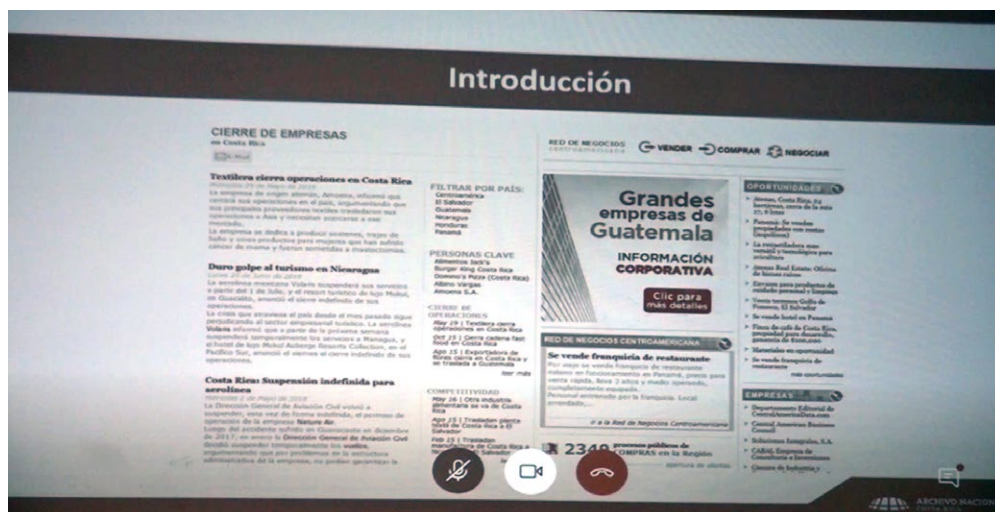
Otra de las características que veo en la parte del recurso humano que es muy importante, aparte de tener unas características de líder, es la motivación que siempre deben de tener. La palabra motivación es el resultado de la combinación de los vocablos «*motus*» (del latín = movimiento) y el otro «*motion*» (inglés, que significa movimiento). A juzgar por el sentido que se le atribuye al concepto desde el campo de la psicología y la filosofía, una motivación se basa en aquellas cosas que impulsan a un individuo a llevar acabo ciertas acciones y a mantener una firme conducta hasta lograr cumplir todos los objetivos planteados. La noción, además, está asociada a la voluntad y al interés. En otras palabras, puede definirse a la motivación como la voluntad que estimula a hacer un esfuerzo con el propósito de alcanzar ciertas metas. Es como las dietas; muchas veces si no tenemos esa motivación, esa voluntad, las dietas no funcionan.

¿Qué características o qué beneficios tiene la motivación? Tiene varios beneficios: genera conductas activas y persistentes, autoestima, autorrealización, logros, reconocimiento, y genera impulso. Entonces las organizaciones tienen que considerar todos estos elementos de las características del recurso humano, si quieren en algún momento lograr sus cambios organizacionales y si quieren establecer culturas organizacionales nuevas. Por esta razón es importante considerar todos estos elementos que les he platicado, porque de alguna manera los estamos viviendo en las instituciones o en las empresas. Y si queremos que las empresas no fracasen es importante que tengan recurso humano preparado o capacitado y que además aporte ideas. Es decir, la competitividad de

ahora está con las tecnologías, el desarrollo del *software*, de mecanismos, de estrategias que generalmente las desarrollan las personas.

Como conclusiones al tema, podría decir que la cultura organizacional sí existe en las organizaciones, pero es un tema que debe entenderse para poder cambiar. La supremacía de las organizaciones depende de sus recursos humanos como el principal activo de generación de conocimiento. El cambio organizacional depende de todos, desde un enfoque de sistemas deben de considerar todas las partes de la organización. Los especialistas en el manejo de la información deben entender los nuevos cambios a los que se deben de enfrentar, los profesionales de la información deben ser líderes en su área de conocimiento y fomentar los cambios. Finalmente, las tecnologías duras o blandas no se desarrollan sin los seres humanos.

De mi parte esto ha sido todo en la exposición, les agradezco mucho.





El valor público en la era digital

Luis Antonio Román Hernández

Gerente del Área de Modernización del Estado del Ministerio de Planificación.

Buenas tardes. Agradezco muchísimo la participación del Ministerio de Planificación (Mideplan) en este evento tan importante para ustedes y para todo el país. La ministra de Planificación pide una disculpa porque tuvo que acompañar al presidente en una prioridad de gobierno y me solicitó que viniera a hacer una exposición sobre el tema, el cual, a pesar de no ser de actualidad, es de suma importancia.

“El valor público”, el concepto es muy amplio y tiene diferentes acepciones, el punto es encontrar armonía con nuestro ordenamiento jurídico interno y con el contexto nacional. Por lo tanto en Mideplan desarrollamos el concepto asociado con la planificación estratégica. ¿Qué es el valor público? Es el bienestar común. Es decir, el bien supremo del Estado costarricense. El artículo 50 de la Constitución Política establece que el Estado está en la obligación de procurar el mayor bienestar a todos los habitantes de la República. Es muy amplio y está dentro de un contexto de respeto a todos los derechos humanos y de igualdad; no hace distinción entre extranjeros o costarricenses, sino que habla de todos los habitantes de la República.

Ese concepto de mayor bienestar es el norte que debe tener el Estado costarricense en su modelo de desarrollo, porque realmente hacia eso nos lleva la Constitución Política. Lo que sucede es que la tendencia -y no de solo de Costa Rica, sino del mundo- ha sido un poco deshumanizada y los intereses particulares han ido creciendo y han ido incrementándose en todos los niveles de gobierno y no de gobierno, como la prevalencia de los intereses privados sobre los intereses públicos o comunes.

Entonces, ha ido dejando de tener importancia. Inclusive el Estado mismo brinda servicios y bienes. Sin embargo, no lo hace en función del bienestar que van a producirle al gobernado (es decir, al usuario). Cuando se busca el valor público - yo lo veo como un concepto muy jurídico-, es mejor para mí hablarlo desde una perspectiva, como bienestar común para poderlo lograr. Además, necesito establecer políticas claras en las diferentes áreas que permitan llegar a la ciudadanía y poder rescatar qué es lo que esta quiere.

Porque el valor público o el bienestar común es aquel que los ciudadanos dicen que necesitan, no el que el estado cree que la ciudadanía necesita. Ese elemento es fundamental, por eso lo vemos como el fin buscado por las personas, por el Estado y por los funcionarios públicos. Esos tres actores deben tener claro que todo servicio o producto que produzca una institución debe generar valor público; es decir, debe generar bienestar.

Vamos a ver un ejemplo, cuando hablamos de valor público en el Instituto Costarricense de Electricidad (ICE), yo les digo “identifiquemos el valor público en esta institución”, y ustedes me dicen “brinda servicios de electricidad a todo el país”. Entonces si hacemos un análisis vemos que ese es el valor privado, lo que se le presta

al ciudadano desde un punto de vista privado. Pero el valor público que tiene el ICE, que se desprende de sus competencias, ese valor público es la cobertura que la institución brinda en el país.

Veámoslo con el internet que es una cuestión más reciente y fue desarrollándose en ciertas áreas del país, ha ido avanzando. Supongamos que el internet no se brinda por entes privados sino por el ICE nada más. Entonces el ICE viene y da cobertura a la zona de San José, pero en el próximo gobierno, por ejemplo, se propone ampliar esa cobertura a la provincia de Guanacaste o hacia la provincia de Limón; entonces ahí lo que estamos generando es el valor público que el ICE produce. Si hablamos de la cobertura telefónica, el incremento de ese valor debe irse previendo en cada plan de la institución (aplicaría también, por ejemplo, para la institución que produzca energía eléctrica).

Desde el Mideplan, desarrollamos una metodología para formular un plan estratégico con enfoque de valor público para que las instituciones puedan llegar a identificarlo. Nosotros vamos a tratar de dar un acompañamiento y una asesoría porque no es fácil, ya que es un concepto que no ha sido manejado a la hora de definir e identificar los bienes y servicios de una institución. Una vez definido esto, preguntamos si está generando un bienestar a la población o a un sector; de lo contrario, ese servicio público o producto no debe seguirse gestando.

Esto del valor público está siendo introducido mediante la aplicación del modelo de gestión para resultados y el desarrollo que el gobierno de la república acogió - hace como dos años -, para que las instituciones orienten su propia gestión. Celebramos que eso esté aconteciendo a nivel gubernamental ya que hace valer lo que la Constitución Pública estableció hace más de cincuenta años, que nosotros nunca debimos haber perdido la perspectiva de que la gestión pública debía orientarse específicamente hacia un norte, que era generar el bienestar común no solo de ciertos grupos, porque de eso se trata la democracia, de generar condiciones y calidad de vida a todos los habitantes.

El concepto lo venimos trabajando a nivel metodológico. Es decir, el modelo de gestión institucional que estamos proponiendo para todas las organizaciones públicas ya está en la página de Mideplan, con el fin de iniciar el proceso de mejoramiento que se va a implementar en los ministerios el año entrante. Ya estamos alistando el material y quizá en un mes podríamos tenerlo en la página y ustedes lo podrían utilizar para que se vayan familiarizando con el instrumento y con la temática.

Definimos el valor público como el bienestar colectivo creado por el gobierno y las entidades públicas, no es apropiable a ninguna persona en especial (eso es valor privado), cubre amplios segmentos de la sociedad o su totalidad y tiene un gran impacto en ella, estos son sus elementos fundamentales. Las condiciones para la generación del valor público son varias en un gobierno como el nuestro en vías de desarrollo, porque los estados en desarrollo ya tienen otra perspectiva de lo que es. Para ellos casi que las necesidades ya son limitadas; es decir, no son muy grandes. La generación de valor público se extiende en los países en desarrollo puesto que se requiere de muchas necesidades para generarlo.

Ahora vean lo importante de esto. Cuando yo hablo de las necesidades es porque depende estrictamente de lo que definan los ciudadanos. Esto se lo quiero dejar en una primera instancia para aclarar ese concepto, porque nosotros tenemos un elemento del nuevo modelo de gestión pública que estamos proponiendo que tiene como variable la participación ciudadana y ese es otro componente importante en nuestra definición como Estado.

Hablando del Estado, este se concibió con la participación del ciudadano. Es decir, porque las instituciones están

creadas para el servicio público; no son un fin en sí mismas y las organizaciones han perdido la perspectiva de que todas deben responder a los intereses nacionales, al desarrollo. La institución que no esté vinculada al desarrollo nacional debe desaparecer, no porque quiera cerrar instituciones, sino que la lógica me dice que la institucionalidad es el instrumento del Estado para alcanzar el desarrollo. Eso significa que toda institución debe generar desarrollo a través del valor público, identificándolo desde su competencia, desde lo que le asigna la ley.

Simplemente es una cuestión de que esa institución, cuando hace su planificación estratégica y define sus productos, debe necesariamente llamar al ciudadano, a sus usuarios y decir, ¿qué es lo que necesita? Yo puedo hacer esto, esta es la competencia, pero nada más porque la administración está sujeta al principio de legalidad y dentro de lo que yo debo hacer, el ciudadano es el que tiene que decir cómo y qué quiere, definir sus necesidades y expectativas para considerarlo en la planificación porque si no es así, ¿dónde está lo estratégico?

Para que una estrategia impacte en el desarrollo, no es que una institución haga 200 bollos de pan al año - con suerte no tenía que hacer ni pan-, porque ni siquiera sabe qué es lo que tiene que generar, entonces sencillamente ahí la esencia está en la institución. No es solo la planificación estratégica, deben identificarse los productos y los servicios y cuando los voy a establecer tengo que hacerlo con la población meta, porque si no los están definiendo los funcionarios públicos, ¿cuál va a ser el efecto de ese servicio? Posiblemente un servicio que deja insatisfacción, si no estamos tomando en cuenta las necesidades y las expectativas.

Imagínense si ni siquiera se toma en cuenta al ciudadano, por eso ustedes oyen las críticas de la población en general, que habla de los servicios públicos, pero si yo lo considero a usted para definir el servicio público el día de mañana usted no puede decir que el servicio es malo, si no me ha dado los requerimientos necesarios para que pueda generar los servicios que requiere. Eso más bien es protección para el Estado, porque sencillamente ahí es donde hay un alineamiento, para que se vaya produciendo ese bienestar a través de la participación del ciudadano en la formulación de la planificación estratégica de cada institución.

Al menos en ese modelo que estamos proponiéndole a la administración, ustedes van a ver todas las variables y los elementos que deben existir en la planificación estratégica y cómo se puede llegar a esto. Existe una serie de pasos para que puedan llegar a una planificación estratégica verdadera, no de papel, porque eso es otro tema, una cosa es la aplicación de un instrumento metodológico y otra cosa es que se permea el enfoque de una institución, son dos cosas muy diferentes. Yo puedo llenar el formulario y hacer el plan como un montón de instituciones que lo tienen hecho, pero vaya pregunte cuál es el valor público que generan y vamos a ver quién le contesta.

¿Hacia dónde está yendo la institucionalidad? ¿Qué es lo que está produciendo?, puedo estar produciendo zapatos y lo que tengo que producir son chayotes y eso pasa cuando la institucionalidad ha llegado al punto de hacer lo que el grupo de gente que está ahí quiere y no lo que la población necesita. Entonces, ¿cómo va a encontrar un punto de equilibrio? Es insondable eso y nunca va a haber una armonía porque no se dan las cosas en la medida en las que tiene que darse.

Ahí viene todo un problema de esas necesidades y por eso hice hincapié en que si no está el ciudadano presente vamos mal, pues no podremos hablar de valor público y los recursos son muy escasos, hay que tener al ciudadano participando. La productividad y la eficiencia son criterios clave de priorización. Es muy lógico en un estado como el nuestro, por eso es importante mejorar el servicio ya que impacta al desarrollo; se necesita la movilización de recursos de la comunidad.

Hablemos de los impuestos, aquí sí hay recursos. De hecho, debido al pago de impuestos es que podemos exigir servicios públicos de calidad. Hay que entender la lógica. Ustedes encuentran en la ley de planificación esos conceptos y estos vienen de enfoques de modelos de desarrollo que han existido, y se pueden dar cuenta que después de cuarenta años de que se creó dicha ley, están vigentes aún. Porque el país no ha llegado a niveles de desarrollo que se pueda decir que ya no se requiere productividad y mayor eficiencia y tener esto como criterio de priorización y movilización de recursos.

Tenemos actores externos que apoyan la creación del valor público, estos son: condiciones, comunicación y educación ciudadana para la movilización de recursos. Es importante entender que toda esta gestión del Estado con este nuevo enfoque sea comunicada a la ciudadanía, ese es uno de los grandes problemas que hay y que puede enfrentar un proceso de modernización que vaya dirigido a estas cosas. Porque parte de esto es una cultura y la gente quiere mejores servicios; entonces tiene que saber qué es lo que se va a hacer y cómo van a participar ellos en ese mejoramiento.

Y perdemos hasta el mismo concepto de una organización porque para nosotros, los funcionarios públicos, esto es un medio de trabajo y todos lo sabemos. Pero hay una gran diferencia y es que no somos empleados iguales al resto; todos los funcionarios públicos tenemos una misión, una gran responsabilidad y un compromiso con el Estado y con el pueblo. El que no tiene dicho compromiso, perdón, pero no sé qué está haciendo en el gobierno; porque al que no lo mueva el interés común y el bienestar de los demás, no sé cuál es su propósito.

El servicio público es para servirle a otros. Bueno para eso nacimos, solo que se nos olvida como seres humanos y pensamos en nosotros mismos y por eso el mundo está como está. Si la gente siguiera el norte para el que nació, que es para servirle a los demás, este mundo sería otro; pero sobresalen los intereses privados. Es una lucha muy grande y de todas las personas, cuando pensamos que queremos una nueva gestión pública, que queremos mejores servicios, eso está involucrando a toda la ciudadanía que de alguna manera tiene que participar y mejorar su confianza y su grado de credibilidad en la función y en lo que hacen los servidores públicos.

Tenemos un liderazgo de cambio social, que es la creación de valor mediante un proceso educativo cívico. El Estado tiene que asumir todo un movimiento y un programa para hacer entender al funcionario público que su manera de trabajar va a ir direccionada hacia otro norte y no solo a producir, sino para algo que realmente tenga un significado, que realmente sepa cuál es su participación en el bienestar del país, ya sea en mucho o en poco pero que haga conciencia también de que se le está pagando para eso y tenga un compromiso más allá que cualquier empleado del país.

Es una realidad que tenemos que cambiar, pues las instituciones no existen, son ficciones jurídicas. No son buenas o malas porque la gente lo sea. Es sencillamente que las personas dejan de entender que son parte de ellas y consideran que nada más son contratadas para llegar y hacer un trabajo. Sin embargo, no se sienten parte del éxito; es más, hay empleados que no saben ni qué hace su organización y eso es muy grave.

¿Cómo tener un nivel de compromiso si no se siente parte de la organización? Las instituciones públicas son nuestras, de los que las formamos y tenemos que mejorarlas. Si no queremos seguir trabajando, después se presentan los cierres de instituciones y uno se queja; pero si es deficiente y no está generando valor público, ni provocando un bienestar a la sociedad, uno tiene razón de cuestionarse.

¿Qué puede significar valor público en términos generales? Para que lo podamos entender fácilmente, es un

mayor crecimiento económico, mejor transporte y comunicación. Es mayor vigencia del Estado de derecho, eso significa lo siguiente: en Costa Rica existen miles de leyes y muchas de ellas no se cumplen, las mismas instituciones incumplen las leyes que las rigen. Así que parte del valor público es asegurarse que se cumpla el Estado de derecho, que se apliquen las leyes, ya que hay instituciones que ni ejercen parte de sus competencias.

Las dimensiones fundamentales del valor público o componentes de bienestar colectivo se generan a partir de la visión de desarrollo integral del país y producen mejoras en la estrategia de una entidad pública. Vamos a verlo en diferentes dimensiones. Por ejemplo, generalmente lo que los planes de desarrollo contemplan son el bienestar humano que es desarrollo social, para lograr equidad, dignidad e integración, sostenibilidad que produce desarrollo ambiental para obtener la armonía con la naturaleza, economía para dar oportunidades, estabilidad y solvencia económica y gobernabilidad, seguridad, autonomía y participación que produce desarrollo político para fortalecer la democracia; la dimensión externa y la seguridad interna.

Dichas dimensiones se generan a partir de esta visión de desarrollo que podamos ver. Esto generalmente lo hace el estado cuando va a hacer un plan nacional de desarrollo y define los grandes ejes, pero es una cuestión a nivel internacional, prácticamente ustedes saben que con la globalización algunos países adoptan los modelos de desarrollo y más o menos son los que la doctrina toma como principales.

Dimensiones fundamentales: áreas de competencia distintiva para las entidades públicas, el primer ejercicio que debe hacer una institución a la hora de hacer la planificación estratégica es ubicarse en la dimensión o dimensiones de desarrollo que pertenece. Sin embargo, siempre hay una que va a tener prevalencia, porque todas tendrían que ubicarse en gobernabilidad, por ejemplo. Eso es lo del marco de derecho, pero la institución se ubica en alguna y partiendo de la ubicación entonces hacia esa área es que vamos a generar el bienestar, digamos que esto es una línea para poder llegar al valor público en términos muy generales, si mi institución es de bienestar social el valor público va a ser sobre este segmento del desarrollo y hay que demostrarlo con esos productos y definirlo, ya que necesito que vincule la gestión institucional al segmento de desarrollo que tiene que estar alineado.

El bienestar humano es desarrollo social y ético que pretende equidad, dignidad e integración social. Las personas pueden tener vidas significativas y valiosas para ellos y para quienes dependen de ellos, eso es lo que se pretende.

Papeles principales de las entidades estatales. Veamos un ejemplo, ubicamos una institución en desarrollo social. Eso es lo que produce, queremos vidas significativas y valiosas, las entidades estatales deben procurar mantener niveles de equidad, igualdad e integración social, políticas y acciones encaminadas a lograr una alta cobertura de servicios fundamentales en salud, educación, vivienda y seguridad social principalmente, uso de recursos públicos para subsidiar costos de servicios a los sectores más pobres; apoyo en desarrollo ético para la ciudadanía, ahí encuentra una temática del papel y el rol que deben jugar las instituciones que pertenezcan a este segmento. Tenemos otros elementos, ahí citamos ONGs y otros actores de la sociedad civil que ofrecen servicios fundamentales para complementar los programas de entes públicos.

Empresas privadas proveen servicios para otros segmentos. Organizaciones religiosas y otros entes formativos impulsan el desarrollo ético. Las familias desempeñan un papel clave en formación ética y en la protección de sus miembros más vulnerables, en el campo de la salud encontramos otras asociaciones que brindan apoyo y generan valor público también entendiéndolo desde que ellas tienen un impacto en el bienestar de la sociedad. Quise ilustrarles pues tenemos cada dimensión con el papel de cada institución para podernos ubicar.

La misión fundamental del Estado y de cualquier institución pública es definir el valor público que va a crear y la cantidad creada de ese valor en determinado tiempo. Un ejemplo sería la cobertura del internet: cuánto voy a crear en este gobierno, hacia dónde lo voy a dirigir (la provincia de Puntarenas por decir algo); es un proceso de mantenerlo y generarlo.

Los elementos a considerar para la creación de valor son cuatro. En primer término está el mandato legal, la ley con la que se crea la institución. El segundo punto son las competencias; son fundamentales para crear esa misión institucional que me va a dar elementos importantísimos del valor público. En tercer lugar está lo que la institución hace. Puede ser que haya instituciones que fueron creadas hace más de setenta años y que ahora están haciendo otras cosas que la ciudadanía requiere, entonces tenemos que analizar toda esa práctica, la demanda ciudadana para generar el valor público. Por último, se encuentra el mandato electoral que es lo dispuesto por el gobierno entrante; es decir, el plan nacional de desarrollo de cada gobierno.

Con los cuatro elementos anteriores se supone, en buena teoría, que una vez que un gobierno entra, toda la institucionalidad tiene que rediseñar su planificación estratégica. Si bien es cierto va a conservar elementos que son permanentes, que los da el marco competencial y el mandato electoral, pero la práctica institucional puede cambiar con la demanda. Cuando se hace una buena planificación estratégica no se tiene que modificar, solo actualizar o adecuar. Es decir, si tengo un plan en este gobierno, el que viene lo tiene que seguir como está y se hace por ley; la práctica institucional ahí está, lo único que cambia es el mandato electoral. Hay que tomar los elementos que les estoy mencionando, y esencialmente la participación del ciudadano, porque ahora vamos a asociarlo con la era digital.

La práctica institucional debe estar adaptada a la era digital. Esto permite atender la demanda ciudadana de manera rápida y transparente, garantizando libre acceso por medio de la tecnología. Es alto importantísimo. Cuando la ley crea las instituciones establece su competencia; pero lo que realmente va a activar todo es la práctica de la institucionalidad. Es en la gestión donde voy a tener que satisfacer la demanda ciudadana, haciéndola partícipe de mi planificación estratégica y de la definición de los servicios y productos. ¿Por qué lo estoy mezclando con la era digital? porque cuando hablamos de un gobierno digital o electrónico, estamos hablando de aquel que ya se ha apropiado de las tecnologías de la información y comunicaciones y que las está implementando.

Partiendo de la lógica de tomar en cuenta al ciudadano, necesitamos el gobierno digital para hacer más eficiente la gestión, para darle más calidad. Esto nos va a permitir instrumentos que nos facilitan la comunicación, la transferencia de información de datos (que realmente ese es el mundo actual). Pero si ese mundo digital no comulga con los principios del valor público, se va a caer solo, porque nada se gana con tener los mejores procedimientos digitales en una institución si los ciudadanos no fueron los que definieron y diseñaron en conjunto con la institución.

Si la ciudadanía no ha participado en ese proceso, va a sentir desconfianza del servicio y de lo que le está ofreciendo la institución digitalmente, empezando por el solo hecho de que entrar a una página digital es un gran problema, porque al momento de su diseño, se pensó en lo estético, con mentalidad tecnócrata, no con acceso sencillo al ciudadano. Una persona no necesita encontrar un montón de conceptos, sino palabras sencillas, e ingresar directamente al servicio y tener información fácil de manejar. Otro ejemplo son los sistemas de telefonía, uno llama a cualquier institución pública y primero se le acaba toda la recarga disponible antes de que le contesten. Una situación como esta, en lugar de generar valor público lo que hace es destruirlo.

Ahora bien, ¿cuál es el vínculo entre el valor público y la era digital? Pues, que a la hora de diseñar requerimientos en instrumentos y aplicaciones dirigidos al ciudadano, y para que él pueda tener acceso y servicio, se pueden generar problemas. Tomemos como ejemplo a la Caja Costarricense de Seguro Social (CCSS). Todos los servicios se están informatizando y digitalizando; todo perfecto. Sin embargo, quisiera saber hasta dónde la gente participó en el diseño de esos programas. Quizá pueden haber costado mucho dinero. No obstante, si eso no era de satisfacción del usuario, ahí viene la caída del concepto de gobierno digital, ya que sin el apoyo ciudadano no se puede mejorar la percepción de este y es esencial, si se quiere un gobierno digital, que se pueda implementar satisfactoriamente. De lo contrario se caen las dos cosas y seguimos en lo que estamos.

De esa forma, un gobierno digital no está generando el impacto que debiera; ni ofreciendo la calidad, ni la eficiencia que se pretende. La confianza es un elemento fundamental. Algunos pobladores ya somos adultos y nos ha costado muchísimo asimilar el cambio. Ejemplo de esto es que cuando me crié ni siquiera la máquina de escribir eléctrica existía, ni el televisor tampoco. Son épocas que marcaron la tecnología; cuando era pequeño aparecieron los equipos de sonido, después el famoso walkman. Uno vivió todo eso.

A veces me pongo a pensar en lo complicado de la tecnología, si privan los requerimientos y los diseños de los consultores que creen que pueden generar los mejores procedimientos para la creación de los productos y no es así. Solo la gente que recibe el servicio sabe lo que quiere y cómo lo quiere. Si usted espera tener una empresa de éxito, pídale criterio al ciudadano y verá sus productos implementarse con gran satisfacción. De no hacerlo, va a tener problemas por todo lado, más de los que tendría aun participándolo. Pero ese es el vínculo que me interesaba, primero desarrollarles un poco ese concepto de valor público y al final ver cuál es la clave para que tanto el valor público como el gobierno digital puedan trabajar juntos y agregar la participación del ciudadano en todo lo que es la definición de política pública. En eso lo enmarcamos todo.

Ha sido un placer poder compartir con ustedes esta tarde, espero que haya sido de interés y de aprovechamiento. Me pongo a su disposición. Ante cualquier duda que puedan tener, les pongo a su servicio la página con esos instrumentos importantes que estamos generando. También los invito a pedir una charla aquí en el Archivo, sobre el modelo y su aplicación, para que ustedes puedan ir familiarizándose con esta nueva era de la gestión pública. Muchas gracias.





El Archivo Digital Nacional (ADN)

Natalia Cantillano Mora

Coordinadora Unidad Servicios Técnicos Archivísticos del Departamento Servicios Archivísticos Externos y líder técnica del Proyecto Archivo Digital Nacional.

Luis Carlo Rojas Mora

Profesional en Archivística Unidad Servicios Técnicos Archivísticos del Departamento Servicios Archivísticos Externos y miembro del Proyecto Archivo Digital Nacional.

Mellany Otárola Sáenz

Profesional en Archivística Unidad Servicios Técnicos Archivísticos del Departamento Servicios Archivísticos Externos y miembro del Proyecto Archivo Digital Nacional.

Evelyn Valerín Alvarado

Técnica en Archivística Unidad Archivo Intermedio del Departamento Servicios Archivísticos Externos y miembro del Proyecto Archivo Digital Nacional.

Sofía Irola Rojas

Técnica en Archivística Unidad Archivo Intermedio del Departamento Servicios Archivísticos Externos y miembro del Proyecto Archivo Digital Nacional.

1. INTRODUCCIÓN

El presente documento busca compartir la experiencia del Archivo Nacional de Costa Rica en la implementación de un proyecto de preservación de documentos digitales, que tiene como objetivo convertirse en un servicio que eventualmente el ente rector brindará a las instituciones del Sistema Nacional de Archivos.

Es así como en primera instancia se explica el proyecto en cuestión, sus objetivos, alcance y componentes. Posteriormente, se explica el modelo de preservación digital en el que se basa el proyecto, y finalmente, se comparte el trabajo desarrollado en el proyecto durante el primer semestre del 2019.

2. PROYECTO ARCHIVO DIGITAL NACIONAL

2.1 Justificación

Actualmente, una de las condiciones que se impone a nivel global es el proceso de transformación digital en diferentes ámbitos de la sociedad, como lo son la producción, la economía, los servicios, entre muchos otros. Es así, como la administración pública no está exenta de estos cambios y se ve en la obligación de buscar la integración y dinamización de la gestión pública, por medio de la centralización de la información, en aras de la mejora en la eficiencia y la eficacia del gobierno y la gobernanza.

De igual manera, la generación de servicios digitales inclusivos, integrados y seguros en la administración pública, aporta tanto al desarrollo económico del país, como a la sostenibilidad ambiental, ante la integración de plataformas digitales y la reducción de las erogaciones estatales en insumos como papel y otros consumibles derivados de su uso, así como de mobiliario, infraestructura y equipo destinado a la conservación de documentos en soporte papel.

Costa Rica, alineada a esta corriente de pensamiento, ha desarrollado durante varios años normativa jurídica que busca regular el uso de los documentos electrónicos, como por ejemplo la Ley de Certificados, Firmas Digitales y Documentos Electrónicos n°8454 y su reglamento; las políticas de formatos oficiales de firma digital emitidas por el Ministerio de Ciencia, Tecnología y Telecomunicaciones (Micitt); las Normas de control interno para el Sector Público N-2-2009-CO-DFOE de la Contraloría General de la República; las directrices y normas técnicas emitidas por el Archivo Nacional en materia de gestión de documentos electrónicos y digitalización, entre otras.

Aunado a lo anterior, recientemente se han elaborado herramientas de buen gobierno que buscan acelerar la transformación digital del Estado costarricense, tal es el caso de:

- El Plan Nacional de Desarrollo y de Inversiones Públicas (PNDIP 2019-2022), que en su Área Estratégica de Innovación y Competitividad hace hincapié en la búsqueda de la sostenibilidad.
- La Estrategia de Transformación Digital hacia la Costa Rica del Bicentenario 4.0 que en sus Ejes de Buena Gobernanza y Transformación Empresarial persigue: la disminución del uso, trasiego y conservación del papel; el aprovechamiento de tecnologías digitales para la protección y conservación ambiental; la gestión

de documentos firmados digitalmente; la disminución del impacto ambiental del quehacer público y empresarial, entre otros.

- El Plan Nacional de Descarbonización 2018-2050 busca incentivar una visión de liderazgo mundial en materia ambiental, a través de las estrategias transversales para catalizar el cambio en Costa Rica.
- La Directriz sobre el Desarrollo del Gobierno Digital del Bicentenario N°019-MP-MICITT en la que “(...) Se ordena a los jefes de la Administración Central (...) que al menos un 75% de todos los documentos que se gestionan y conservan en la institución sean documentos electrónicos firmados digitalmente, antes del 1ero de diciembre del 2020. (...)”

La coyuntura antes descrita plantea a las instituciones del Estado costarricense la obligación de desarrollar proyectos para transformar su producción documental del papel hacia documentos electrónicos con firma digital. Por lo tanto, estas instituciones deberán en un corto plazo desarrollar o contratar una solución informática y un espacio electrónico para gestionar su producción de documentos electrónicos de la mejor manera.

Por las razones antes descritas, el ente rector ha percibido la necesidad de establecer, además de un marco normativo orientador (Política Nacional de Archivos, Plan de Acción y Normas Técnicas Nacionales), un servicio que permita instrumentalizar la normativa vigente y apoye a las instituciones que componen el Sistema Nacional de Archivos en la adecuada transformación digital de su producción documental.

En este sentido, el desarrollo de una iniciativa de este tipo permitirá al ente rector promover la adecuada conservación de documentos a través de un repositorio digital nacional que permita la custodia de los datos e información pública, mediante una plataforma tecnológica normalizada basada en estándares internacionales tales como, las normas internacionales de descripción archivística promulgadas por el Consejo Internacional de Archivos, las Normas ISO 15489, 14721, 30300, solo por mencionar algunas.

Por consiguiente, la ejecución del proyecto de Archivo Digital Nacional (ADN) busca que Costa Rica en un mediano plazo cuente con un portal que centralice el acceso y consulta de los documentos que genera la administración pública. Lo anterior, facilitará la toma de decisiones por parte de la administración, promoverá la rendición de cuentas y la transparencia administrativa al proveerle al ciudadano un punto de acceso único y normalizado a la información y finalmente, permitirá resguardar los documentos patrimoniales, fuente indiscutible para la construcción de la memoria histórica y cultural del país.

2.2 Objetivos y alcance del proyecto

El proyecto Archivo Digital Nacional o ADN tiene como objetivo desarrollar un servicio de preservación y custodia de documentos que brindará el Archivo Nacional de Costa Rica, en su papel de ente rector del Sistema Nacional de Archivos, y que busca ofrecer:

- Un punto único de resguardo de documentos electrónicos en el Estado costarricense.
- Un punto centralizado de acceso a los documentos electrónicos de la administración pública.
- Una solución nacional para la interoperabilidad de sistemas de documentos electrónicos.
- Estandarización de la preservación de documentos electrónicos.
- Seguridad informática y mejora continua.

- Normalización de la descripción archivística.
- Herramientas básicas de producción y recepción de documentos electrónicos, para instituciones que aún no cuentan con este tipo de soluciones informáticas.
- Asesoría y soporte técnico.
- Capacitación y acompañamiento durante su implementación.

Todo lo anterior, con el fin de contribuir a solventar el enorme reto que nuestro país tiene debido al uso cada vez más extensivo de la tecnología y por ende la transformación de la producción documental del papel a documentos electrónicos, así como el uso de la firma digital.

A su vez, el desarrollo del proyecto del Archivo Digital Nacional parte del principio de que su implementación se realizará de forma incremental e iterativa. Es por ello que a partir del I semestre del año 2019 inició la ejecución de un plan piloto en el Archivo Nacional, con la finalidad de poner en funcionamiento el servicio del ADN en nuestra institución, específicamente en dos unidades administrativas.

Tomando como punto de partida la experiencia desarrollada en el Archivo Nacional, se propuso realizar una segunda etapa de este plan, esta vez en una institución del Sistema Nacional de Archivos, específicamente el Ministerio de Cultura y Juventud; en donde se busca emular la experiencia de implantar el servicio del ADN en dos unidades administrativas.

Cabe destacar que aún ambos planes piloto se encuentran en etapa de ejecución, por lo que, posterior a su finalización se brindará la capacitación necesaria para que los encargados del Archivo Central del Archivo Nacional y el Ministerio de Cultura y Juventud, continúen con la inclusión de las demás unidades administrativas en el servicio del ADN, y así se puedan posicionar como unidades rectoras de los sistemas institucionales de archivos, de manera que participen y guíen la transformación digital de documentos en sus respectivas instituciones.

Además, es oportuno mencionar que el conocimiento que se ha generado durante ambas etapas del plan piloto está permitiendo definir la estrategia, procedimientos, actividades e instrumentos que se deberán aplicar en las instituciones que estén interesadas en utilizar el servicio del ADN.

Asimismo, este ejercicio ayuda a establecer y comprobar los mecanismos de comunicación y las acciones de coordinación necesarias para el adecuado desarrollo del servicio, con la finalidad de mejorar la gestión y preservación de los documentos electrónicos de las instituciones participantes. También, ha evidenciado que el nivel de madurez archivística que presentan las entidades que conforman el Sistema Nacional de Archivos es muy variado, un elemento que indiscutiblemente debe tomarse en cuenta a la hora de definir la estrategia de implementación del ADN en una institución.

De igual manera, el trabajo efectuado durante el plan piloto posibilita prever diferentes escenarios, como por ejemplo aquellas instituciones que poseen sistemas de gestión de documentos electrónicos y desean continuar utilizándolos. En caso de que estas organizaciones se interesen en emplear los servicios de preservación de documentos del Archivo Digital Nacional, se están diseñando las estrategias de integración al repositorio digital

nacional, con el objetivo de que no sea necesario que las instituciones abandonen las inversiones realizadas, en aras del adecuado uso de los recursos públicos.

Es preciso indicar que la experiencia desarrollada a través de la ejecución del plan piloto del proyecto ADN es sumamente valiosa, ya que requiere un esfuerzo constante para implementar la normativa y buenas prácticas que en materia de gestión de documentos y preservación digital se han generado, tanto a nivel nacional como internacional. Del mismo modo, se ha adquirido un “know-how” de indudable riqueza que permitirá acompañar, capacitar y asesorar de mejor manera a las instituciones del SNA que estén atravesando por la migración del papel al soporte digital.

Igualmente, se debe señalar que el éxito de un proyecto de esta categoría requiere un fuerte compromiso de las instituciones en donde se implemente, ya que significará en algunos casos la normalización en la ejecución de las tareas archivísticas en soporte electrónico y, en muchos otros, conllevará un cambio en las prácticas administrativas que se desarrollan en las diferentes unidades de las instituciones públicas. Además, implica la conformación de equipos interdisciplinarios que se responsabilicen por atender las necesidades derivadas del servicio.

Finalmente, es preciso indicar que el alcance temporal que tiene el plan piloto del proyecto ADN es el I y II semestre del 2019 y se proyecta iniciar con la prestación del servicio en el I trimestre de 2020.

2.3 Componentes del Servicio ADN

El servicio del Archivo Digital Nacional está estructurado de manera tal que el Archivo Nacional realice un acompañamiento completo durante la implementación del servicio, en dos unidades administrativas a convenir entre las partes. Este trabajo conjunto brindará el conocimiento necesario para que posteriormente, el Archivo Central y la dependencia encargada de Tecnologías de Información administren la solución informática, cada uno desde su competencia. Además, persigue cumplir con el principio de neutralidad tecnológica relacionada con la no dependencia de los fabricantes, desarrolladores, proveedores o distribuidores de los productos o servicios de tecnología.

Tomando como referencia la normativa nacional e internacional y las mejores prácticas en la materia, este servicio está diseñado como una solución adecuada que requiere en su implementación la menor cantidad de tiempo posible de todos los involucrados.

A continuación, se muestran los elementos que componen el ADN.

Ilustración n°1 Componentes del Servicio Archivo Digital Nacional



Fuente: Elaboración propia.

Implementación, Normativa y Capacitación

A través del servicio del ADN se brindará acompañamiento a las instituciones en:

- Diagnóstico de la producción de documentos electrónicos en la institución.
- Obtención e instalación del sello electrónico (firma digital de persona jurídica).
- Interconexión de la institución con el servicio del ADN.
- Análisis de los instrumentos archivísticos existentes
- Elaboración y/o actualización de normativa archivística institucional, en caso de ser necesario.
- Parametrización del repositorio digital (creación de estructura de clasificación, creación de usuarios, creación del contexto de usuarios (roles y perfiles), controles de acceso)
- Carga de documentos electrónicos de las unidades administrativas seleccionadas
- Capacitación al Encargado del Archivo Central y personal de Tecnologías de la Información para la administración de la plataforma tecnológica y la solución de ADN.
- Capacitación a las personas usuarias de las unidades administrativas
- Evaluación de los resultados del uso del servicio.
- Acompañamiento en la definición del cronograma de implementación del servicio en las demás unidades administrativas.

Mantenimiento y soporte

El servicio del ADN contempla:

- Actualización continua de la solución
- Soporte técnico (archivístico y tecnológico)
- Documentación y manuales de uso de la solución

Herramienta de preservación (se pueden sumar interfaces de producción y recepción de documentos)

Para la preservación digital el ADN ofrecerá:

- Repositorio digital basado en el Modelo de referencia OAIS (Open Archival Information System)
- Descripción multinivel de acuerdo con los metadatos descriptivos definidos en la Norma Nacional de Descripción Archivística y el etiquetado de estos metadatos de acuerdo con la estructura de los estándares internacionales correspondientes: EAD, EAC, EAG.
- Almacenamiento de documentos electrónicos de todo tipo: textuales, gráficos y audiovisuales.
- Administración de formatos de almacenamiento.
- Clasificación de los documentos de acuerdo con el cuadro de clasificación institucional
- Uso de certificados de sello electrónico institucional como un elemento más de confianza a la validez de los documentos.
- Conservación de los metadatos relacionados con el contexto, contenido y estructura del documento durante el plazo que sean requeridos.
- Utilización de esquemas y diccionarios de metadatos de preservación (Esquema Mets Metadata Encoding and Transmission Standard y Diccionario de Datos Premis)
- Creación de paquetes de información archivística, compuestos por el documento, firmas digitales, estampas de tiempo, sello electrónico y metadatos incorporados asociados.
- Garantizar el registro de cualquier movimiento o acción generada en el repositorio digital, a través de bitácoras de trazabilidad o pistas de auditoría y notificar la falla o éxito a quien corresponda como responsable del sistema.
- Protección de los paquetes de información archivística mediante cifrado.
- Conservación de los paquetes de información en formato XML y en base 64.
- Creación de índices electrónicos (foliado).

Además, si se carece de una solución para la gestión de documentos electrónicos, las interfaces de producción y recepción de documentos permiten:

- Generación automática de identificadores unívocos por tipo documental de los documentos producidos.
- Creación de documentos electrónicos firmados digitalmente, basándose en los formatos oficiales, incluye documentos con firma mancomunada.
- Asignación y despacho de documentos en el sistema.
- Control en la recepción de documentos.
- Incorporación automática de los documentos producidos y recibidos en el repositorio digital con los metadatos de contexto, contenido y estructura asociados.
- Autenticación de usuarios con firma digital.

Enlaces y continuidad del negocio

Sobre el particular el ADN procura:

- Plan de continuidad del negocio.
- Redundancia de enlaces de conectividad.
- Enlaces punto a punto.
- Plataforma con sistemas distribuidos, que permiten escalabilidad.
- Interoperabilidad con otros sistemas de gestión y/o de preservación de documentos electrónicos.

Almacenamiento y seguridad

Y en cuanto a este aspecto el ADN proporciona:

- Almacenamiento masivo de información en plataformas seguras.
- Redundancia en respaldos de información.
- Planes de contingencia por interrupción del servicio.
- Cifrado de las bases de datos.
- Comunicación cifrada entre aplicaciones.

2.4 Modelo de preservación (OAIS)

Ante una Sociedad de la Información y el Conocimiento, uno de los retos es la conservación de documentos en soporte electrónico a lo largo del tiempo, por lo que, es necesario que las organizaciones cuenten con sistemas

integrales de preservación digital. En este sentido, se desarrolló el modelo OAIS que explica las funciones que debe cumplir un sistema para garantizar la custodia de objetos digitales.

El modelo OAIS se originó en el siglo XX por la *National Aeronautics and Space Administration* (NASA), como una solución a la necesidad de conservar sus datos a través de las épocas, es así que, este modelo proporciona las características con que debe contar un sistema de preservación, el cual fue aprobado en el 2003 por el *Council of the Consultive Committee for Space Data Systems* (CCSDS) (Comité Consultivo del Sistema de Datos Espaciales), bajo el nombre *Reference Model for an Open Archival Information System, Space data and information transfer systems* (Modelo de Referencia para un Sistema Abierto de Información de Archivo, Sistemas de transferencia de datos e información espaciales, OAIS).

De esta forma, OAIS se convierte en una Norma ISO con el código 14721:2003; que en junio de 2012 se actualizó. A pesar de que el modelo OAIS fue originado por la industria aeroespacial, otras áreas del saber han adoptado este modelo, tales como matemáticas, aeronáutica, astronomía y archivística. En este último campo destacan algunas iniciativas:

- Estados Unidos:
 - Lots Of Copies Keep Stuff Safe (Lockss), desarrollado a partir de 1998 por la Universidad de Stanford y Digital Preservation Repository Software (Daitss), se creó en el 2006, por el Centro de Bibliotecas de Florida, ambos son sistemas de preservación.
 - Open technologies for durable digital content (DuraSpace): es una organización que mediante proyectos como, DSpace, Fedora, VIVO, promueven el acceso a largo plazo de los datos digitales. Algunos servicios ofrecidos por DuraSpace son:
 - DuraCloud: para archivar, compartir y administrar contenido en la nube
 - DSpaceDirect: repositorio digital para preservar y brindar acceso a la información.
- España, la Agencia Catalana de Certificación de Cataluña desarrolló en el 2007, el proyecto iArxiu, el cual está fundamentado en el modelo OAIS, para brindar un servicio de archivo electrónico a las instituciones públicas.
- Portugal: Los Archivos Nacionales de Portugal con la la Universidad de Minho desarrollaron el Repositorio de Objetos Digitais Autênticos (conocido como RODA), en 2007.
- Canadá: en el año 2009, se inició Archivemática, el cual es un sistema de preservación digital de código abierto.
- Reino Unido: En el 2015, se creó ArchivesDirect, es una solución para preservar recursos digitales fue desarrollada por Artefactual Systems y DuraSpace. Esta iniciativa que combina Archivemática, una herramienta de flujo de trabajo de preservación diseñada por Artefactual, y DuraCloud , un servicio de conservación y almacenamiento en la nube de archivos de DuraSpace.
- Inglaterra y Gales: En la primera década de los 2000, se difunde Active Digital Preservation (Preservica), la cual es una iniciativa privada que se ofrece como un servicio para la preservación a largo plazo de objetos digitales. Entre sus clientes se encuentran: Banco HSBC, Yale, archivos estatales de Estados Unidos y archivos nacionales.

- Francia: ArcSys, es un repositorio unificado para la conservación a largo plazo de la información. Es una solución privada que se ofrece el servicio de preservación.

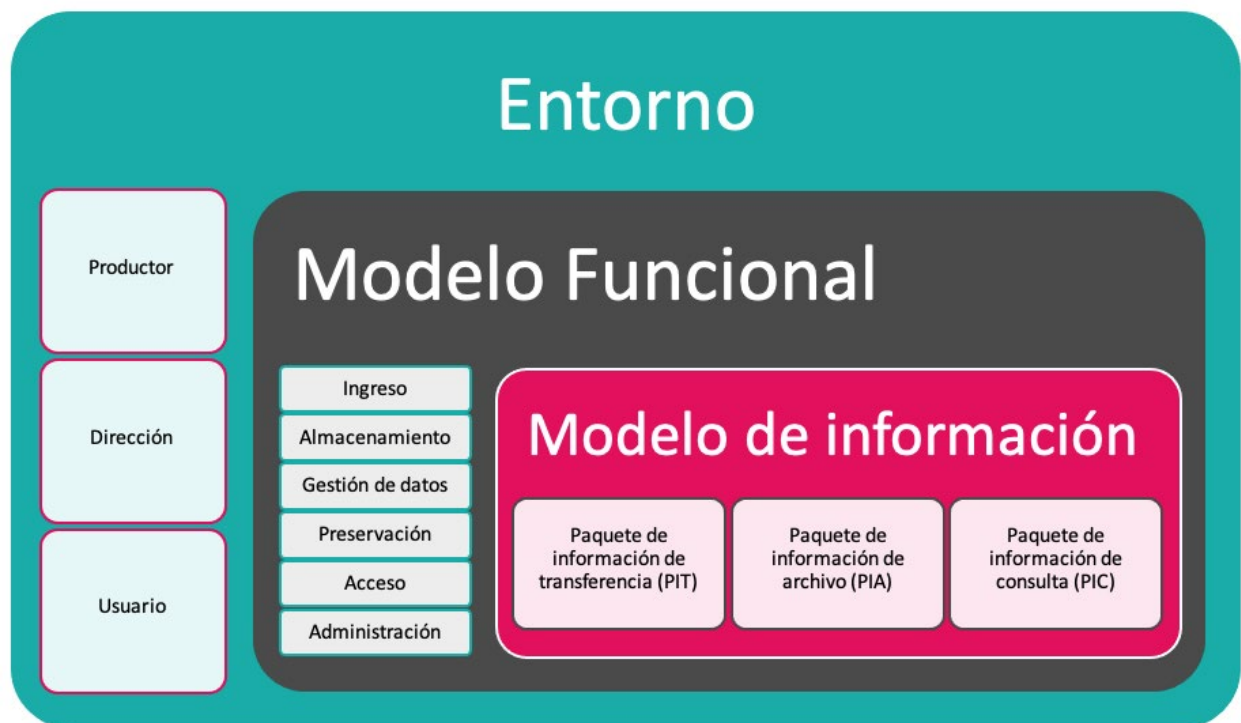
El modelo OAIS se ha convertido en el cimiento, sobre el cual, se ha construido la estructura de muchos repositorios digitales alrededor del mundo, su popularidad es que este modelo garantiza que un documento sea auténtico, veraz e íntegro a través del tiempo, y que, a su vez faculta su accesibilidad, fiabilidad y utilización.

El Archivo General de la Nación Colombia (2018) señala que el modelo OAIS, “es la base para la normalización de la preservación digital y es la principal referencia conceptual para establecer la política, requisitos y acciones. El modelo OAIS establece conceptos, responsabilidades, estrategias de preservación, entre otros, sin que ello implique una implementación específica” (p. 19).

Según indica la norma UNE-ISO 14721:2015 “un Archivo OAIS es un archivo dedicado a conservar información para que pueda acceder a ella y usarla una comunidad específica” (p. 28). Es así que, el modelo OAIS es definido como un archivo digital confiable que emplea herramientas tecnológicas dirigidas hacia la preservación y que, además permite aplicar los procesos archivísticos.

El modelo OAIS tiene tres componentes, los cuales se representan en la siguiente ilustración:

Ilustración n°2 Componentes del modelo OAIS



Fuente: Elaboración propia.

2.4.1. Entorno OAIS

Este entorno está integrado por los actores que están afuera del Archivo OAIS que son:

- Los productores: Constituido por las personas o sistemas clientes que producen y proporcionan la información que se pretende preservar. Ejemplos: áreas de archivo, unidades, gestores de información.
- La dirección: Son aquellos que determinan la política general del OAIS, como un elemento de un círculo político más extenso. Ejemplo: órganos directivos de una institución.
- Los usuarios: Son aquellas personas o sistemas clientes que interactúan con los servicios de OAIS para encontrar y recuperar la información que necesitan. Ejemplo: comunidad específica.

2.4.2. Modelo funcional de OAIS

Seguidamente, se detallan los seis apartados que constituyen el modelo funcional:

- Ingreso: Es la función que se relaciona con los productores. Es la que se encarga de recibir los paquetes de información de transferencias (PIT) que envían los productores, de preparar los contenidos para el almacenamiento y gestión en el archivo digital generando los paquetes de información de archivo (PIA).
- Almacenamiento: Proporciona los servicios y funciones para el almacenamiento, mantenimiento y recuperación de los PIA.
- Gestión de datos: Dispone los servicios y funciones para ingresar datos, mantener y acceder a la información descriptiva y a los datos administrativos que gestiona el archivo digital. También incluye la administración y actualización de base de datos.
- Administración: Proporciona los servicios y funciones para la ejecución del sistema de archivo, entre ellas están: gestión de usuarios, de las políticas del archivo, de plantillas y esquemas de metadatos usados para la descripción de los PIT, de la jerarquía documental y de la auditoría y trazabilidad de los eventos ocurridos en OAIS.
- Preservación: Ofrece los servicios y funciones de control del entorno del archivo, para señalar recomendaciones y planes de preservación para conservar la información contenida en OAIS accesible e íntegra al pasar el tiempo.
- Acceso: Brinda los servicios y funciones de apoyo a los usuarios para determinar la existencia, descripción, localización y disponibilidad de la información, lo cual incluye interfaces para el acceso de los documentos mediante la aplicación de controles que limiten el ingreso, además permite la descarga de copias del PIA.

2.4.3. Modelo de información de OAIS

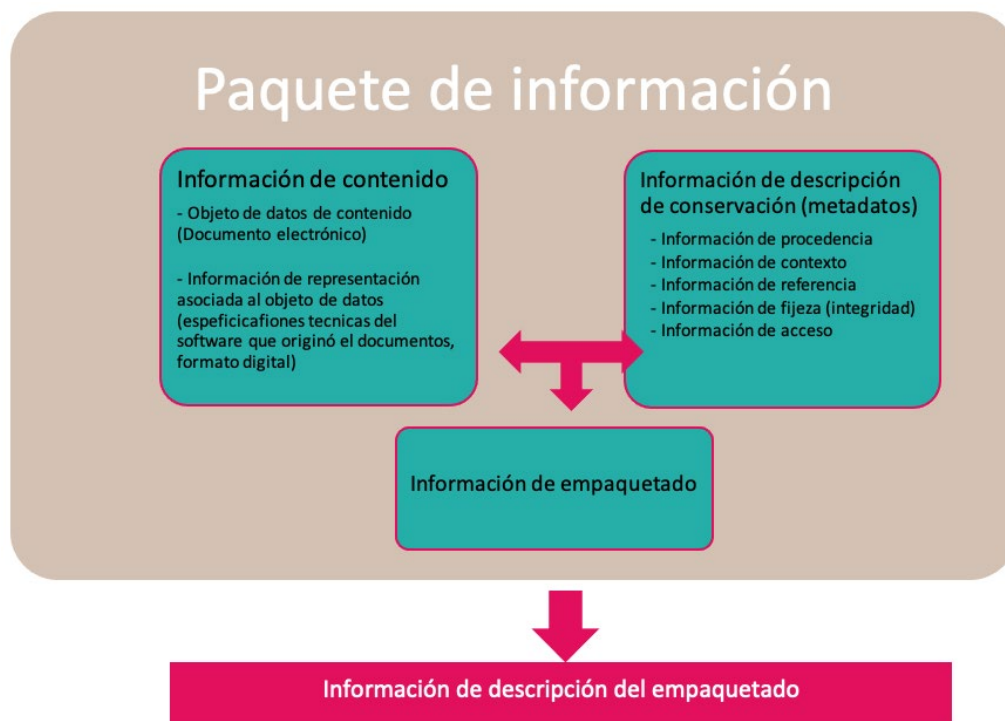
Dentro de este modelo de información existe un concepto básico que es el Paquete de Información (*Information Package*), el cual es definido por la norma UNE-ISO 14721:2015 como un “contenedor lógico compuesto por la información de contenido opcional y la información de descripción de conservación opcional asociada. Relacionada con este paquete de información, la información del empaquetado se usa para delimitar e identificar la información de contenido y la información de descripción del paquete usada para facilitar búsquedas de la información de contenido” (p. 25).

En otras palabras, el paquete de información contiene:

- La información de contenido: es el documento electrónico (objeto de datos de contenido) con especificaciones técnicas del software y el formato digital (información de representación asociada).
- La información de descripción de conservación, que son los metadatos (procedencia, contexto, referencia, integridad (fijeza) y acceso).
- La información de empaquetado: es la información de la estructura del formato contenedor que alberga el paquete de información.
- La información descriptiva del empaquetado: Permite la búsqueda y recuperación de la información.

En la siguiente ilustración se detalla el concepto de “Paquete de información”:

Ilustración n°3 Paquete de información



Fuente: Elaboración propia.

El paquete de información se puede mostrar en tres estados con relación al ciclo de vida del documento dentro del archivo OAIS, los cuales son:

- Paquete de Información de Transferencia (PIT): es un paquete de información enviado por el productor

al archivo OAIS para la construcción o actualización de uno o más PIA y/o información de descripción asociada.

- Paquete de Información de Archivo (PIA): es un paquete de información, el cual se conserva en un archivo OAIS.
- Paquete de Información de Consulta (PIC): es un paquete de información, derivado de uno o más PIA, remitido por el archivo OAIS al usuario.

A continuación, en la siguiente ilustración se detalla el modelo OAIS

Ilustración n°4 Modelo OAIS



Fuente: Elaboración propia.

3. EXPERIENCIA DE IMPLEMENTACIÓN DEL PROYECTO ADN EN EL ARCHIVO NACIONAL

3.1 Requisitos de implementación

Cuando una institución decide gestionar y preservar los documentos que produce y recibe de forma electrónica debe cumplir con una serie de requisitos, con el fin de garantizar la autenticidad, fiabilidad, integridad y disponibilidad de los documentos, independientemente del soporte en el que se encuentren y su plazo de conservación.

A partir del análisis de normativa jurídica nacional y normas sobre buenas prácticas internacionales en materia de gestión de documentos electrónicos y preservación digital¹, se determinó que los requisitos para implementar

¹ En el desarrollo del proyecto se consultaron los siguientes documentos: Norma UNE-ISO 15489-2016 de Gestión de Documentos; Norma

esta tarea se encuentran dispersos. Por tal razón, producto de la investigación y la experiencia en el desarrollo del proyecto, se identificó un listado de requisitos fundamentales que se debe contemplar para poder asegurar la gestión y conservación de documentos, indistintamente de la solución tecnológica que se utilice.

Requisitos mínimos para gestionar y conservar documentos electrónicos:

- Firma digital certificada de los funcionarios que produzcan y firmen documentos.
- Certificado de sello electrónico institucional.
- Instrumentos archivísticos vigentes, validados y normalizados a nivel institucional que incluyen:
 - Cuadros de clasificación.
 - Tablas de plazos de conservación de documentos.
 - Definición de roles y permisos de usuarios.
 - Tablas de acceso de documentos.
- Diseño de plantillas por tipo documental para la normalización en la producción de documentos.
- Mapeo de los flujos de trabajo e identificación de los documentos que se producen.
- Mapeo de normativa institucional existente para la gestión y preservación de documentos electrónicos: políticas, planes, normas, manuales, procedimientos y directrices.
- Identificación de la infraestructura tecnológica existente para el almacenamiento: servidores internos y/o externos, plataformas en línea (nube), dispositivos de alta disponibilidad (NAS, SAN), entre otros.
- Concientización, cultura y capacitación sobre la importancia de la gestión y preservación de documentos electrónicos para el personal de la institución (usuarios internos).

Cabe destacar que el abordaje en el cumplimiento de los requisitos mencionados varía de una institución a otra, dependiendo de factores como los recursos humanos, económicos y tecnológicos disponibles.

De acuerdo con el análisis efectuado, los requisitos mínimos para sistemas de gestión y preservación de documentos electrónicos, incluidos en un cuadro anexo, se deben cumplir tanto en soluciones tecnológicas de gestión como de preservación, independientemente de que estas soluciones estén integradas o se encuentren por separado.

3.2 Metodología de implementación en el Archivo Nacional

La implementación de un archivo digital para la gestión y conservación a largo plazo de los documentos electrónicos de una institución implica el desarrollo de una serie de actividades previas que contribuyan al éxito del proyecto.

En el caso del Archivo Nacional, en primera instancia, se estableció un equipo de trabajo interdisciplinario que involucró profesionales en archivística e informática; además, se contempló la necesidad de contar con

UNE-ISO 14721-2015 Sistemas de Transferencia de Datos e Información Espaciales. Sistema Abierto de Información de Archivos (OAIS), Modelo de Referencia; Modelo de Gestión de Documentos y Administración de Archivos de la Red de Transparencia y Acceso a la Información (RTA); Norma Técnica para la Gestión de Documentos Electrónicos; la Norma Nacional de Descripción y la Norma Técnica para la digitalización de documentos en soporte papel y la autenticidad de imágenes dirigidas al Sistema Nacional de Archivos.

profesionales del área financiero contable/proveeduría para la adquisición de los recursos necesarios para el plan piloto. A su vez, se debe destacar el apoyo por parte de los altos mandos de la institución y el compromiso de la totalidad de las personas funcionarias involucradas en cada una de las fases.

Definido el equipo que se encargaría del plan piloto en el Archivo Nacional, se estableció un cronograma de trabajo en el que se asignaron las tareas y responsabilidades para cada uno de los miembros, con el propósito de tener un mejor control del tiempo, los recursos y los avances del plan.

ETAPA 1: Identificación y diagnóstico

Una de las primeras tareas consistió en hacer una revisión de los instrumentos archivísticos que resultaban indispensables para la puesta en marcha del plan piloto, como lo son el cuadro de clasificación institucional, las tablas de plazos de conservación de documentos, el manual de procesos, los procedimientos institucionales y la normativa sobre gestión de documentos y archivos.

A partir de este trabajo, se determinó que no había un cuadro de clasificación normalizado a nivel institucional, las tablas de plazos estaban desactualizadas, existía una escasa automatización de la gestión de documentos electrónicos y debilidades en la seguridad de la información; también, es importante señalar que la institución carece de un encargado de Archivo Central desde inicios del año 2018.

La situación antes descrita evidenció que la institución presentaba un bajo nivel de madurez en materia de gestión de documentos electrónicos, ya que la producción de documentos en su mayoría se efectuaba en soporte papel. Por lo tanto, no se consideró conveniente un cambio en el sistema de clasificación orgánico que se utiliza, debido a que se está generando una serie de modificaciones significativas en la cultura archivística institucional que podrían derivar en reticencia por parte de los usuarios del Archivo Digital. De este modo, se pretende una implementación de cambios paulatina, iterativa e incremental, que favorezca la apropiación de las herramientas por parte de toda la organización.

Por consiguiente, el cuadro de clasificación se actualizó, ya que constituye la base para conformar la estructura del repositorio digital donde se archivarán los documentos. Como resultado de esta primera fase se originó una nueva versión del cuadro de clasificación institucional que, a la fecha, está en proceso de validación con las unidades productoras, el cual incluye series, subseries documentales y expedientes con una codificación numérica; un repertorio general de series y un listado de los registros de autoridad de cada unidad con su respectiva codificación, siguiendo los lineamientos establecidos para este efecto.

Asimismo, se analizaron las tablas de plazos aprobadas por las diferentes unidades y jefaturas de departamento, debido a que, en entornos electrónicos, los plazos de las series se deben consignar a nivel del sistema desde antes de la creación de los documentos. Sin embargo, a raíz del trabajo efectuado con el cuadro de clasificación, se concluyó que estos instrumentos requieren una actualización, con el fin de normalizar la nomenclatura de las series documentales, recomendación que será remitida oportunamente al Comité Institucional de Selección y Eliminación de Documentos (CISED).

De igual manera, se realizó un diagnóstico para conocer el estado de la gestión de documentos en el Archivo Nacional, así como la cantidad de funcionarios que contaban con firma digital, para lo cual se elaboró un

formulario en línea con preguntas relacionadas con la producción, recepción y almacenamiento de documentos electrónicos y se definió un cronograma de entrevistas para recopilar la información en cada una de las unidades.

Tomando como base los resultados plasmados en el informe del diagnóstico, se seleccionó el Departamento de Archivo Histórico y la Unidad Financiero Contable del Departamento Administrativo Financiero, ya que son las dependencias con mayor volumen de documentos electrónicos, donde la mayoría de sus funcionarios contaban con firma digital. También, esta muestra representa tanto funciones facilitativas como sustantivas de la institución, lo cual permite evaluar la implementación en diferentes niveles organizativos.

ETAPA 2: Configuración del Repositorio Digital

Con los insumos del cuadro de clasificación y las tablas de plazos de conservación de documentos fue posible elaborar la estructura del repositorio, es decir, la organización desde el fondo hasta las unidades simples o compuestas para custodiar los documentos y establecer los plazos de vigencia a nivel de las series documentales.

De forma paralela a la elaboración de esta estructura del repositorio se realizó la parametrización de la Norma Nacional de Descripción, con la finalidad de definir los metadatos obligatorios que se deben incorporar, manual o automáticamente, al efectuar las entradas descriptivas.

Asimismo, fue posible la definición de los roles y permisos de los usuarios a nivel del sistema, por medio de la categorización de perfiles de usuarios, según los puestos y funciones asignadas para cada persona colaboradora.

ETAPA 3: Recopilación y carga de documentos electrónicos

Se recopilaron los documentos electrónicos de las unidades seleccionadas, por medio de carpetas en un sitio colaborativo en línea que permitió su centralización, con el objetivo de facilitar el proceso de carga en el repositorio por parte del equipo de trabajo del Archivo Digital Nacional.

Por su parte, la carga de documentos al repositorio se realizó por medio de la herramienta ADN|Captura, tomando como base el cuadro de clasificación actualizado, por lo que fue necesario reclasificar algunos de los documentos. Al finalizar esta tarea se generó un informe de carga de documentos que se entregó a cada unidad productora, con el propósito de que las personas funcionarias que tengan que utilizar el repositorio comprendan la dinámica de organización de los documentos. Adicionalmente, se realizó la delegación del acceso a las series correspondientes a cada usuario.

Durante el proceso de carga de los documentos fue necesaria la comunicación constante con las unidades productoras para aclarar dudas sobre la conformación de los expedientes. Asimismo, se detectaron algunas inconsistencias a nivel de la gestión de los documentos por parte de las unidades, las cuales fueron consideradas a la hora de actualizar la normativa de la institución en esta materia.

Como parte del proceso de normalización de la gestión de documentos se elaboraron plantillas para cada tipo documental, ya que este es un requisito indispensable para el uso de la herramienta ADN|Producción. Este trabajo se desarrolló en conjunto con la unidad de Proyección Institucional, con el fin de incluir las especificaciones definidas en el libro de marca del Archivo Nacional.

ETAPA 4: Capacitación y acompañamiento en la implementación

Para la capacitación se realizó una presentación general sobre la solución, explicando los beneficios y ventajas de contar con estas herramientas en la institución, no sólo en lo que respecta a la normalización de la gestión de documentos, sino también en lo que se refiere a la simplificación de algunos de los trámites que actualmente se realizan con los documentos en soporte papel, así como en el seguimiento adecuado de los procedimientos y la consulta de información a través de un punto único de acceso.

Además, la capacitación incorporó una parte práctica donde se hizo una demostración personalizada a cada una de las personas funcionarias, con el propósito no sólo de ver y probar el funcionamiento de las herramientas, sino también de atender las consultas particulares de cada uno y conocer sus necesidades como usuarios.

ETAPA 5: Actualización de normativa archivística institucional

A raíz del análisis de las tareas relacionadas con la gestión de documentos y de la forma en que se realizan las prácticas administrativas en las unidades que conforman la muestra del plan piloto, fue necesario elaborar y/o actualizar una serie de documentos normativos, con el fin de adaptarlos a la nueva dinámica de trabajo, tales como el Procedimiento gestión de documentos textuales producidos y recibidos en el Archivo Nacional, el Manual de producción de documentos electrónicos, los manuales de uso de las herramientas informáticas, el Plan de preservación de documentos electrónicos del Archivo Nacional y los Lineamientos para la gestión de permisos por perfil de usuario en el Archivo Digital Institucional del Archivo Nacional.

Además, se vio la necesidad de facilitar la operatividad de la Norma Nacional de Descripción Archivística, motivo por el cual se revisó el documento y se está trabajando en una versión 2.0, en la que se agiliza la descripción de las entidades (documentos, funciones, archivos y productores).

Adicionalmente, es importante mencionar que, tanto la Norma técnica para la gestión de documentos electrónicos, como la Norma técnica para la digitalización de documentos en soporte físico y la autenticidad de imágenes, dirigidas a todas las instituciones que conforman el Sistema Nacional de Archivos, así como las Normas para la descripción de documentos especiales del Archivo Nacional, también serán revisadas por el equipo de trabajo del plan piloto para su respectiva actualización.

ETAPA 6: Documentación del proceso

Es importante recalcar la importancia de documentar todo el proceso, pues esto contribuye a un mayor control en cuanto a las tareas realizadas, lo que está en ejecución y lo que aún queda pendiente. Además, facilita la transmisión de la información y el conocimiento a quienes se vayan incorporando en cada una de las etapas, así como el uso correcto de las herramientas y la ejecución adecuada de los procedimientos relacionados con la gestión de documentos.

4. EXPERIENCIA DE IMPLEMENTACIÓN DEL PROYECTO ADN EN EL MINISTERIO DE CULTURA Y JUVENTUD DEL PROYECTO ADN

Como se indicó en el primer apartado de este documento, una segunda etapa del plan piloto comprende emular la experiencia vivida en el Archivo Nacional, hacia una institución del Sistema Nacional de Archivos.

4.1 Experiencia Ministerio de Cultura y Juventud

La selección del Ministerio de Cultura y Juventud (MCJ) como parte del plan piloto del Archivo Digital Nacional respondió a la relación administrativa existente con el Archivo Nacional, así como a la presencia de un Archivo Central consolidado y a la expresa voluntad de los jerarcas de este ministerio para participar en el plan.

Como parte de las acciones de coordinación, se programó una serie de reuniones orientadas a definir los responsables de las diferentes tareas que deben ejecutarse, tanto para las labores propiamente archivísticas del proceso, como para los trabajos necesarios de interconexión de las plataformas tecnológicas de la institución con el repositorio del Archivo Digital Nacional. Dentro de las acciones de coordinación se desarrollan las siguientes tareas:

- Presentación del proyecto a las autoridades de la institución.
- Designación del personal requerido para la ejecución del proyecto.
- Definición del cronograma de trabajo.
- Selección de las dos unidades donde se implementará el plan piloto.
- Suscripción de un convenio de cooperación.

Para el plan piloto, se seleccionó al despacho de la ministra y el despacho de la Viceministra de Cultura. Por ser dos unidades de carácter sustantivo, así como productores de documentación sustantiva y con valor científico cultural. Además, se tiene especial interés en el despacho de la Ministra con miras a la transferencia de documentos establecida en el artículo n°53 de la Ley n°7202 prevista para el año 2022.

Sobre el convenio de cooperación, los involucrados establecieron una serie de obligaciones indispensables para la consecución de los objetivos del plan piloto que requiere de la intervención tanto del encargado del Archivo Central, como del Departamento de Informática del MCJ. Así como, el compromiso de ambas instituciones en recurso humano, económico y tecnológico. El convenio abarca los siguientes compromisos de las partes:

- Asesoría y capacitación en las soluciones de software propias del Archivo Digital Nacional relacionada con los siguientes aspectos:
 - Creación de la estructura de clasificación de documentos en el repositorio digital.
 - Asesoría en la elaboración de las entradas descriptivas a nivel de fondo y subfondo, serie y unidad documental.
 - Aplicación de las vigencias administrativo-legales y las declaratorias de Valor científico cultural

establecidas en las tablas de plazos a las series documentales de los dos despachos seleccionados

- Asesoría en la implementación de esquemas y diccionarios estandarizados de metadatos de preservación digital.
- Definición de políticas para la administración de usuarios y del sistema, enfocadas en los elementos que se detallan, a continuación:
 - Creación de usuarios
 - Definición de roles y permisos
 - Reglas de trazabilidad
 - Bitácoras de eventos
- Facilitar el personal necesario para el desarrollo del proyecto.
- Facilitar en las instalaciones del MCJ el espacio físico, mobiliario y equipos necesarios.
- Facilitar asistencia recíproca, con el objetivo de resolver satisfactoriamente cualquier clase de requisito administrativo, procedimiento o exigencia que deba ser cumplida para lograr la ejecución adecuada del convenio o de cualquier acuerdo relacionado con éste.

El resultado de la implementación del supracitado convenio deviene en una serie de tareas que deben ejecutar las partes involucradas y que se detallan a continuación:

Labores que debe efectuar el departamento de Informática del MCJ

- Obtener e instalar el certificado de sello electrónico para la institución, así como el certificado de agente electrónico.
- Interconexión entre las plataformas tecnológicas del MCJ y del Archivo Digital Nacional. Este trabajo requiere la cooperación del departamento de Informática del MCJ y del Departamento de Tecnologías de la Información de la Dirección General del Archivo Nacional.
- Instalar el certificado de sello electrónico en los servidores del Archivo Digital Nacional.
- Integración del software de gestión de documentos utilizado en MCJ con el repositorio del Archivo Digital Nacional.

Labores que se desarrollan entre el equipo de trabajo del Archivo Digital Nacional y el Archivo Central del MCJ para los dos despachos ministeriales seleccionados.

- Aplicar un diagnóstico sobre la gestión de documentos electrónicos. Este diagnóstico abarca las siguientes temáticas:
 - Cantidad de funcionarios que producen, gestionan y almacenan documentos electrónicos firmados digitalmente.
 - Medios de almacenamiento de los documentos electrónicos.
 - Formatos en los que se producen y reciben documentos electrónicos.
 - Cualquier otro dato que el encargado del Archivo Central considere importante para comprender las particularidades de la gestión de documentos en ambos despachos.

- Evaluar los resultados del diagnóstico con la finalidad de establecer las estrategias orientadas a la incorporación de los documentos en el repositorio.
- Revisar los diferentes instrumentos archivísticos elaborados en la institución (cuadros de clasificación, tablas de plazos de conservación de documentos, tablas de acceso, etc.), a fin de recabar la información requerida para la parametrización del repositorio.
- Crear la estructura de clasificación en el repositorio.
- Crear y parametrizar los usuarios del sistema de Archivo Digital Nacional.
- Recopilar los documentos para la incorporación en el repositorio.
- Instalar y parametrizar las soluciones de software del ADN en los equipos de los funcionarios involucrados para la carga de documentos.
- Cargar los documentos.
- Efectuar búsquedas de los documentos cargados.

Cabe señalar que la implementación de este plan piloto presenta la característica particular de que el MCJ cuenta desde el año 2013 con un sistema de gestión documental, cuyo uso se ha hecho extensivo con el tiempo y que ha sido adaptado a los requerimientos definidos por el Archivo Central y el departamento de informática del MCJ. Por lo tanto, el caso de esta institución permitirá explorar el proceso de interoperabilidad entre el sistema de gestión utilizado y el sistema de preservación del ADN, especialmente con miras a la próxima transferencia de documentos del despacho ministerial prevista para el año 2022, de conformidad con lo establecido en el artículo n°53 de la Ley n°7202.

La etapa final del plan piloto consiste en que tanto los funcionarios designados del MCJ como del Archivo Digital Nacional elaboren un informe sobre los resultados de la implementación del plan piloto, el cual será remitido a los jerarcas de la institución y fungirá como cierre de la implementación de dicho plan piloto.

Además, este informe incluirá recomendaciones, cronograma y presupuesto para la implementación del Archivo Digital Nacional en el Ministerio de Cultura y Juventud con el fin de implementar el Archivo Digital Nacional en el resto de la institución, así como una correcta gestión y preservación de la documentación digital. A partir de este momento, el Archivo Nacional fungirá como asesor en el caso de que surjan dudas durante esta etapa, y se brindará el soporte técnico y tecnológico necesario.

Finalmente, el estado actual de la implementación del Archivo Digital Nacional en el MCJ se encuentra en la fase de coordinación, se ha realizado un diagnóstico de la gestión de documentos en los dos despachos seleccionados, se han emprendido las primeras acciones relacionadas con la interconexión de las plataformas tecnológicas, el levantado de los requerimientos relativos al certificado de sello electrónico y el certificado de agente electrónico.

5. HERRAMIENTA DEL ARCHIVO DIGITAL NACIONAL

Se presentarán algunas imágenes de las herramientas que conforman la solución del Archivo Digital Nacional.

6. ANEXOS

Anexo 1. Listado de Requisitos para Sistemas de Gestión de Documentos y Sistemas de preservación digital

	Requisitos mínimos	Sistemas de gestión de documentos electrónicos	Sistemas de preservación de documentos electrónicos
1	Firmar digitalmente documentos electrónicos, basados en los formatos oficiales del Micitt.	X	
2	Permitir el uso de certificados de sello electrónico de la Jerarquía Nacional de Certificadores Registrados, como un elemento de confianza para incorporar de manera automática y calendarizada, evidencias de validez de los documentos.	X	X
3	Verificar certificados digitales, firmas digitales, sellos de tiempo y componentes relacionados de la Jerarquía Nacional de Certificadores Registrados.		X
4	Permitir la creación y actualización de una estructura lógica de almacenamiento para clasificar los documentos de acuerdo con un cuadro de clasificación institucional, donde se identifique una relación lógica de pertenencia bajo esa estructura. Esto implica la posibilidad de crear series, subseries documentales y expedientes.	X	X
5	Clasificar los documentos donde corresponda sin crear duplicados, que puedan utilizar mayor espacio de almacenamiento.	X	X
6	Permitir la descripción de los documentos, su contexto, contenido y estructura, según la Norma Nacional de Descripción Archivística emitida por el Archivo Nacional y que está basada en normas internacionales: ISAD G, ISDF, ISAAR CPF e ISDIAH y etiquetar la información de acuerdo con la estructura de los estándares internacionales correspondientes: EAD, EAC, EAG.	X	X
7	Incorporar de forma manual y/o automática los metadatos de creación relacionados con el documento.	X	
8	Incorporar nuevos metadatos a lo largo del ciclo de vida del documento según las necesidades de la institución y las normas vigentes.	X	X
9	Conservar los metadatos archivísticos relacionados con el documento durante el plazo que se requieran.	X	X

10	Utilizar esquemas y diccionarios estandarizados de metadatos de preservación (Esquema Mets Metadata Encoding and Transmission Standard y Diccionario de Datos Premis)		X
11	Asignar y aplicar vigencias en los documentos a nivel de serie documental según el ciclo de vida consignado en las tablas de plazos de conservación. Es decir, permitir la eliminación o la transferencia de documentos según corresponda de manera desatendida.	X	X
12	Elaborar actas de eliminación cuando se den procesos de eliminación de documentos.	X	X
13	Crear y asignar roles de acceso y permisos de uso según el perfil de los usuarios de acuerdo con los puestos y competencias que desempeñen las personas funcionarias en la institución.	X	X
14	Garantizar el acceso restringido para los documentos que lo requieren, por períodos definidos.	X	X
15	Definir políticas de acceso y confidencialidad multinivel (serie, subserie, expediente, documento) según corresponda.	X	X
16	Usar plantillas normalizadas para la producción de documentos.	X	
17	Permitir la trazabilidad de los documentos para la resolución de trámites y consultas.	X	
18	Garantizar el registro de cualquier movimiento o acción generada en el sistema o en los documentos en bitácoras de trazabilidad o pistas de auditoría y notificar la falla o éxito a quien corresponda como responsables del sistema.	X	X
19	Generar cuadros, gráficos y/o reportes diarios, semanales, mensuales, anuales, según solicitud de administradores y usuarios, relacionados con actividades y movimientos en el sistema y en los documentos gestionados y custodiados.	X	X
20	Despachar documentos electrónicos desde la plataforma del sistema o vía correo electrónico.	X	
21	Recibir documentos electrónicos, sean creados digitalmente o digitalizados.	X	
22	Crear automáticamente números de referencia (identificadores únicos) por tipo documental de los documentos producidos.	X	
23	Permitir la migración y conversión digital de los documentos cuando se requiera, en procesos en lote que se ejecuten de manera desatendida para todos los documentos existentes en el repositorio.		X

24	Almacenar documentos electrónicos de toda clase: textuales, gráficos, audiovisuales.		X
25	Permitir cambiar formatos de origen por formatos oficiales de preservación sin alteraciones en el contenido.		X
26	Administrar y usar formatos de estándar abierto y soportes estables.	X	X
27	Crear índices electrónicos (función para el foliado electrónico).	X	X
28	Evitar alteraciones o modificaciones en los documentos custodiados por medio de la verificación continua de la integridad de los documentos y la protección de sus contenidos y estructura.	X	X
29	Comprobar y verificar la autenticidad, integridad y fiabilidad de los documentos electrónicos gestionados y almacenados.	X	X
30	Disponer de los documentos para su acceso, por medio de una interfaz de búsquedas simples y avanzadas de acuerdo con las necesidades de los usuarios, por contenido o cualquier información contenida en los metadatos.	X	X
31	Contar con suficiente documentación técnica, manuales y cualquier documentación de uso que respalde las acciones y funcionalidades.	X	X
32	Contar con almacenamiento seguro, confiable y con suficiente capacidad para gestionar y preservar los documentos electrónicos custodiados.	X	
33	Conservar los documentos electrónicos en conjunto con la información relacionada (firmas digitales, sellos electrónicos, metadatos).	X	
34	Permitir la interoperabilidad con otros sistemas de gestión y/o de preservación de documentos electrónicos mediante interfaces estandarizadas y suficientemente documentadas.	X	X
35	Contar con un repositorio digital basado en estándares internacionales de preservación, teniendo como base el Modelo de Referencia para un Sistema Abierto de Información de Archivo (OAIS).		X
36	Tener la capacidad de crear paquetes de información archivística, compuestos por el documento, firmas digitales, sello electrónico y metadatos incorporados asociados.		X

37	Tener la capacidad de recibir paquetes de información de transferencia, provenientes de sistemas de gestión de documentos electrónicos.		X
38	Tener la capacidad de crear paquetes de información de consulta, para el acceso de usuarios internos y externos, y permitir la descarga de los documentos cuando el rol lo permita.		X
39	Proteger los paquetes de información archivística por medio de cifrado, ante posibles modificaciones o ataques.		X
40	Conservar los paquetes de información en formato XML y en base 64.		X
41	Permitir la aplicación de técnicas de redundancia y funcionamiento a través de múltiples enlaces de datos.		X
42	Contar con una arquitectura de sistemas distribuidos y que permitan escalabilidad.		X
43	Permitir el adecuado funcionamiento según los planes de continuidad del negocio ante interrupciones en el servicio.	X	X
44	Mantener el software actualizado, de acuerdo con las necesidades institucionales y tecnológicas requeridas.	X	X
45	Incorporar mecanismos que permitan analizar amenazas que puedan perjudicar el software y la información contenida, y activar protocolos de seguridad en caso de ser necesario.	X	X
46	Disponer de soporte y mantenimiento tecnológico.	X	X
47	Permitir acciones y permisos específicos para los administradores del sistema.	X	X
48	Permitir múltiples instancias del servicio para poder generar repositorios independientes por fondo documental.	X	X





MESA REDONDA:

Gestión de riesgos en el entorno digital para la continuidad del negocio

Roberto Lemaitre Picado

Encargado de Ciber Seguridad del Ministerio de Ciencia, Tecnología y Telecomunicaciones (Micitt)

Randall Barnet Villalobos

Analista de Ciber Seguridad del Instituto Costarricense de Electricidad (ICE)

Ricardo Villalón Fonseca

Informático, profesor investigador de la Escuela de Ciencias de la Computación e Informática de la UCR

Moderadora: Carmen Campos Ramírez

Subdirectora general del Archivo Nacional

CARMEN CAMPOS RAMÍREZ

Me permito darles a nuestros invitados unas brevísimas reglas para la mesa redonda. Van a tener aproximadamente treinta minutos cada uno para hacer su presentación y seguidamente vamos a contar con treinta minutos más para el debate entre ustedes, y también por supuesto participando a nuestro público para que puedan hacer las preguntas que considere. Yo les estaré indicando cinco minutos antes de que se les vaya venciendo el tiempo.

Tenemos una mesa redonda que trata el tema de la Ciberseguridad, de la Seguridad Informática como también lo denominamos, seguridad de las tecnologías de la Información. Se trata de áreas relacionadas con la Informática y la Telemática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con ella. En particular, y de mucho interés para nosotros, el tema de la información, tanto la que pueda residir en una computadora como la que esté circulando por medio de las redes sociales, la nube, etc.

Con la ayuda de nuestros panelistas, vamos a analizar el tema de los riesgos. Técnicamente hablando, esto significa la identificación de los activos informáticos, sus vulnerabilidades y amenazas a que estamos expuestos, así como la probabilidad de su ocurrencia y por supuesto el impacto que esto pueda generar. Todo esto con el fin de determinar los controles adecuados para aceptar que evidentemente hay riesgos eminentes en esta materia. Lo que se busca es poder disminuirlos, trasladarlos o bien evitar que ocurran, tomando en cuenta que la materialización de un riesgo evidentemente genera daños y pérdidas, entre ellas financieras, administrativas y particularmente de información. Por lo tanto, habrá que aplicar los controles más adecuados para ellos y tener la seguridad de que debe ser un mega control o toda una arquitectura completa de seguridad para poder encarar los riesgos que nos acarrea el mundo digital.

Así que sin más preámbulo le voy a dar la palabra a don Roberto Lemaitre para que haga su presentación.

ROBERTO LEMAITRE PICADO

Buenos días, buenos días compañeros del panel. Es un gusto compartir con profesionales que tengo algún tiempo de conocer y con la categoría y nivel de conocimiento, compartir con la familia de archivística. Ustedes tienen una gran responsabilidad a nivel país, tanto que mucha de la documentación que tienen es tan valiosa que ese es el objetivo del cibercrimen en este momento.

Desde el Ministerio de Ciencia y Tecnología tengo el gusto de coordinar el Centro de Respuestas de Incidente Informático de Costa Rica. Creo que ya algunos han tenido contacto con nosotros tanto a nivel informativo y a otros les hemos atendido y colaborado para la atención de incidentes. Hoy la idea es que hablemos de para qué sirve conocer los delitos informáticos, si soy archivista.

Hay una fecha que siempre me gusta recordar y que insisto que debe ser una fecha que algún día declaren feriado nacional aunque solo los informáticos hemos estado pidiendo eso. ¿Cuándo se abrió la caja de pandora en el país? El 26 de enero de 1993. Internet tiene muy poco tiempo en Costa Rica; el desarrollo de la tecnología con base a internet realmente solo tiene veintiséis años. A veces suponemos, dada la normalidad con que usamos la red, que internet ha estado siempre.

Ya las nuevas generaciones no entienden cuando uno hacía tareas sin internet y yo siempre cuento una anécdota

de una profesora que me puso cero. Yo usé desde muy pequeño internet; tuve la suerte de tener acceso a la plataforma en la oficina donde mi papá e hice una tarea sobre las hojas de los árboles. Entregué la tarea y la profesora me puso un cero. Obviamente mi mamá fue a reclamar que como me había puesto esa calificación. La profesora dijo algo que siempre me marcó (y en este momento quisiera topármela ahora para preguntarle); la profesora dijo que era una tarea hecha en internet y que no valía. “Usted tenía que ir a buscar un libro a una biblioteca”, dijo. Yo no me imagino ahora, teniendo que hacer tareas o trabajos sin internet, o a un estudiante que le pongan un cero por usar internet de consulta. Los tiempos han cambiado, ¿qué pasó desde esa fecha? El internet nace sin pensar en seguridad; nace pensando en que la información llegue a su destino. Después es cuando comenzamos a pensar en las plataformas, en las capas de seguridad que debieran de tener. Alguien dirá ahora, “pero ¿cómo no pensaron en seguridad?”. No, no lo pensaron. Buscaron que la información llegara a su destino, más que eran procesos de desarrollo académico y científico en su momento. Hace veintiséis años; recuerden esa fecha el próximo año para la celebración.

¿Qué pasa ahora? Todas las instituciones o empresas son ciber empresas. Al final, ¿qué institución no tiene algún tipo de tecnología desarrollada, algún tipo de información de forma digital? Todos las tenemos y el sector público no es la excepción. Trabajamos con tecnología; pero hay que recordar un punto, los mesías cibernéticos no existen. Ese es un primer punto importante, porque muchas empresas o personas en el área relacionada van a decir: “mire esta es la solución totalmente segura para algo”. Sin embargo, les voy a decir una realidad: el riesgo cero no existe, siempre nos va a pasar algo en materia de ciberseguridad, siempre vamos a tener algún incidente. El tema es estar preparados para responder adecuadamente a estos hechos y eso se logra con la planificación y medidas adecuadas que se puedan tener dentro de las instituciones, para lograr responder en tiempos cortos y adecuados. De nuevo recuerden esta frase: “riesgo cero no existe, pero las medidas adecuadas sí”.

La velocidad de crecimiento de las organizaciones en materia digital es enorme y nos agarró a muchos desprevenidos en el desarrollo tecnológico de las empresas y de las instituciones. Tuvimos que entrar muchas veces de manera golpeada a tener que desarrollar las plataformas tecnológicas y los servicios que tuviéramos, sin nuevamente pensar en el tema de seguridad. Lo que interesaba era lograr que los servicios estuvieran digitales. Actualmente tenemos que mejorar en materia de seguridad, porque vean que apenas tenemos veintiséis años con internet y los servicios ya se están ofreciendo al usuario. Dentro de nuestras instituciones los canales digitales son ahora lo más común para lograr de manera efectiva trabajar. Uno de los puntos fundamentales cuando nos ocurre algo es que el tiempo es vital para lograr disminuir el impacto. No solo pensemos en el impacto económico; también está el que causa no tener un servicio disponible al público, el que tiene en las personas no tener manera de comunicarse con nosotros, el que a lo interno no se pueda hacer un desarrollo o enviar alguna información que se requiera. Y además está el impacto de imagen que muchas veces no lo tenemos tan medido o tan valorado; pero también la imagen de una institución se ve afectada cuando sus servicios están siendo vulnerados.

Hay tres aspectos base que estoy seguro han escuchado a la hora de seguridad de la información y ciberseguridad. Un incidente es cualquier situación que afecte tres aspectos: confidencialidad, disponibilidad e integridad. Si alguno de estos se ve afectado dentro del desarrollo de alguna situación que ocurra dentro de una institución, ahí estamos frente a un incidente. Esto me lleva a una aclaración que me parece importante y que en la experiencia desde el Centro de Respuesta de Incidentes Informáticos nos ha ocurrido. Un incidente puede no ser un ataque cibernético. Eso es importante recordarlo, porque a veces cuando hablamos de ataques o hablamos de incidentes, todo el mundo relaciona “nos están atacando desde equis país, nos están atacando los cibercriminales mal llamados hackers nos están atacando”. Un incidente puede ser la detección de una plataforma caída; quizá

estamos haciendo una actualización y no nos salió bien desde del servidor y en este momento el servicio no está disponible. O puede tratarse de un archivo que no llegó, un archivo que se borró. Pero también tenemos los incidentes relacionados con ciberataques que podrían ser malware o un ransomware, entre otros.

Ocurre por diversas causas: tenemos por una avería (eso es un incidente también), un suceso no controlado (incendio, fuego o algún tema natural que ocurra dentro de una institución), una acción no intencionada de algún usuario o intencionada (podría ser que haya una fuga de información o un error al enviar información por un correo). Ha pasado también con una información que se equivocan y lo envían a un destinatario que no era la persona, o un ataque intencionado en función de los recursos afectados.

Hay incidentes a nivel mundial que nos han afectado. Este fue un caso a nivel mundial en el que Costa Rica también estuvo involucrado. No sé si conocen a la empresa Ashley Madison que ofrecía que todos los que quisieran tener una aventura extramarital podían integrarse en una gran base de datos que aseguraban cien por ciento seguridad. Es decir, nadie se iba a dar cuenta y nada iba a ocurrir; su propaganda era “La vida es corta, tenga una aventura”. Mucha gente se unió. ¿Qué pasó? Parece que los cibercriminales hackearon la base de datos, robando treinta y nueve millones de infieles y cuando lo hicieron le dijeron a la empresa (y puede ocurrirnos un secuestro de este tipo de información) “mire, pague tanto o liberamos esta base de datos”. La empresa no aceptó y liberaron la base de datos. El tema se tornó delicado, tanto que obviamente hubo varias familias destruidas. Pero el tema más delicado fue que mucha gente, al ver su información vulnerada y publicada, tomó la decisión de suicidarse en Estados Unidos. Por cierto, la base de datos tenía gente de Costa Rica también. Entonces, nada es cien por ciento seguro.

Pero también ocurren hechos que a uno realmente lo sorprenden porque espera niveles de seguridad mucho más altos. Por ejemplo, roban documentos militares clasificados porque nadie cambió la contraseña del router; a nivel militar tenían un router con la clave tradicional de “Admin” y así ingresaron al router del equipo militar. Los investigadores dijeron que posiblemente los que hicieron el ataque no eran tan expertos porque realmente hubieran obtenido muchísima más información con todo el tiempo que estuvieron conectados.

¿Qué está pasando a nivel regional? Estos son los incidentes que más están pasando en Latinoamérica. Tenemos infección por malware (eso es algo que a nuestras instituciones les está afectando bastante), tenemos por ransomware. A los que no conozcan que es un ransomware les explico: ahora la información la secuestran y piden un rescate (normalmente una criptomoneda, bitcoin). Secuestra la información, la tienen cifrada, controlada y si usted no paga no le dan la clave para volver a descifrarla. Eso es algo que hemos estado viviendo en las instituciones y que por ende necesitamos medidas técnicas como respaldos de seguridad que se tengan adecuadamente administrados para evitar que esto nos suceda. Vulnerabilidades, ataques de negación de servicios, etc. Costa Rica no escapa de que estén ocurriendo estas acciones, en un 42% según el estudio de ESET Smart Security. Esa es a la realidad que nos enfrentamos.

¿Cómo están los gastos de ciberseguridad a nivel mundial? Están en aumento, pero la respuesta y lograr disminuirlo todavía no es algo que se logre. También pasa porque la solución no está solo en la parte técnica. Está en poner más equipos y más herramientas; esto también es muy importante pero no lo es todo. También es muy importante la capacitación del personal y el cambio de cultura a cultura digital (a la hora de que manejemos activos digitales e información dentro de nuestras instituciones).

Cuando hay incidentes, la mayoría de las empresas identifican las consecuencias más visibles; pero dejan de

lado las consecuencias de carácter más técnico. ¿Qué ocurre en esto? Cuando una empresa se encuentra con una situación de estas, busca rápidamente resolver la problemática y volver a estar en línea. Sin embargo, el problema es que no hace una retrospectiva de por qué ocurren las cosas y cómo podemos solucionarlo para que no vuelva a ocurrir. Muchas de las situaciones con incidentes informáticos son reiterativas dentro de las mismas instituciones o a veces no se solucionan situaciones identificadas.

Por ejemplo, dentro del ministerio hemos estado trabajando en las diferentes instituciones públicas y vamos desarrollando etapas para analizar vulnerabilidades de los portales web. Determinamos la situación en que se encuentran y desarrollamos los planes remediales para que los atiendan y evitar que les vuelva a ocurrir los mismos problemas. Sin embargo, la idea de estos planes es que los apliquen y disminuya la posibilidad de que un incidente informático se dé. De nuevo, no hay riesgo cero; lo que buscamos es disminuirlo a niveles aceptables.

¿Cómo responder ante un incidente informático? Las encuestas demuestran que los controles de seguridad más utilizados son antivirus, firewall y los backup de información a nivel latinoamericano. No obstante, esto no hace que se disminuyan los incidentes; lo que tenemos que hacer es tomar las medidas adecuadas para que cuando ocurra un incidente podamos responder de la mejor forma. Esos son los controles que se están aplicando a nivel latinoamericano: software, antivirus, firewall, backup, anti-spam, usuarios autenticados, etc. Todas son medidas importantes que se deben tener dentro de las instituciones y que aportan seguridad a cierto nivel. Pero de nuevo el tema de los controles y la capacitación adecuada se vuelve fundamental.

Las medidas prácticas que se vienen aplicando en Latinoamérica son: políticas de seguridad, auditorías internas, clasificar la información. Uno de los temas que estamos buscando trabajar con las instituciones es que tengan personal capacitado en materia de atención de incidentes y ciberseguridad. En esto hay un punto que se debe considerar: no importa a qué tema estemos específicamente dedicados los informáticos, o nos ven como “arregla chunches” o no saben el tipo de conocimiento que tenemos y en qué línea estamos especializados. Ese es un tema cultural que hay que ir trabajando desde los departamentos de Tecnologías de la Información. No son departamentos de ciberseguridad y muchos de los informáticos no tienen la base en temas de atención de incidentes en materia de ciberseguridad. Ese es un tema en que estamos buscando trabajar para capacitar a los informáticos, porque tener esta profesión no es lo mismo que conocer de ciberseguridad. Por esto es necesario que en las instituciones se brinden y se planifiquen recursos para capacitar equipos especializados en la materia, o por lo menos una o dos personas que tengan la capacidad y respuesta de atención de incidentes informáticos y de atención en materia de ciberseguridad. Como les digo, TI no es igual a ciberseguridad.

Ante todas estas situaciones se vuelve necesario dar una respuesta jurídica también, y que se vuelva importante conocer a la hora de tener que determinar si algo que está sucediendo puede ser judicializado, si algo está sucediendo por qué camino ir. También se requiere identificar si algo de lo que está sucediendo es un delito, o qué puedo hacer y qué no puedo hacer dentro de este marco. Debemos recordar que existe Ley de protección de la persona frente al tratamiento de sus datos personales. Tenemos la agencia de protección de datos que busca proteger o que se administren adecuadamente las bases de datos de información tanto impresas como digitales. La normativa incluye a ambos escenarios, las sanciones de la ley de protección de datos van en línea administrativa y también directamente a personas por el mal uso que se le da a los datos.

En los derechos que tienen las personas, por otra parte, se ubican el acceso, la rectificación o supresión y consentir la aserción de sus datos. Algo que me parece fundamental también reiterar, y que sé que don Alexander Barquero en este tema está mucho más versado que yo, es la ley de firma digital y documentos electrónicos

y su reglamento. En este aspecto la firma digital certificada oficial, el certificado oficial del país, es el único elemento técnico que tiene respaldo jurídico. Tiene una ley que le permite todo un marco de acción; podemos aprovecharlo y utilizarlo tanto para nuestros trámites como para que las personas pueden hacerlo bajo los servicios de firma digital. Esta tramitología es fundamental porque además da un respaldo por ley y eso nos da seguridad jurídica. Eso es importante tenerlo presente porque los tres elementos principales que nos da la firma digital son autenticidad, integridad y no repudio.

En el 2012, 2013 el Código Penal sufrió una reforma en que integró más de veinte nuevos delitos en materia informática. Es importante que los mencione rápidamente; me interesó ver algunos relacionados con el tema de archivistas, como lo son la violación de correspondencia o comunicaciones para que los tengan presentes. Existen y tienen un agravante importante para quienes los cometen: las personas encargadas de la recolección, entrega o salvaguarda de los documentos o comunicaciones. Es importante saber que los que estamos encargados de administrar información y salvaguardarla, tenemos una pena más alta si alguien realiza alguna acción contra la información que se tenga contenida ahí. Pero también para los informáticos, las personas encargadas de administrar o dar soporte al sistema de red informática tienen una pena más alta si realizan una acción de violación de correspondencia o comunicaciones, o información no dirigida a ellos.

También tenemos el delito de violación de datos personales en el que se sanciona de uno a tres años a quien en beneficio propio o de un tercero, con daño para la intimidad o integridad y sin autorización del titular, realice algunas de las acciones descritas se apodere, modifique, interfiera, accede, copie, tramite, difunda, recopile, utilice, etc., para un fin distinto para el que fueron recolectados o de un tratamiento a esa información no autorizada. Recordemos que un dato personal es cualquiera que identifique a una persona directamente o que en su conjunto haga identificable a una persona. Todos trabajamos con datos personales indiscutiblemente. Y ¿adivinen para quién hay una pena más alta en estos casos? De nuevo para las personas encargadas de la salvaguarda o las personas encargadas del soporte o mantenimiento.

Tenemos delitos relacionados con daño informático que puede ser realizado por alguien de Archivística. Hay una sanción de uno a tres años al que sin autorización se le hubiera concedido, en perjuicio de un tercero, suprima o destruya información contenida en un sistema de red informática; y aumenta si la información se vuelve irrecuperable.

Y el tema de daño agravado también, cuando el daño recayera sobre redes o sistemas o sus componentes físicos, lógicos o periféricos o sea hasta el hardware. Si alguien realiza una acción contra él puede estar dentro del daño agravado.

También el tema de sabotaje. Si alguien sabotea la información contenida en bases de datos está dentro de esta figura y con la intención de sabotear viene todo un análisis que podemos conversar luego.

En materia de suplantación de identidad es importante que lo conozcan también porque muchas instituciones, empresas, o a nivel personal, pueden sufrir una suplantación de identidad y el tipo penal lo contempla para las personas físicas, jurídicas o marca. Entonces si una institución sufre una suplantación podría como persona jurídica, por ejemplo, poner la denuncia porque suplantaron a su institución en una red social.

Tenemos también la figura de espionaje informático, al que sin autorización (valiéndose de cualquier manipulación) se apodere, transmita, modifique, estudie, utilice, bloquee o recicle información de valor para el

tráfico económico de la industria y del comercio.

Hay otro delito muy amplio de instalación y propagación de programas informáticos maliciosos en el que si alguien realiza alguna acción por medio de la cual instale (o distribuya) dentro de su sitio web software malicioso (como malware, virus, troyanos, etc.) estaría dentro de esta figura que en Costa Rica es pena.

En cuanto a suplantación de páginas electrónicas, si el sitio se suplanta ya hay una pena de uno a tres años; pero si además el sitio captura información de las personas, la pena aumenta. Si alguien utiliza sus plataformas o algunos medios tecnológicos para facilitar los delitos informáticos descritos, la pena es de uno a cuatro años. Por ejemplo, los casos en que las personas facilitan sus cuentas bancarias para que se realice una estafa informática o pongamos el escenario que alguien facilita sus plataformas de servidores, equipos, etc., para ponerlo al servicio de alguno de los delitos, esa persona que facilita estaría dentro de esta figura. Igual está el delito de difusión de información falsa que afecte temas relacionados con perjuicios financieros o al sector financiero.

Entonces rápidamente, ¿cómo atendemos un incidente? El primer paso consiste en estimar las necesidades para la gestión de incidentes. Es una fase de preparación que tener personal que va a trabajar en la gestión de incidentes. Por eso es importante comenzar a planificar y capacitar a las personas que van a dedicarse a esta área, documentar los sistemas y redes que se usan en la institución para determinar qué es normal en una actividad de nuestro día a día y qué sale del contexto o de la normalidad de los procesos que realizamos, así tendremos algún tipo de mapeo que nos permita tener indicios de los incidentes que ocurren. Un punto importante es registrar los contactos de terceras partes. Muchas veces tenemos subcontratadas empresas que se encargan de la parte tecnológica. Entonces debemos tener claridad de a quién llamamos de esas empresas para que atiendan rápidamente si nos está ocurriendo alguno de estos tipos de incidente. Requerimos saber que existen los centros de respuesta y en el caso nuestro, a nivel nacional, saber que existe el C-SIRT Nacional que es el director de orquesta en materia de ciberseguridad a nivel país; buscamos colaborar y ayudar para mejorar la atención de incidentes a nivel público.

Los temas de los procedimientos de gestión son fundamentales. Las buenas prácticas señalan la necesidad de definir una política de gestión de incidentes y así determinar qué procedimientos seguir. Las instituciones tenemos que desarrollar estas políticas de gestión de incidentes dentro de nuestros procesos y tener un catálogo de cuáles son los incidentes que van ocurriendo o cuáles son los que pueden ocurrirnos más tradicionalmente ya que muchos conocemos estas listas y que pueden dar un impacto dentro de la institución.

La fase dos va a ser una detección y análisis y obviamente no se puede gestionar sino ha ocurrido un incidente; pero en caso de que ocurra hay que ver los indicadores. Los equipos de TI participan directamente, así como los equipos de la institución relacionados con ciberseguridad para ver qué alertas hay, qué ha pasado, que un antivirus levanta algún tipo de señal, la caída de un sistema o que los accesos por ejemplo estén lentos. Eso comienza a dar indicios de que algo puede estar pasando. Recuerden que un incidente no es solo un ataque; puede fallando algún equipo por algún tema natural o por deterioro, por ejemplo. Uno de los ejercicios importantes es la elaboración de mapeos de redes o de algunos grupos. De esta forma, se puede visibilizar una equis situación que está pasando en el país o si alguna institución está recibiendo una amenaza de un ciberataque o una amenaza de un grupo “hacktivista”. Por ejemplo, que ha pasado, se puede detectar que uno de estos grupos está organizando un ataque a equis institución para hacer un bloqueo de su sitio web.

En relación con las amenazas, es importante la priorización dentro del incidente. Debemos clasificarlas, porque

resulta fundamental ver qué vamos a atender primero y qué vamos a ir dejando dentro de la línea de atención de los servicios. Esto implica una metodología de “triage”. ¿Alguien ha escuchado ese concepto? Se utiliza mucho en medicina porque cuando hay una situación de emergencia se tiene que determinar a quién se atiende primero; si usted tiene un montón de situaciones de gente enferma en el mismo momento tiene que determinar quién está más grave, quién más propenso a sobrevivir o a quién voy a dejar que se muera. Así pasa en situaciones de emergencias graves, situaciones de guerras, situaciones donde se debe decidir a quién se salva y a quién no. En temas informáticos y en temas de un incidente informático debemos definir qué vamos a atender primero, qué vamos a levantar y que vamos a ir dejando. Dependiendo del corte a nuestro negocio, vamos a notificar el incidente e iniciar un seguimiento del evento en gestión dentro de este proceso.

En la fase tres vamos a un tema de contención, resolución y recuperación. Debemos recuperar todas las funciones, ver cómo fue la gravedad, recopilar la información y aplicar las estrategias y procedimientos definidos anteriormente. Ya contenido el ataque vemos que sistemas están afectados. Vamos a pasar a un tema de revisión, eliminar los componentes asociados y volver a poner en funcionamiento nuestros sistemas. Aquí hay actividades de resolución y recuperación.

Y finalmente están las fases posteriores al cierre. Es importante tener un registro común de lo que ocurrió para primero corregir y que no vuelva a suceder por lo menos un incidente igual; y sobre todo aprender. Eso es una parte fundamental para la que es muy útil llevar el registro de la atención de incidentes, para saber cómo actuar y evitar que vuelvan a ocurrir estos tipos de acciones.

Con esto cerraría, ahí les queda mi contacto cualquier cosa y ha sido un gusto compartir. Ahora en el foro esperamos estar ampliando dudas o consultas. Muchas gracias.



CARMEN CAMPOS RAMÍREZ

Muchas gracias a don Roberto. Considero que nos ha dejado muchas ideas centrales muy importantes.

También nos hace una propuesta de un día feriado, el 26 de enero, por el nacimiento del internet. Así que señor director tome nota. Nos da la mala noticia, o nos recuerda, de que no hay riesgo cero. Creo que eso es importante de destacar.

Y por el otro lado, en contraposición, la mejor forma es prepararnos para enfrentar ese riesgo y el tiempo es vital para poder atender un incidente que se nos pueda presentar. Normalmente reaccionamos o hay impacto en la prestación de servicios y en la imagen de una institución. Sin embargo, no debemos de olvidar que hay que buscar las causas reales y no solo centrarnos en la restauración de los servicios. Tenemos que buscar cuál fue el problema para poderlo enfrentar, prepararnos y que no nos vuelva a suceder.

Además, hace una caracterización de qué es un incidente, por qué lo llamamos ataque o qué significa un ataque y qué es lo que realmente sucede. Nos plantea algunos ejemplos para acercarnos a la temática y nos dice que es importante tener medidas y que, sobre todo, es muy importante tener personas preparadas en este campo. Eso es fundamental y constituye un desafío con los limitados recursos que tenemos: cómo hacer para poder organizarnos y que siempre podamos tener personas capacitadas para ayudarnos a enfrentar estas situaciones en la institución.

Nos habla de la importancia de la firma digital en todo este contexto y ¿qué decir de este recorrido rápido por el cuerpo normativo también?, para establecer sobre todo los delitos y las sanciones que vienen asociadas. Esperamos nunca vernos enfrentados a una situación como esas y por eso estamos hoy aquí, para aprender y evitar que nos suceda una situación similar. Termina don Roberto haciéndonos un recorrido por lo que él denomina los pasos para enfrentar la aparición o un incidente tecnológico. Seguidamente, le pido entonces a don Randall Barnett que nos acompañe, y le concedemos la palabra.

RANDALL BARNET

Muchas gracias, buenos días. Mi nombre es Randall Barnett, soy funcionario del Instituto Costarricense de Electricidad (ICE) del Centro de Respuesta de Incidentes Informáticos, muy similar a donde trabaja Roberto pero en la parte completamente del ICE. El ICE tiene su propio CSIRT.

Voy a empezar diciendo un nombre: Sayano-Shushenskaya. ¿Lo identifican? Es una central hidroeléctrica cerca de Siberia, en pueblo que se llama Sayanogorsk, en Rusia. Más o menos el otro mes se cumplen exactamente diez años del primer ciberataque exitoso contra una central eléctrica. Mucha gente cree que el primer ataque fue en el 2010 contra una central nuclear llamada Natans, en Irán. Pero el de Irán no fue ese el primero; fue ese el que les estoy mencionando en la Federación Rusa. ¿Por qué se los menciono? Ya casi aterrizo en ese sentido.

Las centrales hidroeléctricas tienen su generador eléctrico que funciona con la fuerza que el agua le da a unas aspas que hacen girar un eje metálico y este a su vez genera un campo eléctrico. Sí, el ICE tiene montones de represas hidroeléctricas. En este caso en particular, al igual que las del ICE, la infraestructura de esas represas representa en dimensiones aproximadamente unos tres pisos de altura. En el caso de las represas están pisos

hacia abajo. No tengo que decirles que los aparatos que generan la electricidad pesan toneladas y que son manipulados por sistemas que se llaman “Sistemas Scada”. Estos muestran a los técnicos en pantallas toda la información que esos sistemas van generando: la velocidad en la que giran las aspas, la cantidad de energía eléctrica que están produciendo, la velocidad con la que el agua baja a través de ese tubo madre y llega a las aspas para mover y generar energía eléctrica, etc. Me imagino que más de uno de ustedes ha ido a pasear a Guanacaste y han visto que en el camino hay unas grandes torres tubulares pintadas de rojo y blanco. Cerca de las represas hidroeléctricas existen esas torres que sirven porque el agua que baja por el tubo madre cuando golpea las aspas se devuelve; a eso se le dice golpe de ariete. Lo que hacen esas torres es recibir ese golpe de ariete y bajar el impacto del agua para que las máquinas no se descompongan porque pueden salir disparadas por el aire.

Bueno, volviendo a la parte rusa, resulta que probaron una ciberarma contra los sistemas scada de esta represa rusa. Fue tal el acceso que tuvieron, que cambiaron los números que esos sistemas presentan, y la medición con la que giraban las aspas fue tal que se desprendieron desde su base tres pisos bajo tierra y salieron disparadas varios metros en el aire. De las cinco turbinas dos salieron disparadas en el aire. Obviamente despedazaron el techo y se causó una inundación. El primer ciberataque registrado de la historia causó 64 muertes. Se considera que los códigos maliciosos ya no solamente te friegan el Word o que no podás encender tu celular sino que además causan muertes; es decir, se convierten en ciberarmas. No es una bala lo que te mata, es un código.

Para que ustedes más o menos aterricen en el contexto, el Instituto Costarricense de Electricidad tiene ya bastantes años y hemos pasado por muchas etapas de madurez con respecto al aseguramiento de sistemas de generación. Tenemos ahorita un modelo integrado de seguridad corporativa en donde se dan todas las directrices, normativas, procedimientos, guías, entrenamientos, software, gente especializada para lo que nosotros llamamos sistema crítico de infraestructura nacional. ¿De qué sistema estamos hablando? De la electricidad. Es decir, lo que les permite cargar sus celulares, lo que les permite tener luz en la cochera cuando meten el automóvil, etc.

Muchas veces nosotros damos por sentado la facilidad con la que en Costa Rica usted mueve la llave para que salga el agua y sale el agua, enciende el interruptor de la pared y hay luz en el bombillo. En muchos países eso no se da con tanta facilidad; sin embargo, cuidar eso que es parte de todo el conglomerado de infraestructuras críticas nacionales es una de las tareas más importantes. Les cuento un cuento. Si conocen el cantón de Valverde Vega, en la Zona Norte, y todos esos lados, sabrán que en ese cantón hay tres represas. Está el río Toro Amarillo. El ICE hace muchos años creó la represa hidroeléctrica Toro I y la Toro II; por ahí del 2013 creó la Toro III. Cuando se dio el terremoto de Cinchona el acceso físico a ese lugar era completamente bloqueado. ¿Qué hacían los técnicos del ICE? tenían que irse de Toro I por dentro a través de un túnel que comunica con Toro II para poder salir. Dentro de las obligaciones que tengo como funcionario del área en donde estoy, se encuentra hacer análisis de vulnerabilidades de todas las infraestructuras, subestaciones, agencias, edificios del ICE, represas, etc. Estamos hablando de no solo de lo hidroeléctrico, sino también de lo geotérmico y de patios solares, entre otros.

El ICE es gigantesco. Resulta ser que para poder llegar allá y no dar toda la vuelta con el carro para ahorrar combustible decidimos hacer el viaje entre Toro I y Toro II por el túnel. Estamos hablando de que es una caminata de 45 minutos en donde tenés que ir en línea recta, diagonal, para arriba, línea recta, diagonal, para arriba, para arriba y después línea recta. Más o menos como a los veinte minutos de caminar, tenés que llegar al final o te tenés que devolver y vas a durar lo mismo porque son 45 minutos para atrás o para adelante y 45 más 45 son 90 minutos de viaje solo ida y vuelta para llegar recoger la información de los servidores y devolverte. Son trabajos que no se ven; sin embargo, le permiten al costarricense cargar su celular, tener luz en la casa. Me imagino que los del Acueductos y Alcantarillados deben tener las bombas funcionando en las diferentes

municipalidades para que el agua llegue y salga al tubo.

¿Qué tiene que ver esto con ustedes, con archivística? Lo tiene que ver todo. Resulta ser que ustedes en su entorno de trabajo también deberían tomar en cuenta los riesgos inherentes a la ciberseguridad. Hay diferentes tipos de seguridad, hay seguridad electrónica, de la información, ciberseguridad, perimetral, cada uno con sus diferentes especialistas. La academia tiene que ver mucho y la razón es que si hay carreras que formen profesionales en esas áreas, el mercado costarricense va a necesitar nuevos campos de acción para que nuevos profesionales trabajen y puedan desarrollar sus habilidades.

Costa Rica, al igual que muchos países en el mundo, ha movido sus negocios hacia donde la tecnología apunte. Actualmente es al revés, uno debería mover la tecnología hacia donde el negocio apunte. La razón es que la tecnología solamente es una herramienta y no el fin. Así que le permite a usted no depender de proveedores o de ciertas marcas ni de ciertos profesionales para poder decidir hacia donde quieren producir. Costa Rica está en este momento en la revolución 4.0, en donde tenemos que pensar de forma lateral -decimos los informáticos-. Pienso de manera diferente, “out of the box” dicen los gringos. Muchas veces estamos en nuestro escritorio y tal vez podemos arreglar un documento de un compañero que no está. Perdón el tiquismo, nos hacemos los majes. Decimos “no, que lo arregle él”. Los norteamericanos tienen varias pero hay tres acepciones más usadas para decir responsable: “liable, accountable y responsible”. El liable es el responsable legal, el accountable es el responsable por otros y el responsible es el que básicamente presiona el botón de la bomba atómica, el directo. Muchas veces fungimos como mandos medios, o mandos superiores o como subalternos, y tenemos responsabilidades por otros o por uno mismo.

Básicamente, debemos definir la cancha cuando hacemos un análisis de riesgos en nuestra empresa. Tenemos que ver los procesos, los mapas de calor, la gente que está encargada de esos procesos. Si toda la parte de seguridad no importa en el ámbito, esto cambia si es archivística, sobre todo en la parte de documentación de seguridad de la información. Eso es de alta importancia para el país, la razón es que ustedes también son parte de la infraestructura crítica del país porque ustedes son los resguardos de la memoria del país, la memoria legal, etc., de todo lo que el país produce como documentación.

El mundo está produciendo aproximadamente unos 6.7 zettabytes de información. ¿Les es familiar la palabra zettabyte? Me explico con un ejemplo; un KB de información podrían ser unos granitos de arena en una cuchara; un mega, una cuchara sopera llena de granitos de arena; un gigabyte, podría ser un camión lleno de granitos de arena; un tera podría ser, no sé, medio país tapando las montañas llenos de granitos de arena. Un zettabyte podría ser Centroamérica completa llena de granitos de arena y ahí siguen para arriba. Yottabyte sería el continente completo lleno de granitos de arena tapando las montañas. Estamos generando tanta información de todo tipo que muchas veces se convierte en “infoxicación”; es decir, nos intoxicamos. Ustedes que manejan información, porque es su campo de trabajo, deben saber cuándo la información es importante o no y eso se hace mediante reglas definidas por especialistas en seguridad de la información.

En el ICE, como les dije, tenemos ya un largo camino recorrido. No ha sido sencillo. El ICE es enorme y en muchas ocasiones tenemos nuestra forma “Iceísta” de hacer las cosas. Pero siempre apuntamos hacia el beneficio del país o tratamos de hacerlo la mayoría de los que trabajamos ahí. El Instituto se ha preocupado por muchos años por velar por esa infraestructura crítica que es de ustedes, que les permite mantener una paz institucional, que funcionen las cosas, que los carros estén en las calles. ¿Se acuerdan para la huelga de las gasolineras? Costa Rica duró dos días y medio sin gasolina y ahí todo se paralizó. Eso es lo que dura el país, esa es la ventana de

atención. Después de dos días y medio de caos total, todo el mundo a pie, porque no hay con qué quemar puesto que todo el combustible se acabó y se quedó varado.

Pero lo que quiero que se lleven de esta charla es que a nivel internacional, en cuanto a seguridad cibernética, a la zona de Latinoamérica es uno de los sitios a los que más atención se le está poniendo por parte de los gobiernos. Ustedes también están montados en eso, la seguridad cibernética es horizontal a todas las profesiones, ¿quiénes no tienen un smartphone en este momento? Ustedes saben que ese teléfono es casi mil veces más potente que la computadora que llevó el Apolo XI a la Luna. Si hubieran tenido ese smartphone los del Apolo XI, muy probablemente no habrían sufrido de ningún problema computacional, a excepción de que hubiera consumido un poquito más de energía eléctrica.

Sin embargo, si usted pone a comparar el poder de cómputo de ese aparatejo que llegó allá contra el smartphone que usted tiene en la mano, tienen una supercomputadora, y eso no se lo enseñan a usted cuando compra el teléfono. ¿Qué hace usted con su aparato? Ver Facebook, YouTube, Netflix (para los que tienen dinero). Muy pocos lo utilizan para ofimática. Que sé yo, de repente tenés bitcoins y querés minar, ahí lo ponés; tal vez no mine mucho, pero podés hacerlo. Ese es el asunto; tomamos mucho la tecnología por omisión y no tenemos los cuidados que esta demanda. Si usted le da un smartphone a un niño (“tome entreténgase, porque estoy aburrido de estarlo chineando”), mejor dele un arma y que se dispare en el pie. Por ejemplo, puede caer en manos de un pedófilo.

En el 2013 el Ministerio de Salud declaró el suicidio infantil como problema de salud nacional. Costa Rica se nos está muriendo joven. Hace muchos años trabajé en el Organismo de Investigación Judicial (OIJ), en la sección de cárceles, y no es nada bonito ver a una persona ahorcada, más como en las películas que hacen hasta feo y vuelven a ver a la cámara. No les voy a describir escenas de ese tipo; pero no es nada bonito ver a un adolescente en la flor de la edad ahorcado en el baño, debido al bullying. Son tantas aristas en que la seguridad cibernética está tan metida en nuestra sociedad, es que nosotros ya nacemos con la tecnología. Y todavía se verán cosas peores en donde llegamos a la computación cuántica y a nuestra parte cognitiva. De hecho, creo que Elon Musk tiene un proyecto para implantación en el cerebro para ayudarnos a aprender mejor, tipo Matrix. Vean hacia dónde vamos, inteligencia artificial.

Los nuevos negocios, si ven la estrategia del ICE, incluye big data, ciberseguridad. Usted mira todas estas nuevas tendencias y dice: “¿Hay gente preparada en el ICE para eso? ¿Hay universidades que enseñan eso?”. La Universidad de Costa Rica enseña bioinformática para la parte de secuenciación genómica. Eso no es una carrera de la Escuela de Computación; es de la Escuela de Medicina. Sí se enseña aprendizaje de máquina en el país; hay cursos y especializaciones para inteligencia artificial, la parte de redes neuronales. Aquí tenemos un especialista; vean que el país tiene todas las condiciones para que los científicos puedan desarrollarse, y que eso suceda en instituciones del Estado es excelente.

Es un tema de aprendizaje. Aquí la tecnología nos afecta a todos, es horizontal a todas las profesiones; no podemos deshacernos de ella, a menos de que nos vayamos allá a los Crestones del Chirripó y ahí nos quedemos viviendo.

Les agradezco mucho su atención, muy amables.



CARMEN CAMPOS RAMÍREZ

Vamos a continuar; vamos muy bien de tiempo y los panelistas han sido muy puntuales. Don Randall nos da una perspectiva muy amplia. Nos saca del escenario y nos lleva al mundo y a los primeros incidentes tecnológicos. Nos recuerda, y nos emplaza, sobre cuáles pueden ser las consecuencias, no solo de la pérdida potencial de la información (que es un tema muy cercano a nosotros como archivistas) sino que también ya tiene que ver con las personas hasta su muerte, como lo comentaba, y de cómo es vital en una institución como en la que trabaja él, con un servicio vital para la sociedad como es el servicio de energía eléctrica. Muchas gracias a don Randall.

Ahora le cedo la palabra a don Ricardo Villalón quien nos va a compartir también sus experiencias en este campo.

RICARDO VILLALÓN FONSECA

Buenas tardes. Yo traigo una presentación pequeña; pero primero voy a presentarme nuevamente por aquello de que alguna persona no estuviera en la sala al inicio. Mi nombre es Ricardo Villalón soy profesor de la Universidad de Costa Rica. He trabajado en los últimos años en temas como computación en la nube, firma digital (apoyando al Micitt y al Banco Central). De hecho con Alexander Barquero hemos realizado una buena cantidad de trabajos en el tema. En los últimos meses nos hemos enfocado más en el tema de seguridad, en un modelo de seguridad que venimos trabajando y que queremos propagar, como le llamamos nosotros, a “grandes ligas”, si se puede a nivel de estándares internacionales.

No sé si a ustedes les pasó ahora que estaban oyendo a Roberto. Yo lo invité a una clase hace como cinco años.

Cuando terminó la clase yo dije “necesito una profesión alterna”; qué susto “meter las patas”, como decimos nosotros y hasta por ignorancia vernos envueltos en un problema complicado. Porque la ley es rigurosa. Cuando esto me pasó, me senté y pasé varios días pensando cuál podría ser la profesión alterna, hasta que yo dije: “no, vamos a entrarle al problema”. Y si a eso le sumamos el tema de una explosión como la que Randall nos presentaba ahorita, uno dice “ok, y a veces no soy capaz ni de cuidar mi maletín, ni mi teléfono apropiadamente, y me mandan a cuidar una cosa grandota que no entiendo cómo funciona y no sé qué hacer”.

Al respecto, me parece que la mesa redonda tiene un nombre muy apropiado. ¿Qué hacer? Porque realmente tenemos problemas para saber qué hacer cuando nos meten con temas de seguridad y en el caso particular de la temática del congreso que anotan ustedes: gestión de riesgos para lo que es continuidad del negocio.

Así que voy a dedicarle un rato a que intentemos entender qué hacer y entonces, como en su momento dije, vamos a reducir ese miedo a que me metan a la cárcel por hacer una cosa incorrecta (incluso sin quererlo). Vamos a ver cómo entrarle al problema de la seguridad y a proteger mi negocio con un poco más de base. Pienso que cuando uno reduce la incertidumbre, el problema se empieza a hacer pequeño. Entonces intentemos que el problema reduzca su tamaño.

Eso me pasó a mí y me gusta trabajar en las presentaciones usando los ejemplos en los que he cometido errores. Me imagino que a alguno de ustedes les ha pasado, pero esto que les voy a contar fue vergüenza de la propia, grande, cuando yo dije “trabajo en seguridad y se me quebró el teléfono”. Tan simple, lo tenía en una mesa estaba revisando un aparatito y un tornillito se cayó, y también el teléfono. Y así se quebró la pantalla. Y entonces dije “¿dónde quedó el aseguramiento del teléfono?”. Realmente me enojé conmigo mismo porque lo peor de todo es que tiene protector. Entonces yo dije “pero si hice análisis de riesgos, me senté a pensar en vulnerabilidades y amenazas y toda la cosa y después lo compré. Sí hice la tarea. Y aun así se quebró”. Eso es lo mismo que le pasa a los sistemas informáticos cuando nos hackean. En general ya tenemos un nivel de conciencia apropiado como para saber que algo tenemos que hacer en seguridad. Y entonces hacemos nuestro máximo esfuerzo, nos reunimos y empezamos a hablar de vulnerabilidades. Empezamos a hablar de amenazas y tratamos de proponer cuáles son los riesgos, de qué nos tenemos que defender. Avanzamos y hacemos algo... y al final nos golpean.

Ante la pregunta de qué podría estar fallando, voy a tirar algunas ideas que en la literatura a veces se quedan de lado y empezamos los procesos de aseguramiento en una etapa posterior. Vamos a revisar dónde debimos haber empezado y por ahí va el tema de la presentación.

¿Qué pasa normalmente cuando queremos hacer seguridad? Empezamos hablando de vulnerabilidades, amenazas y riesgos. ¿Cierto? Casi todas las conversaciones que tienen que ver con seguridad empiezan de la misma manera. Hoy les quiero proponer como mensaje importante de la presentación que realmente hay que hacer algo antes de entrar en ese análisis. Son cosas que incluso son más sencillas de establecer, como por ejemplo tener claras cuáles son las políticas de mi negocio. Se trata de las cosas que incluso si quiero defino antojadizamente porque así deseo que funcione mi negocio. Esas tienen que estar claras. Ahora voy a usar el ejemplo del teléfono para construir un poquito la solución.

Si tengo claro qué quiero como negocio, posiblemente pueda establecer objetivos de mi organización derivados de esas decisiones racionales o antojadizas, no importa. Se vale para lograr alcanzar los objetivos de mi negocio y a partir de ahí puedo empezar a trabajar en objetivos de seguridad. Si quiero tener un mayor nivel de confianza de lo que estoy haciendo, es hasta después de eso que tiene sentido empezar a hablar de vulnerabilidades,

amenazas y derivar riesgos y hacer todo ese proceso técnico que es complejísimo. Con esto no voy a pretender reducir el nivel de complejidad de seguridad; lo que vamos a hacer es entrarle de una manera más específica, más apropiada para el problema que yo tengo que resolver. La seguridad es compleja ahorita y vamos a tratar de dimensionar por qué es compleja, para entender por qué la vemos como una masa muy diluida, difusa. Si no entendemos es porque es un problema muy grande y en algunos elementos se vuelve muy técnica; pero en la base es un problema muy grande por atacar. Por esta razón debemos tener objetivos específicos para poder reducir.

Empecemos con el tema del teléfono. Si a la hora de proteger mi teléfono hubiera definido por ejemplo qué es lo que quiero, entonces digo “quiero que mi teléfono celular opere correctamente cuando los clientes necesiten comunicarse conmigo”. Vean que fue una definición de muy alto nivel, pareciera ser lo que vulgarmente llamamos una habladilla pero no; tiene mucho de fondo porque con eso estoy marcando el terreno. Ahí, por ejemplo, ya lo tengo explícito; pero está medio solapado, el que el sistema que quiero defender o que quiero atender es mi teléfono. Ahí no estoy hablando todavía de seguridad; sin embargo, sí estoy hablando de atender a mi teléfono. Ese va a ser mi sistema en este ejemplo y ahora cuando caminamos podemos hacer la analogía con sistemas que ustedes tienen aquí, como por ejemplo los sistemas del Archivo Nacional o los sistemas de las organizaciones donde ustedes estén trabajando.

Teniendo eso claro necesito velar porque el teléfono opere correctamente. Ahí tenemos que trabajarlo un poquito más. Así tan general está ambiguo. Se vale decir cualquier cosa de lo que yo quiero, pero el nivel de generalidad con que lo digo no puede ser cualquiera. Tiene que llegar a ser de niveles en donde puedo empezar a trabajar y construir cosas para que quede bien. Entonces me interrogo o me entrevisto a mí mismo y digo “¿qué es exactamente lo quiero decir con eso”; porque aquí soy el técnico y el cliente al mismo tiempo.

Aterricemos un poquito y definamos objetivos. Defino que quiero poder realizar llamadas de voz y conversaciones de chat. Además, decido que no quiero usar mi teléfono -de hecho así lo uso yo- para almacenar información sensible. Este aparato se lo llevan y hay un mínimo de información sensible; aunque después de que se me quebró, dudo que haya hecho bien el análisis de riesgos y entonces a lo mejor voy a tener que volver a revisarlo siguiendo un proceso como este. Pero digamos que en principio lo quiero solo para eso, ahora sí que necesito el nivel de seguridad de ese sistema para alcanzar los objetivos que la organización está planteando, necesito poder hablar y chatear. Intentemos bajar un poquito el nivel y entonces por ejemplo digo que el teléfono celular y todos sus componentes deben estar íntegros al realizar las llamadas de voz y conversaciones de chat, porque si el teléfono tiene algo malo no lo voy a poder usar. Supongamos que a partir de que se quebró la pantalla tengo problemas para chatear porque ya no veo en la base y con ese montón de rayitas menos veo. Ahora ya tengo problemas y hay momentos en que la gente dice que me escribe y no contesto, porque no veo y el teléfono no me ayuda o lamentablemente lo dejé que se dañara y algo en el parlante ya no me funciona bien. Se dañó el parlante y ya no es íntegro; no funciona para lo que quiero.

Pero, vean que estoy definiendo mis objetivos. Defino mis requerimientos que de seguridad, hablo de la integridad del teléfono. Defino que necesito que mi aparato esté materialmente correcto, que sea íntegro. Y así “marco la cancha” en cuanto a lo que necesito en materia de seguridad.

Noten que para llegar a este nivel no necesariamente tenemos que ser informáticos. Lo que tenemos que hacer es sentarnos a pensar en qué es lo que queremos y hasta dónde necesitamos llegar. Entonces no necesito un profesional en informática para este escenario. Lo que requiero es que a mi teléfono no le pase nada y

ahorita vamos a ver el análisis que hice. Este razonamiento que estoy haciendo aquí ahorita no lo realicé en su momento. Solo compré el aparato y le coloqué un protector para protegerlo. ¿Alguien analizó cual era el nivel de integridad que necesitaba en mi teléfono? Nadie, porque yo era el encargado y no lo hice así.

Muchas veces compramos soluciones tecnológicas que ofrecen proteger a toda la organización y nadie se sentó a definir cuáles eran los objetivos de seguridad que se necesitaban. Entonces por supuesto que cubren un montón de cosas. Por ejemplo, protegí todo mi teléfono excepto la pantalla porque el protector no llegaba a la pantalla, y ahí justamente se me quebró. Aquí es casi trivial decirlo, se entiende es como evidente Pero ¿qué hacemos cuando estamos con tecnología, cuando tenemos aplicaciones de software, componentes que no vemos, que ni siquiera entendemos que forma tienen porque ni los informáticos lo sabemos? ¿Qué hacer cuando tenemos un conglomerado de software de diferentes fabricantes implementando un sistema? Ya no puedo hablar fácilmente de la carcasa del teléfono, de la pantalla, de los componentes que están adentro porque no se ven, no tienen forma. Sin embargo, terminan siendo las partes de la cosa que quiero proteger. Necesito definir objetivos para que en el momento en que establezco controles yo pueda hacer un match para determinar si que lo estoy poniendo de seguridad corresponde con lo que necesito. Si es tan sencillo equivocarse con un simple teléfono imagínense si no lo va a ser con un sistema tecnológico grande.

Una de mis definiciones iniciales fue que requiero que el teléfono celular y todos sus componentes deben estar disponibles para realizar llamadas de voz y conversaciones por chat. Eso me pone a pensar: “si se lo roban no va a estar disponible; si lo pierdo no va a estar disponible; si se me queda encerrado en un cuarto con llave, no va a estar disponible. ¿Lo ven? Esto me pone a reflexionar, por ejemplo, en otro escenario de la seguridad. Porque la seguridad realmente se hace grande; a fin de cuentas termino estableciendo la seguridad sobre el sistema y todos sus componentes hasta el nivel en que decida que voy a implementarla. Entonces ese nivel de granularidad en el que atiendo la seguridad de un sistema me lleva a que sea algo muy simple (en función de las decisiones que tomé) o muy complejo (y posiblemente muy costoso) porque realmente el escenario lo ameritaba. Vean que aquí nosotros sabemos que el teléfono sólo lo protegemos por fuera; realmente no implementamos nada para todos y cada uno de los componentes que están dentro. Esto se debe que hacemos algunos supuestos que normalmente llamamos “verdades base”: suponemos que toda la estructura que está ahí dentro está bien hecha y que no necesita que la asegure; entonces si bien es cierto es parte de mi sistema, son piezas que yo asumo que no voy a tener que asegurar.

Cuando ya definí mis objetivos (es decir, definí que mi teléfono esté íntegro y disponible), puedo empezar a escarbar en todo el planeta (suponiendo que no soy profesional en seguridad), buscando cuáles son las posibles vulnerabilidades y amenazas para un teléfono que necesito que se mantenga íntegro y disponible.

Piensen en sus organizaciones. Cuando hay tareas que están distribuidas, hay un equipo de trabajo que tiene los recursos tecnológicos, otro tal vez hace las aplicaciones, otro maneja los datos. Pero todo es un sistema. Entonces se complica el tema de hacer la seguridad. Es más bien un tema de cómo nos organizamos para protegerlo, pues el sistema en sí es una unidad. Si ya definí y delimité mi sistema sea lo que sea (puede ser un teléfono o toda una nube), en ese momento podemos empezar.

Vean qué interesante a iterar por todos y cada uno de los componentes del sistema. Entonces hasta informáticamente se convierte en informatizable un poco la seguridad. Empezamos a iterar por los elementos, tratando de atender los requerimientos de seguridad que acabamos de definir (yo definí solo disponibilidad en integridad). Si me equivoco en paso previo de los objetivos objetivos, mal para mí; aquí ya no hay nada que

hacer. Si tenía que atender temas de confidencialidad de la información del teléfono y no los definí, va a pasar lo mismo que sucede cuando uno compra chunches para ponerle seguridad al sistema y no tiene muy claro por qué los está poniendo. Y como les digo, en tecnología es difícil ver cuál fue la omisión; porque si no la ve uno en el mundo real, menos con aparatos tecnológicos en donde casi nunca hay una persona que conozca el 100% y a profundidad el sistema que tengo aquí al frente. Eso ya no pasa, los niveles de complejidad son tales que ya no nos podemos dar el lujo de encontrar esos niveles de comprensión.

Ahora sí podemos empezar a hablar de vulnerabilidades y de amenazas. ¡Vieran qué interesante la literatura! Se revuelve mucho y parece no haber claridad en qué es una vulnerabilidad y qué es una amenaza. La primera es una debilidad en el sistema. Les comento este ejemplo me gusta usar: Superman es vulnerable a la Kryptonita, a Superman no le va a pasar nada en tanto no tenga la amenaza de tener Kryptonita cerca. En cambio Luisa Lane puede tener la Kryptonita a la par que nada le va a pasar porque no es vulnerable. ¿Qué es lo que pasa que en los procesos de aseguramiento? Al rato empezamos a proteger a Luisa Lane de la Kryptonita y nadie evaluó si eso tenía sentido. Porque resulta que me venden o me instalan aparatos que dicen “esto lo protege contra todo lo que usted necesita” y uno piensa “¿cómo sabe que es todo lo que necesito si no se lo he dicho?”.

Si bien es cierto los que están metidos en esto definitivamente no son nada tontos y ya hay patrones de todas las cosas que normalmente son un problema, por supuesto. Cuando monto una solución de seguridad, definitivamente esperaré que lo que me implementan resuelva una buena cantidad de los problemas con los que me voy a enfrentar. Pues tampoco somos tan diferentes; a la hora de montar sistemas tecnológicos, en muchos casos necesitamos requerimientos de integridad y en las mismas cosas. Por decir algo, necesito que no ingrese un virus y me modifique la aplicación de software que estoy usando o me dañe el sistema operativo. Eso sin pensarlo mucho lo va a querer casi cualquiera. El punto es: ¿eso resuelve todos mis problemas? O sea, ¿realmente definí mis objetivos de seguridad y los controles atienden las necesidades que tenía? La respuesta es: no se sabe, hay que establecerlos.

Otro ejemplo y así es en la vida real. Para mí, del teléfono, lo que me interesa es que funcione; evito almacenar información sensible. Imagino que si hago este análisis para una persona que pasa montada todo el día en un avión y que tiene que atender gente de un montón de países, no solo la comunicación va a ser indispensable; posiblemente tiene información sensibilísima aquí y mecanismos para ingresar a lugares porque necesita conectarse cada vez que se baja del avión en un sitio diferente. Tiene requerimientos de confidencialidad y de autenticación realmente relevantes. Pero noten que en mi caso no es así.

Realmente el tema de la seguridad hay que amarrarlo a objetivos. En esos no nos podemos equivocar porque el análisis siguiente va a estar incompleto. Ahora sí, luego de este punto empezamos a hablar de vulnerabilidades, de amenazas. Cuando se junta una vulnerabilidad con una amenaza se forma la contraparte y caemos a la definición de un riesgo.

Cuando vayan a hacer seguridad y quieren empezar a sacarse un poquito la angustia que nos dejó Roberto con toda esa legislación que tenemos y que hay que cumplir, tratemos de pensar en las altas esferas de la organización y cada uno en su nivel. Pensemos en cuáles son los objetivos de seguridad. Es necesario hacer un desarrollo y mapearlo, asociarlo con requerimientos de seguridad y necesitamos aprender qué es exactamente confidencialidad, integridad y disponibilidad. Son palabras que pueden sonar un poco ligeras; pero si queremos realmente hacer seguridad, hay que entenderlas. Qué es autenticación, autorización, auditoría, o bien, qué es no repudio. Hay una lista de objetivos que perseguimos con los sistemas de seguridad y ahorita estoy aquí

generando una de las condiciones o por lo menos describiendo, no generando, por qué la seguridad es compleja. Porque si estoy proponiendo un teléfono celular como un ejemplo simple y quisiera describir todas las partes de mi teléfono y decidir en cuáles me preocupan los servicios de seguridad que son relevantes, podemos hacer una hoja electrónica en donde tenemos todas las partes del sistema que me interesa proteger y todos los servicios de seguridad, y ya se hizo grande. Y si eso lo cruzamos con todas las posibles vulnerabilidades y amenazas que se pueden dar en cada punto y para cada servicio de seguridad, la cosa se hace más grande todavía.

En el modelo que hemos venido trabajando, para el que espero estar transmitiendo las ideas principales, no pretende inventar el agua tibia. Es decir, describamos el sistema con una estructura del todo y las partes, hagamos diagramas de los escenarios de interacción de los diferentes componentes del sistema y tratemos de encontrar los problemas de seguridad.

Este diagrama corresponde a uno de los trabajos que hicimos para firma digital nacional. Este es un escenario de un sistema para creación de una firma digital. La raíz de esa estructura jerárquica representa todo el sistema y de ahí para abajo se van desglosando o describiendo las partes del sistema y esas son todas las partes que tenemos que proteger. En este caso, por ejemplo, el objetivo de seguridad era solamente el no repudio porque era firma digital. Ahí teníamos un objetivo: que nadie pueda decir “yo no fui”; porque sí fue, y la ley lo manda. Tenemos un escenario, digamos, de lo que se llama un caso de uso, que es una persona creando una firma digital en donde componentes de este sistema se utilizan para hacer una firma y estoy delimitando en mi sistema cuáles son las cosas que voy a asegurar. Porque la complejidad de la cosa que tengo que proteger siempre va a estar ahí; lo que pasa es que necesito definir cuáles son mis prioridades, cuándo quiero proteger algo, si hay algo que no me importa que se dañe, o que se pierda. O que lo conozcan otros, ese no es un riesgo, no hay problema, asumo el riesgo y digo “para esto no voy a hacer controles”. Pero no debo hacer seguridad sin tener claro que estoy incluyendo todas las cosas que sí me importan y una manera es enumerarlas. Esto empieza a eliminar la incertidumbre. Es tener claro cuál es el sistema con el cual están trabajando, describan su sistema en sus partes y traten de aterrizar cuáles son los requerimientos de seguridad usando esas palabritas mágicas de integridad, confidencialidad, disponibilidad, etc.

A partir de ahí, el resto se vuelve bastante más mecánico porque si ya hice lo que necesitaba, entonces haciendo un análisis de riesgos que identifique precisamente lo que me dolía, ya puedo definir políticas, puedo definir controles que implementen esas políticas. Hay veces que en algunos sistemas el proceso de aseguramiento empieza en el último paso, se compran soluciones en donde llegan y montan controles de seguridad y todo el proceso para atrás no existe y la gente cree que está segura. Tal vez en algunas cosas porque, de nuevo, hay cosas que se implementaron para hacer seguridad y evidentemente no van a ser totalmente inútiles. Por eso es que de un momento a otro dicen, por ejemplo, “es que se me metieron y ¿por dónde, si yo tenía el firewall?”.

El problema sigue siendo más complejo todavía cuando hacemos seguridad. No solo nos interesa la dimensión del espacio; también el tiempo. Necesitamos hacer seguridad muchas veces y decidir si la hacemos antes, durante o después de los eventos. Entonces la cosa se multiplica por tres, el nivel de dificultad fácil es complicado. Y esta es una idea nueva, no la han visto en ningún lado: estamos trabajando una propuesta que le llamamos “cadenas de objetos”. Vean que cuando hablamos de seguridad empezamos a hablar del teléfono, de la información, del sistema operativo, de las aplicaciones y son un montón de cosas diferentes. ¿Cómo se aseguran? Resulta que hay relaciones entre ellos y puedo atender por ejemplo un proceso de aseguramiento solo de la información. Ese lo van a encontrar documentado en estándares. Sin embargo, también puedo encontrar procesos de aseguramiento de la infraestructura tecnológica. Resulta que si establezco una cadena de objetos que ayudan precisamente a

definir cómo se relacionan, digo por ejemplo “necesito confidencialidad de la información en un cierto sistema” y me fijo cómo proteger la información cuando esté almacenada. Pero eso me lleva a un objeto diferente que es -sigo con el ejemplo- la aplicación de software que quien lo manipula también necesita algún servicio de seguridad. Supongamos que la aplicación sea íntegra para lograr obtener la confidencialidad de la información, o que el sistema operativo que gestiona la aplicación también lo sea, o que el computador que contiene el sistema operativo y la aplicación también lo sean. Entonces hay una dentro del modelo que venimos trabajando; estas son cosas que estamos empezando apenas a proponer a nivel general.

Esto ayuda a simplificar el proceso, porque esa nube de piezas (que no entendemos cómo se relacionan unas con otras) se simplifica. Entonces me puedo enfocar en la información, en las aplicaciones de software, en los sistemas operativos, en la infraestructura tecnológica, en la persona. Por ejemplo, pensemos en la privacidad de las personas. Terminamos siendo parte de los sistemas. Si delimito que mi sistema cuida mi privacidad, esta se preserva de forma directa cuando me protegen algo a mí. Sin embargo, cuando se trata de mi información que está en un sistema, en ese caso no es un proceso directo y necesito que se preserve la confidencialidad de esa información para que mi privacidad sea la que necesito. El modelo lo que hace es intentar ser iterativo y desgranar el problema de la seguridad en piezas. Pienso que tal vez con los mensajes que les dejé, al menos se pueden sentar a pensar cuál es el problema que ustedes tienen por resolver y qué es lo que les preocupa, y posiblemente podamos mejorar un poquito.



CARMEN CAMPOS RAMÍREZ

Muy bien, hemos escuchado a don Ricardo con esta presentación que nos ha dado, haciendo uso de su capacidad didáctica de docente. Creo que nos ha permitido una mejor comprensión de un proceso que se llama análisis de riesgos, que resulta muy complejo sin lugar a dudas. Es de los análisis más difíciles que nos toca hacer, indistintamente de donde trabajemos, en este caso en los Archivos y en los sistemas de información que tenemos que hacer con muchísima seriedad. Hay mucho por aprender y se trata de procesos complejos; pero Ricardo nos ha hecho sentir que es muy sencillo. Esperamos poder hacerlo. Nos reta y nos presenta una metodología que nos dice que antes de abrumarnos con las vulnerabilidades y las amenazas es importante cumplir unas etapas previas. Esta metodología es la definición de la ruta de nuestro negocio, del objetivo principal, de nuestra misión en el caso de instituciones públicas, de nuestra visión, de nuestra misión, de nuestros objetivos y finalmente establecer objetivos de seguridad y hacer toda esta desagregación de tareas que nos plantea don Ricardo.

Muchísimas gracias a don Roberto, don Randall y don Ricardo por habernos acompañado el día de hoy y compartir con nosotros conceptos, ejemplos y propuestas metodológicas sobre e cómo abordar este tema. Un aplauso para nuestros panelistas.





The Role of the Archivist in Digital Transformation

James Doig

Assistant Director at National Archives of Australia

Thank you very much for the invitation to talk on “the role of the archivist in digital transformation.” It is an opportune time because the National Archives of Australia is leading a digital transformation push across Australian government, and we are also undertaking an internal digital transformation program in difficult fiscal circumstances, as we try to position ourselves as an exemplar agency for other government agencies.

Today I intend to discuss that work of digital transformation in the context of where the NAA has come from, where it is placed today, and where we are going. In that way I hope to give you some ideas about what has worked for us, what hasn’t worked for us, and our vision for the role of the NAA in the digital future.

It is important to take a step back sometime and see the forces that have shaped what we do and how we do it. That we get a much clearer idea about the role of the archivist in digital transformation.

So, what I intend to provide today is:

- An overview of the NAA
- The functions of the NAA and our role within government
- Challenges
- Current projects
- Future directions

Background

The National Archives of Australia is an executive agency of the Australian Government, established under the *Archives Act 1983*. We are a relatively young national archive.

The French National Archives was established by law in 1790; in the United Kingdom, the Public Records Office, as it was called then, was established in the 1850s; in the United States the National Archives and Records Administration was established in 1934, and it was not until 1950 that NARA acquired a Federal Records Act. Canada set up its public archives in 1872, and acquired its legislation in 1912.

The National Archives of Australia is younger than any of those institutions, and that is a good thing – it means we are more flexible and less tied to traditional approaches.

The National Archives was established as a small unit of one person within the National Library of Australia in 1944. It grew through the 1940s and 1950s to be a Division within the National Library, and its aim was to improve efficiency in the Executive arm of government by, amongst other things, providing training to records managers in government departments.

It was not until 1961 that the Archives Division got its independence from the National Library and became the Commonwealth Archives office. It took many more years for us to gain our foundation legislation. The Archives Bill was introduced to the Australian Parliament in 1978 and it did not become law until 1983. I'll talk a bit more the Archives Act later, but before that I'll talk about our organisation and our collections.

Collections

Australia is a big country, and we have an office in every state and territory in the country. Our head office is in Canberra, where I am speaking from. We have custody of over 356 kilometres of physical records held in repositories nationally. The largest proportion of holdings is in New South Wales (37% or 134km) and the Australian Capital Territory (33% or 116km), then Victoria (15% or 53km), Queensland (9% or 32km), Western Australia (4% or 14km), South Australia (4km), the Northern Territory (2km) and Tasmania (1.5km).

Of the physical records, by far the highest proportion as you would expect are paper files and documents – they comprise 77% of the total physical collection. But we hold many other record types like architectural drawings, maps, photographs, models, cards and so on.

Increasingly we have digital records – we have three primary digital collections. These are:

- Digital Archive – This collection contains primarily document and text based digital records transferred from government agencies or deposited by personal records donors. This collection comprises about 10 million digital files consisting about 10 tb.
- Audiovisual Archive – This collection contains digital audiovisual formats transferred from government agencies, and digitised copies of audiovisual formats produced for preservation and access. This collection comprises about half a million digital files, consisting of over 1.2 petabytes.
- Digitised Images – This collection contains images created through the digitisation of paper and photographic records. This collection comprises of 120,000 million mostly JPEG files, consisting of 75 terabytes.

Of course, these collections are constantly growing at a significant rate, and by 2026/27 we expect the digital collection to have grown to about 25 petabytes.

In total, our collection comprises about 40 million items – physical and digital – that's a lot of records to manage. Of that 40 million, about 15 million items are described on our catalogue, which means that most of our collection are not discoverable by the public at item level.

Archival Management Systems

What systems do we have to control and manage our collection? Our archival management system is called RecordSearch. It's an in-house built system comprising a number of modules that carry out archival functions and workflows. The main modules of RecordSearch were introduced between 1997 and 2004. Our delivery or access system is called Search and Retrieve – it is one of the modules of RecordSearch and is our public catalogue and the platform on which digitised records are displayed and downloaded.

Our other main systems are **Mediaflex (MFX)**, a commercial off-the-shelf asset management system acquired in 2014 for physical and digital audiovisual material, which was customised to meet the National Archives' requirements. And the **Digital Preservation System**, an in-house built software platform that went into production in 2007 that ingests, manages and preserves non-audiovisual digital records, like emails, office documents, data sets and so on.

Archival Control System – the Australian Series System

One last point to make – the archival control system – or descriptive system – we use to control our collection, is called the Australian Series System, which was developed by National Archives' staff in the 1960s and 70s. It is a system that is used across Australia and New Zealand, and in some overseas jurisdictions. It is an extremely flexible system that separates provenance information from record context – it is thereby able to track and document changes in the control and ownership of records by government agencies over time. This is important to us because government functions, and the records that document those functions, move around from government agency to government agency quite a lot – a process called administrative change.

Government Recordkeeping

I mentioned the Archives Act earlier, which is our foundation legislation and which clearly sets out our functions.

The Archives Act gives the National Archives very strong powers concerning recordkeeping practices in government agencies. In particular, the Archives Act is quite strong on disposal of records and transfer to the Archives. Only the Archives can authorise the disposal and destruction of Commonwealth records – we do this through legal instruments called Records Authorities. The Act introduced penalties if government agencies destroy or alter records. Once records were 25 years old, they were transferred as soon as possible to the Archives, unless destruction had been agreed. 25 years has now been reduced to 15 years. Also, the Archives has overall responsibility for determining which material is of permanent, archival value and therefore should be transferred into the custody of the Archives.

The Archives Act also has a very broad definition of “record” – basically it is any *thing* in any format that contains information – and the Act confirmed the Archives as the main adviser to agencies on keeping, evaluating and disposing of the records.

Digital Transformation in Government

You might be asking yourself, what does this have to do with digital transformation? It's actually quite fundamental – the Archives Act gives us strong powers to take a lead role in digital transformation across the Australian government.

Why is this important for archivists? One reason is that the quality of government recordkeeping and information management has profound downstream effects on the Archives. If government agencies are creating records in a consistent way in systems that are interoperable and designed according to recognised standards and best-practice, the Archives should receive archival-value records that are well described, complete and authentic. Poor recordkeeping and information management creates a huge legacy burden for Archives to impose control over records.

So, the National Archives has been in the business of transforming information management in government for a long time.

If we go back almost a quarter of a century, in December 1995, Australia became the first country in the world to develop a standard on records management – Australian Standard 4390.

Following the approval and release of the Australian standard, the international records management community began work on the development of an International Standard using AS 4390 as its starting point, and which was published as ISO 15489 Information and Documentation - Records Management. The Standard represents recognised international best practice guidance on records management.

In the late 1990s, the National Archives played a lead role in the development of a metadata standard called the Australian Government Locator Service (AGLS), which specifies 19 core metadata elements for resource discovery within a networked environment (in particular, the World Wide Web). All Australian governments have adopted AGLS as their standard for describing web resources.

At the same time, in the late 1990s, the Archives embarked on an ambitious research and development program that included a digital transformation program internal to the Archives.

It began with a world-first national archival institution training initiative – in 1998 the Archives placed all archival staff in the Government Services Branch in a year-long professional development program on contemporary recordkeeping – these were a set of tertiary units on digital records and recordkeeping providing by Monash University in Melbourne. Services offered to agencies were scaled back while professional officers of the branch juggled the roles of practitioner and student.

This period of professional development also marked the beginning of a new round of product development for government agencies.

The culmination of this activity was the release in March 2000 of the *e-permanence* suite of products. *e-permanence* delivered a re-invigorated message to government agencies on the importance of good recordkeeping to good government, backed up by a comprehensive suite of advisory products that agencies could use to build best-practice recordkeeping environments.

The cornerstone of *e-permanence* was the DIRKS Manual. DIRKS stands for Designing and Implementing Recordkeeping Systems, and built on ISO 15489 to provide comprehensive practical guidance on designing and implementing a recordkeeping system via an eight-step methodology. The manual also contained information about a range of related activities (such as how to build a business case for a recordkeeping system development project) and was supported with a training course.

The methodology gave rise to a number of practical tools that underpin good recordkeeping. It provided the essential framework to:

- establish a business case for recordkeeping;
- develop a business classification scheme that identifies and defines the unique functions and activities of an organisation;
- construct agency-specific classification tools such as a functions thesaurus;
- compile a functions-based records disposal authority for records unique to an agency;
- compile a general disposal authority for records relating to common administrative functions;
- adopt appropriate metadata standards for control and retrieval of records; and
- design or select records management software products and other electronic business information systems that meet an agency's requirements to create, control, retrieve and dispose of records.

A key component of *e-permanence* was the Recordkeeping Metadata Standard, which is a critical tool to describe information about records and the context in which they are captured and used in Australian Government agencies.

The first version of the metadata standard was developed in the late 1990s. It was designed to be used in conjunction with the DIRKS Manual, and the focus was on a single entity – the record. The second version of the standard was published in 2008 and was a complete revision, extending the standard to a four-entity model – Record, Agent, function and mandate, and describing in detail the relationships between the entities. This work fed into the international standard on Metadata for Records – ISO 23081 – which is a suite of three standards setting out principles, implementation issues, and a self-assessment checklist.

We are now up to version 2.2 of the recordkeeping metadata standard, which was released in June 2015. It's important to understand that the Recordkeeping metadata standard is a key product because it describes in detail the metadata properties that should be captured for each entity (i.e. record, agent, function and so on). Like any standard it describes a consistent approach for government agencies to manage their records, and as I mentioned previously, good recordkeeping practice makes the work of archivists easier when it comes to selecting, transferring and accessioning archival-value records.

The National Archives continued to produce products for agencies throughout the 2000s, including ideal functional specifications for recordkeeping systems and business systems, and contributing to standards development such as ISO 16175 – principles and functional requirements for records in electronic office environments.

However, just because the National Archives develops and publishes standards, guidelines and methodologies on recordkeeping and information management doesn't mean that government agencies implement them or even that they can be implemented by agencies. And this is an important lesson learned

- effecting digital transformation in government requires active and ongoing whole-of-government management and monitoring.

In 2007, for example, a report on recordkeeping in the Australian public service, *the MAC Report*, found that agencies were having difficulty in implementing the DIRKS methodology and that consequently it was taking a long time, in some cases years, for agencies to develop a Records Authority. As a result of this, the National Archives streamlined the DIRKS process and implemented quicker ways for agencies to develop records authorities.

What was more worrying was that we found as the 2000s progressed that most agencies had recordkeeping and information management practices that were far less than best practice.

One example of this was that we found very few government agencies had implemented the recordkeeping metadata standard. The feedback from agencies was that they were finding it difficult to implement because it is quite a complex standard, and recordkeeping areas within agencies were generally quite small, comprising lower level staff, and weren't well funded.

Our response to this problem was to develop what we call a minimum metadata set, which is a subset of the recordkeeping metadata standard, but easier to implement. The minimum metadata set defines a core set of 9 metadata properties required for the management of business information, and we require these properties to be mandatory when agencies transfer their records to us.

This is quite a good lesson learned – we need to be able to respond effectively when agencies are telling us they are having problems implementing our standards. If we fail to act, agency information management will not improve, which not only effects their efficiency and ability to conduct business, but it will have downstream effects on archives.

Another significant issue with government recordkeeping was that it became clear that agencies weren't necessarily managing their records digitally, but were printing them to paper. In 2010 we estimated the cost to government of storing their paper records was \$220 million per year. And of course printing to paper has a cost in terms of efficiency – records that are managed digitally consistent with best-practice principles and standards, are easier and quicker to find and retrieve for business purposes, it's easier to use and reuse the data and content in ways that add value, and it's easier to make those resources available to different users through digital channels.

So, since 2011 we have been a lead agency in pushing whole-of-government digital transformation. In July 2011 the Australian government released the Digital Transition Policy. This policy, developed by the Department of Prime Minister and Cabinet, aimed to move government agencies towards digital records management for efficiency purposes. Under the Digital Transition Policy, the 200+ agencies were expected to self-assess annually and submit the results to the National Archives; senior managers in government agencies were expected to drive change; agencies were expected to reduce their paper stockpiles, and agencies were expected to transition towards fully managing their digital information in digital formats.

The National Archives had a lead role in this work – we were to lead and promote the policy, develop a Digital Continuity Plan for whole-of-government, measure the success of agencies in effecting change, and report to government on the rate of transition and recommend further strategies.

In 2014 the National Archives released an online software tool called Check-up Digital that allowed government agencies to self-assess their digital information management capability and their maturity. The Check-up Digital tool allowed whole-of-government benchmarking and produced individual agency reports, so we were able to gauge their progress. These reports are published online, so they are publicly available.

In 2016 results showed that approximately 70% of government agencies had completed their transition to a digital information and records management environment. This was a strong result, as in 2013 the figure was only 40%.

The Digital Transition Policy said that the National Archives would develop a Digital Continuity Plan for government agencies, and this was issued in October 2015 as Digital Continuity 2020. DC2020 contained three principles: information is valued; information is managed digitally; and information, systems and processes are interoperable. DC2020 also identified a number of key actions for government agencies as well as interim targets and pathways. These targets include agencies having an Information Governance Framework by 31 December 2016; agencies have a Chief Information Governance Officer by 31 December 2017; and agencies implementing a program of professional development of information management staff to achieve professional recognition – in that way agencies will develop the skills and capability of their staff, which is key to digital transformation.

DC2020 winds up next year, and we are in the process of deciding on our information policy approach after 2020, so we can continue to build on the progress made. There is still a lot of work to do – a number of recent government reports have all noted the need for improved data and information in government, the importance making big data openly available to the public using digital channels, and the need to provide better digital services to the public – over the years there have a lot of failures in government due to poor recordkeeping and information management practices. In 2016 the government established an agency, the Digital Transformation Agency, which is charged with improving government digital services to the public. Late last year it released a *Digital Transformation Strategy*, which aims for Australia to be one of the top three digital governments by 2025. Whether that is achievable remains to be seen, but the strategy has direct implications for the National Archives, as the custodian of the most significant government data and information; and as the organisation that sets standards, and provides information management policies and advice to government agencies.

This is a good point to shift my focus and talk about digital transformation within the National Archives.

Digital Transformation Within NAA

In order to progress digital modernisation across the Australian Government, the National Archives needs to establish itself as an exemplar digital agency.

Over time the National Archives must transition to become a 'digital archive by default', meaning that the National Archives will move from working primarily with analogue records to working primarily with digital records (either in the form of born-digital records or digitised copies of analogue source records). However, this will mean that we will be working with a 'hybrid' collection for the foreseeable future. Our analogue collection is significant (over 350 kms in our custody, with an additional estimated 178km of permanent, archival-value records in agency custody). As I mentioned earlier, our digital collection will continue to grow

at ever increasing rates. In saying that the National Archives will move to working primarily with digital, the aim is to move for business decision making to be recorded digitally and for business processes to be more fully digital. Every action taken should have a digital outcome.

This future state is not something that the National Archives can control, but we can plan for it. We know that Commonwealth government agencies are creating vast amounts of records in digital formats, and that a significant proportion of those digital records will be transferred into the custody of the Archives. Some figures:

- A 2016 survey commissioned by the National Archives found that, of the 143 agencies that estimated their storage of digital records, approximately 29.4 petabytes of digital records were being stored. Approximately 15% of that storage capacity (or approximately 5 petabytes) is Retain as National Archives) and should be transferred to the Archives within the next 10 or so years. This figure does not include the vast quantities of digital records created by the national television broadcasters, or by the large scientific and research agencies.
- Of the 155 agencies that provided an estimate of their storage of physical records, approximately 102 million physical files were being stored, comprising about 15 hundred shelf kilometres. Approximately 12% of this storage volume (or about 200 kilometres) is estimated to be RNA. It's worth pointing out that General Records Authority (GRA) 31 allows agencies to destroy certain records after digitising them, so it is reasonable to assume that many of these physical records will be transferred to the National Archives in digital formats.

The future state of a 'digital archive by default' is a huge strategic challenge for the National Archives for the following reasons:

- The digital systems used by government agencies to create and manage information are diverse and complex, and they are rarely designed to support selection, disposal, and transfer to the National Archives.
- Digital records are complex – they *can* be a threaded discussion using a web-based application, a tweet with embedded video, websites, structured datasets and computer code – organising and managing digital records requires considerable digital knowledge and capability.
- Preserving digital records is difficult – because technology is continually changing (a generation of software and hardware only lasts a few years), there is no single solution to ensuring digital records remain accessible in the long term. The Archives must continually invest in order to ensure digital material continues to be accessible.
- User expectations have changed – the Archives must be able to provide meaningful access for the public to born-digital records. We must respond to changing user expectations around access and use. The world is becoming increasingly mobile, digital and virtual, built for personalised user experiences. Users expect services to be intuitive, for transactions to be easy and for results to be immediate. We need to make use of multiple digital channels – trends like the shift to mobile and tablets have had a significant impact on user expectations.

Current state

We also have concerns about our current systems, in particular the digital preservation software platform and the modules of RecordSearch. These were developed in-house some years ago. Some of the modules of RecordSearch are over 20 years old.

Specific concerns include:

- Lack of integration between different systems – as a result, end-to-end workflows are quite manual, and there is an increased risk of user error because system validation is not always possible
- Systems are inflexible, and cannot rapidly meet new business requirements;
- There is no standard metadata schema used to define files for digital ingestion or access. This impacts on the ability of the system to support automated workflows as well as inhibiting the ability of digital consumers to search for and retrieve digital content;
- There is system duplication within the Archives, with systems such as Mediaflex, RecordSearch, and the Digital Archive replicating some functionality;
- Digital access is currently limited to Search & Retrieve, which provides an incomplete view of digital content within NAA. Further, the process for identifying and linking common digital content across systems (e.g. RecordSearch and the Digital Archive) is manual and error-prone;
- There is no current capability for digital consumers to search across multiple repositories without significant manual effort
- There is limited capacity to deliver digital information to users in a form and method that meets their information needs yet retains the authenticity of the information.

In essence, the current digital archiving capability and policy framework cannot meet the minimum requirements for modern archival and preservation management.

Digital Transformation initiatives

Of course, we have known about these issues for a long time, and we know that digital transformation requires significant investment, beyond what we can afford within the budget constraints of government.

Over the years we have put proposals to government, called New Policy Proposals, for additional funding to effect change, which is to say funding to replace our aging systems, refresh our infrastructure, build skills and capability and so on. Sometimes these NPPs have been in partnership with other institutions such as the National Library, the National Film and Sound Archive and others. However, on each occasion we have been unsuccessful for whatever reason – sometimes these reasons are outside our control such as the Global

Financial Crisis. Nevertheless, we will continue to develop and put forward NPPs that set out clear value statements about the importance of investing in archiving.

Within our existing fiscal envelope there is still a lot we can do. For example we have, over the years, conducted internal efficiency reviews to look at our workflows and practices to determine what can be improved. In this way we have moved to almost entirely digital approvals for all processes, so we no longer need to keep paper forms, or scan paper forms into our systems.

We also look for opportunities to collaborate with other institutions on innovative projects. Some examples of recent work include:

- A project in partnership with Data61 and Department of Finance to bring together information on the location of functions within the Commonwealth Government, capturing how the responsibilities for each function are assigned to Commonwealth entities for any given point in time
- Building tools using AI and machine learning to automate the appraisal and disposal process in digital information and records management systems
- Participation in a UK National Archives Project to test the application of distributed ledger (ie blockchain) technology to archival digital records, eg to prove the long-term authenticity and integrity of digital records.

We intend to look for more opportunities for collaboration - there is the potential to develop more international collaborations, working with archival institutions around the world. However, once again the ability to collaborate successfully comes down to availability of staff and resources.

DA Taskforce and Capability Program

In July 2018, the Director General of the National Archives, David Fricker, established a Digital Archive Taskforce to develop and coordinate a Digital Archive Program for transformation within the National Archives. This represented a recognition that we needed to push digital transformation along at a faster rate if we want to become a leading archive in the digital age.

A number of projects and initiatives sit under the umbrella of the Digital Archive program, and I'll talk a bit about those.

Procurement

Firstly, there are a number of procurement projects underway. In 2018 the National Archives procured Enterprise Grade Storage, an S3 Object Store, for the secure storage of our digital collections and corporate records. The procurement will establish data centres at our Chester Hill and Canberra offices with high speed data links between them, and it will significantly increase our storage capacity in the coming years.

We are also transitioning away from using in-house built software to using widely-used open source and/or commercial off-the-shelf software systems. In late 2018 we issued an Approach to Market for an Integrated

Archival Management System to replace our current systems. The systems include digital preservation, archival management, and access and discovery systems. This is a large and complex procurement that fits within the wider whole-of-government digital transformation agenda, and will enable us to ingest, preserve and manage the large volumes of information created by government agencies.

Digital archiving policy framework

A key component of internal digital transformation is a policy framework that supports our digital business. Since the beginning of 2017 we have been reviewing our principles and approaches to digital preservation. Amongst other initiatives, the review published a new digital preservation policy which was released in 2018.

The revised policy moves away from the earlier emphasis on in-house developed, open source software solutions, and changes our earlier approach of converting proprietary formats on ingest. The policy places more emphasis on preservation planning and monitoring of data formats, and on other key elements such as the re-use of recordkeeping metadata standards for archival management purposes.

We have also developed a policy matrix setting out policy gaps and policies in need of review or updating, with a view creating a full suite of practices, plans and operational policies.

Data model and schema

We are also developing a new archival control model, building on the Australian Series System, that is capable of representing complex record structures. We have also developed a draft metadata schema for digital records based on existing standards such as the Australian Recordkeeping Metadata Property Reference Set (the Australian and New Zealand standard) and PREMIS, the key preservation metadata vocabulary.

We are also doing some work with linked data as we believe it has great strengths in terms of the exchange and sharing of metadata, and also in representing the complex interrelationships between records and other entities.

Capability

There are also a couple of important projects that aim to develop staff digital skills. Last year we carried out an audit of staff digital archiving skills using a European digital curation skill set called DigCurV. A group in the United Kingdom called Digital Preservation at Oxford and Cambridge (or DPOC) have done a lot of work in using DigCurV to create a training needs assessment toolkit and training programme pilot – they are very good products and we could easily pick them up and customise them for our own circumstances.

The DigCurV Curriculum Framework provides three ‘lenses’ onto digital archiving, one each for staff engaged as *Executives*, *Managers*, and *Practitioners*. Each of the lenses can be used to develop, evaluate, and plan training and professional development for staff engaged in digital archiving. We revised the DigCurV skill set in line with the particular skills required by archivists, and developed a survey that was completed by about 60 staff engaged in digital archiving activities, including digital preservation and digitisation.

The results of the survey were analysed and a Training Needs Assessment developed by Adrian Cunningham, a well-known international archivist. We are now in the process of implementing the training options recommended in the Training Needs Assessment. For example, in February we had Nancy McGovern and Kari

Smith from MIT deliver the 5-day Digital Preservation Management Workshop, and we are in the process of customising and reusing that material to develop internal training going forwards.

Future directions

I'll talk briefly about our future directions. The National Archives' vision is to be a world leading archive in the digital age. This requires us to re-envision our role within government and society in the digital future.

The National Archives holds more information than any other government agency, and it is the single entity that understands what information is held across other government agencies. This puts us in a particularly strong position to be the leading entity in providing government information as a service.

In other words, the National Archives of the future is the central point for whole-of-Government information. This role depends upon ensuring that government information is readily available to anyone who requests it. The role also requires a more proactive approach to managing information – it involves actively interpreting, curating and promoting the information, rather than waiting for users to seek the information or the National Archives merely 'making information available'. The National Archives is not the Government's storehouse, but a vital social, economic, cultural and educational resource. Innovations and technologies need to support this goal.

The projects we are undertaking will go some way to ensure we are doing the right things in the right way, and that we continue to drive the digital transformation agenda to position us for the future. But there is still a lot of work to do. Particular challenges include:

- Continuing to integrate, improve and replace our archival business systems so we can manage our digital collections;
- Providing meaningful access to the public and researchers to born-digital records, in particular complex data;
- Involving ourselves more closely in the development and procurement of hardware, software, business systems and standards that create and manage information in government agencies;
- Setting ourselves up as a research and development organisation that conducts digital research; and finally
- Continuing to invest in and develop staff digital skills.

These are big challenges and we've a long way to go.

Conclusion

In this talk I've tried to give an indication, based on the experience of the National Archives of Australia over the last twenty five years, of the range of digital transformation initiatives archivists can provide leadership on.

There are good reasons why archivists should have the lead role in digital transformation; in a fundamental way, archivists have always needed to understand recordkeeping systems, and the need for good recordkeeping practices by records producers.

Half a century ago, in 1969, Peter Scott, the person who developed the Australian Series System, said this about the role of the archivist: "the archivist concerns himself/herself not merely with historical records but above all with recordkeeping *systems*. I see the archivist as custodian, analyst, restorer, preserver and interpreter of original record-keeping systems in their historic context, and of the historical evidence and information, of the contents of such systems."

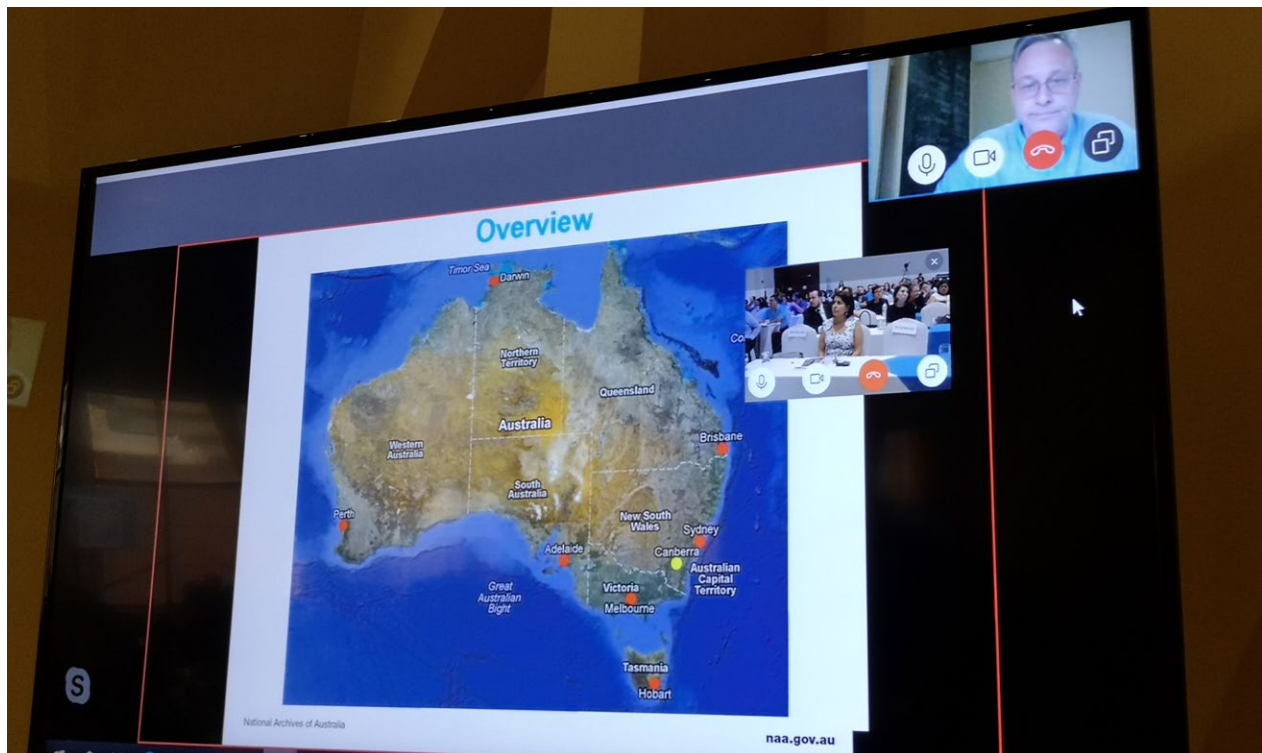
Understanding the systems used to create, manage and deliver records is our bread and butter. Understanding and analysing those systems is fundamental to our role of managing archives and making them accessible in meaningful ways. We understand what good recordkeeping is, because we've all seen the results of bad recordkeeping.

Our leadership in digital transformation in government will give government information inherent qualities and characteristics that enable that information to be managed for its intended business use and beyond, including its archival preservation, public discoverability, access, and delivery.

In terms of *internal* digital transformation, archivists of course have the key role. Our role there is to ensure that archival and digital preservation principles are heard and understood by ICT professionals who are responsible for procuring and commissioning systems and infrastructure. We do tend to speak a different language from ICT professionals, terms like "archiving", "backups", "storing multiple copies" have a different meaning or are interpreted differently. Data compression, which is ubiquitous in storage systems, may be anathema to archivists.

The role of the archivist here is absolutely essential to avoid catastrophe.

Much of this relates to the fact that we see things in the long term, and that's a rare thing in the digital environment where it's all about now, or what is just around the corner. The Records Continuum Model tells us that the life of the record is never-ending, that a digital record is always in a state of becoming, and that's the knowledge we always bring to the table.





ISBN: 978-9968-690-10-2

