La seguridad de la información en la administración pública

Kadú Josep Altamirano-de-la-Borda
kje1_2003@hotmail.com, kje12003@gmail.com /Investigador independiente

Recepción: 24/8/2020 Aceptación: 23/10/2020

Resumen. La información pública es producto de la administración y transformación de otra información que tiene un efecto directo en la ciudadanía, por lo cual debe ser protegida asegurando su confidencialidad, integridad y disponibilidad, teniendo siempre presentes los principios del derecho al acceso a la información de los ciudadanos. Si bien en el Perú se han dado los pasos adecuados para implementar los sistemas de gestión de seguridad de la información en el ámbito público, solo el 6 % de los organismos públicos ha cumplido con implementar lo dispuesto por la normativa vigente. Por lo cual se hace necesario que el Estado redoble los esfuerzos para proteger su información a través de la implementación de sus sistemas de gestión de seguridad de la información, ya que los nuevos escenarios referentes a la tecnología, la información y la interacción entre Estado y ciudadanía así lo requieren.

Palabras clave: seguridad / información pública / ciberseguridad

Information Security in Public Administration

Abstract. Public information is the product of the administration and transformation of other information that has a direct effect on citizens; thus, it must be protected by ensuring its confidentiality, integrity and availability, always keeping in mind the principles of the citizens' right of access to information. Although the appropriate steps have been taken in Peru to implement information security management systems in the public sphere, only 6 % of public entities have complied with implementing the provisions of current regulations. Therefore, it is clear that the government should redouble efforts to protect its information by implementing Information Security Management Systems, required by the new scenarios regarding technology, information and the interaction between government and citizens.

Keywords: security / public information / cybersecurity

1. INTRODUCCIÓN

Desde el inicio de los tiempos la información ha sido considerada como uno de los activos más importantes de una organización, ya que con base en esta se toman decisiones que impactan directa o indirectamente en la vida de las personas. A lo largo del tiempo, las formas de tratarla y protegerla han ido cambiando y evolucionando de acuerdo con las diferentes tendencias que se han ido desarrollando y adoptando según las necesidades propias de cada organización. En el presente trabajo se trata de dar una aproximación de lo que significa la seguridad de la información en el contexto de la administración pública, donde la información adquiere características muy particulares.

Este artículo está dividido en tres partes; en la primera se detallan las bases teóricas sobre el tema a tratar. En la segunda parte se desarrolla en sí lo que significa en el Perú la implementación y el avance de la seguridad de la información en la administración pública. Y, por último, en la tercera parte se realiza un análisis de lo expuesto y se expresan conclusiones sobre el tratamiento de la información y la seguridad de la información en el país.

2. ¿Y QUÉ ES LA INFORMACIÓN?

Es un mensaje producto del procesamiento de un conjunto organizado de datos que cambia el estado de conocimiento de una persona o sistema que lo interpreta. Este "mensaje" puede ser de diferentes tipos, formas y estructuras, que puede estar contenido en un sinfín de objetos ya sean tangibles o intangibles, de acuerdo a su naturaleza y tratamiento. Es importante mencionar que la información es cambiante, dinámica y que se puede ir transformando de acuerdo a nueva información o nuevos datos que influyan en esta. La información, se puede decir, tiene un ciclo de vida; en la actualidad el que ha sido definido y aceptado por la comunidad es el ciclo planteado por Rich Mogull de Securosis en el 2007:

Figura 1. Data Security Lifecycle 2.0
Elaboración propia, con información de Mogull (2011)

3. LA INFORMACIÓN EN LA ADMINISTRACIÓN PÚBLICA

Cleveland (1986) sostiene que "la administración pública e información es lo mismo, ya que la administración trabaja con información y el producto de la administración no es otro que información que ha sido transformada".

En el 2001, Muñoz Cañavate define a la información en el sector público como "toda aquella información que sirve al ciudadano". Indica también que:

> A diferencia de la información científica y técnica, cuyos límites vienen marcados por sus propios usuarios, especialistas en cada área de conocimiento; la información que se deriva de los flujos informativos entre administración y administrado no tiene los límites anteriores, ya que cualquier ciudadano es usuario potencial de los servicios de una administración (local, regional o nacional) y la información que se deriva de esos servicios es motivo de tratamiento.

Es en este entender que a los ciudadanos se les genera un derecho que es el del "acceso a la información", el cual sostiene que toda persona puede acceder a información que se encuentra en poder de las entidades públicas y, por tanto, estas deben entregar dicha información, siempre y cuando esta no se encuentre protegida por alguna de las excepciones previstas en la normativa que corresponda.

Este derecho está soportado por los principios siguientes (Mendel, 1999):

a. *Máxima divulgación*. Sostiene que toda la información del Estado debe ser pública, salvo excepciones debidamente justificadas contempladas en la ley o Constitución.

b. *Obligación de publicar*. Precisa que los organismos públicos tienen la obligación de atender las solicitudes de acceso a la información, así también, de procurar la publicación y difusión de información de interés público. Este principio considera ciertos límites razonables, que se circunscriben a recursos y capacidad. Las entidades estatales deben hacer pública la información siguiente como mínimo:

    i. Información operativa sobre el funcionamiento de las entidades públicas

    ii. Información sobre solicitudes o quejas realizadas ante una determinada entidad pública

    iii. Información sobre cómo la ciudadanía puede contribuir al proceso de formulación de políticas públicas; los tipos y formas de información en poder de las entidades públicas

    iv. Información sobre decisiones y políticas que afectan a la ciudadanía, la cual contiene los antecedentes sobre las mismas, la evidencia que llevó a su formulación, así como información relacionada

c. *Promoción del gobierno abierto.* Sostiene que para garantizar el derecho a la información, los gobiernos deben promover de forma activa una cultura de apertura y transparencia.

d. *Alcance limitado de excepciones.* Las excepciones al acceso libre a la información deben tener una base en excepciones con una justificación razonable y explícita.

e. *Procesos para facilitar el acceso.* Precisa que las solicitudes de información pública deben ser procesadas de forma justa y rápida; asimismo, se debe proporcionar un mecanismo de revisión independiente al solicitante en caso se dé un rechazo.

f. *Costos.* Sostiene que los costos de acceso a la información pública no deben ser un obstáculo para que el ciudadano pueda acceder a realizar una solicitud de información.

g. *Reuniones abiertas.* La libertad de información contiene el derecho de la ciudadanía a participar en la toma de decisiones y a saber cómo se comporta el gobierno en su nombre.

h. *La divulgación tiene prioridad.* Toda ley relacionada con el tratamiento de la información pública debe ser consistente con el principio de máxima divulgación y los demás principios que sustentan la libertad de información.

i. *Protección para denunciantes.* Las personas que comparten información al público sobre las irregularidades del gobierno, como la corrupción, entre otros, deben ser objeto de protección ante cualquier tipo de sanciones administrativas, legales o de otro tipo.

4. LA SEGURIDAD DE LA INFORMACIÓN

La norma ISO/IEC 27001 define a la seguridad de la información como el conjunto de medidas preventivas y reactivas que adopta una organización o sistema tecnológico que permite el resguardo y protección la información teniendo como base los siguientes principios:

a. *Confidencialidad*. Es la propiedad que asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.

b. *Disponibilidad*. Es la característica de la información de encontrarse a disposición de quienes deben acceder a ella en el momento que así lo requieran.

c. *Integridad*. Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas.

5. SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI)

La norma ISO/IEC 27001 define a un SGSI como un conjunto de políticas de administración de la información cuyo propósito en una organización es el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente el acceso a la información, con el fin de asegurar la confidencialidad, integridad y disponibilidad de la información minimizando a la vez los riesgos de seguridad de la información.

6. PROTEGER LA INFORMACIÓN PÚBLICA

En los últimos años se ha visto un creciente esfuerzo por parte de las entidades del sector público de "proteger" la información, teniendo como base las directivas y normas legales vigentes referentes al tema y como ejemplo la implementación del estándar ISO/IEC 27001, la Ley de Protección de Datos Personales, entre otros. Además de ello, es preciso mencionar los esfuerzos del Estado para poder compartir la información relevante con la ciudadanía, como la Ley de Transparencia, entre otros.

En un estricto sentido conceptual y teórico se podría sostener que para "proteger" la información simplemente debemos cumplir con la implementación y cumplimiento de las normas y directivas vigentes. Sin embargo, en razón del "matiz" único que asume la información en la administración pública, la aplicación de la seguridad se vuelve una tarea compleja, ya que se abren diferentes frentes basados en el punto de vista de las partes del Estado, lo cual hace necesario buscar y encontrar un "justo medio" para definir qué información se debe proteger, hasta qué punto se debe proteger y de quiénes debe ser protegida; en otras palabras, definir la confidencialidad, integridad y disponibilidad, ya que desde el punto de vista del ciudadano, tomando en cuenta lo indicado por Muñoz Cañavate, este puede considerar que tiene el derecho de poder acceder a todo tipo de información. Ahora bien, desde el punto de vista de la administración pública se puede considerar que el ciudadano solo debe recibir cierta clase de información.

7. ¿Y CÓMO LOGRAMOS EL "JUSTO MEDIO"?

Sería ideal poder seguir una única fórmula, pero al ser un problema tan complejo, que está influenciado por diferentes intereses y una variedad tan amplia de información, se hace imposible establecer una receta general. Aun así, es posible definir los aspectos generales que determinen cómo se puede llevar a cabo la tarea, pero ¿cómo? Pues bien, la primera tarea es definir las reglas de juego, es decir, el "qué" y el "cómo"; en este punto en el Perú se han dado pasos significativos, primero desde la definición de los parámetros de la transparencia en la administración pública

que en el Perú se tienen previstos en la Constitución Política y la Ley 27806, Ley de Transparencia y Acceso a la Información Pública (Novoa, 2016), y luego a través de la Secretaría de Gobierno Digital que "lidera los procesos de innovación tecnológica y de transformación digital del Estado y que tiene entre sus funciones elaborar los planes, políticas, normativas y directivas en el marco de las competencias teniendo en cuenta las necesidades y realidades del Estado en su conjunto" (PCM, 2020), es decir, definir toda la estructura legal y regulatoria para soportar la implementación y mantenimiento de la seguridad de la información.

La segunda tarea es la implementación; en este punto dicho trabajo se vuelve un tanto difuso, ya que existen diferentes factores que impactan negativamente en este esfuerzo (Seclén Arana, 2016); es en este punto en que la búsqueda del equilibrio se hace imperante, pues al establecer el Sistema de Gestión de Seguridad de la Información, las organizaciones deben definir cuáles son los alcances de las características de la información, situación que representa una tarea delicada y de precisión para no ir en contra del ciudadano y su derecho al acceso a la información, soportado por los nueve principios previamente descritos, aunque es importante indicar que estos pueden ser enmarcados en los ámbitos de los objetivos de los principios de la seguridad de la información:

Tabla 1
Relación entre principios

Principios "Derecho de acceso a la información"	Principios de seguridad de la información			Relación entre principios
	Confidencialidad	Disponibilidad	Integridad	
Máxima divulgación	X			La información debe estar clasificada para "autorizar" su divulgación según corresponda.
Obligación de publicar		X	X	La información debe ser compartida en tiempo y forma, guardando las garantías de autenticidad necesarias.
Promoción del gobierno abierto		X		El gobierno debe procurar la "disponibilidad" de la información.
Alcance limitado de excepciones	X			La información debe estar clasificada para "autorizar" su divulgación según corresponda.

(*continúa*)

(*continuación*)

Procesos para facilitar el acceso		X	X	El gobierno debe brindar las herramientas y recursos que sean necesarios para compartir la información en tiempo y forma.
Costos	X	X	X	El costo no puede ser obstáculo para garantizar la seguridad de la información y el acceso a la información.
Reuniones abiertas		X		El gobierno debe procurar la "disponibilidad" de la información.
La divulgación tiene prioridad	X			La información debe estar clasificada para "autorizar" su divulgación según corresponda.
Protección para denunciantes	X			La información en casos de denuncias debe ser clasificada y asegurada.

Elaboración propia

Se ha mencionado que la información es cambiante; por ende, su protección también adquiere esta característica, situación que se refleja en el ciclo de vida de un sistema de seguridad de la información, según la norma ISO/IEC 27001:

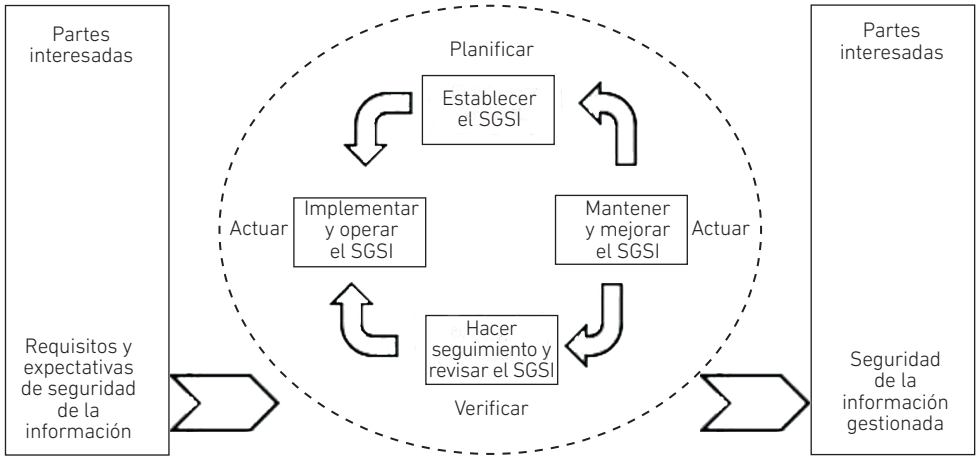

Figura 2. Ciclo de vida de un sistema de gestión de seguridad de la información

Fuente: ONGEI (2010); Frayssinet (2016)

Esto significa que la tercera tarea es el seguimiento y control; como se ha mencionado antes no basta con "cumplir" con la normatividad vigente, sino que es necesario evaluar cómo se está desarrollando la protección. Es importante medir de forma constante cuán eficiente y eficazmente está siendo protegida la información de modo que, de acuerdo a las necesidades, se ajuste a la seguridad de la información.

Por tanto, se puede sostener que el camino para proteger la información pública tiene tres etapas y por su naturaleza estas tienen una relación cíclica:

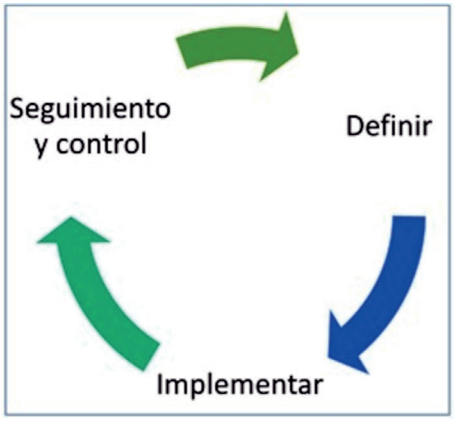

Figura 3. Tareas para proteger la información pública
Elaboración propia

8. LOS PARTICIPANTES

En el punto anterior se ha explicado cuál es el camino para lograr proteger la información pública, y la pregunta cae de madura: ¿y quién hace qué? La respuesta es muy compleja en razón de la naturaleza propia del Estado y su estructura; sin embargo, se pueden determinar dos actores macro: el ciudadano, representado en la sociedad civil, y el Estado. El primero tiene un derecho que es el de "acceso a la información" (Novoa, 2016), el segundo tiene la obligación de cumplir con ese derecho. El Estado peruano se puede representar de la siguiente manera:

Figura 4. Estructura del Estado peruano
Fuente: Correa (2010)

Ahora bien, dentro de la tarea de cumplir con el derecho al acceso a la información de la sociedad civil, es necesario ir especificando cuáles son las funciones y responsabilidades de cada parte del Estado, partiendo de la premisa de que unos definen y otros hacen, ya que el Estado tiene una naturaleza jerárquica:

a. Los que definen

   i. Gobierno nacional

   - *El Poder Ejecutivo*. Entre sus funciones varias tiene como objetivo el reglamentar la normativa establecida para cumplir la ley y reglamentar las normas que correspondan. En el caso estricto materia del presente artículo, vendría a ser la parte del Estado que establece el "cómo" hacer las cosas, así como velar por el cumplimento de los objetivos planteados respecto a la seguridad de la información en la administración pública. En el país, el organismo encargado de esta función es la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital.
   - *El Poder Legislativo.* Esta parte del Estado es quien, en representación del pueblo, dicta el "qué" hacer, esto a través de las leyes que son la norma general sobre algún aspecto de las relaciones sociales. En referencia al tema

tratado, por ejemplo, el Congreso ha establecido la Ley de Transparencia o la Ley de Protección de Datos Personales, por citar algunos ejemplos.

- *Entes autónomos*. En el sentido estricto del tema tratado, el rol de estos entes viene a ser el de consultores del Poder Ejecutivo. Y en algunos casos, de ahondar en las definiciones establecidas para adecuar o fortalecer a su área de influencia.

b. Los que hacen

En esta categoría se agrupa a todo el aparato estatal, es decir, a los tres niveles de gobierno y a la sociedad civil. Ya que es responsabilidad de todos el cumplir con las normas establecidas. Todas las entidades deberán realizar la tarea de implementar la seguridad de la información, adecuando de acuerdo a sus necesidades y utilizando las herramientas y mejores prácticas permitidas por la ley. Es preciso mencionar que la "adecuación" a las necesidades no les da a las organizaciones la discrecionalidad de poder "interpretar" la normativa, escoger qué parte de la normativa se va a cumplir o implementar, o modificar los procesos macrodefinidos, ya que esto iría en contra de los principios del derecho al acceso a la información, solo le da la potestad de poder "organizar" y "clasificar" su información para poder definir las excepciones de forma justificada, explícita y de alcance limitado y al "matizar" los procesos de acuerdo a la necesidad y recursos que tienen.

9. ¿CUÁNDO PROTEGER LA INFORMACIÓN?

Ya se han definido el qué, el cómo y el quién, ahora corresponde definir ¿cuándo? Y la respuesta es simple y tajante: siempre. Sin embargo, en la práctica esto no es tan simple; si bien la seguridad de la información ha formado parte de la vida cotidiana a través de la historia de la humanidad, los esfuerzos por normarla y estandarizarla a nivel global son relativamente nuevos; podemos considerar un punto de quiebre e hito en este esfuerzo: la publicación, en el 2005, de la norma ISO/IEC 27001 a nivel mundial.

10. ¿Y EN EL PERÚ, CUÁL ES EL ESTADO DE LA SITUACIÓN?

En el país, en concreto en el ámbito público, se dispuso, en el 2016, mediante Resolución Ministerial 004-2016-PCM la obligatoriedad de la implementación del Sistema de Gestión de la Seguridad de la Información según la norma técnica peruana "ISO NTP/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos, 2.ª edición", en todas las entidades integrantes del Sistema Nacional de Informática en un plazo no mayor de dos años. Se debe resaltar que este mecanismo fue

necesario, ya que por naturaleza las normas técnicas peruanas son enfocadas más que todo en el sector empresarial y son de cumplimiento voluntario, no pasibles de sanción (INACAL, 2016).

Esta ordenanza, sin embargo, nos presenta algunas interrogantes, siendo las más importantes las siguientes: ¿qué es el Sistema Nacional de Informática?, ¿quiénes conforman este sistema? y ¿se cumplió el objetivo propuesto? Pues bien, El Sistema Nacional de Informática era "el conjunto de entidades del sector público, interrelacionadas entre sí, que en forma integrada, coordinada, racionalizada y bajo una normatividad común, desarrollan actividades informáticas oficiales" (ONGEI, 2010) y estaba conformado por algunas entidades del sistema público; es importante mencionar que no era parte de este sistema TODO el aparato estatal, estaba restringido a entidades como ministerios, organismos autónomos y algunas organizaciones adicionales. ¿Y los resultados? Pues, en primera instancia, se podría decir que sí se ha cumplido con el objetivo, ya que todos los integrantes del Sistema Nacional de Informática, conformado por setenta y un organismos públicos (Seclén, 2016), implementaron sus sistemas; sin embargo, se debe considerar que el aparato público cuenta con 2940 entidades públicas aproximadamente (PCM, 2017). Es decir, en un principio, bajo el cumplimiento de la Resolución Ministerial 004-2016-PCM solo el 2,4 % de entidades públicas implementaron su Sistema de Gestión de la Seguridad de la Información.

Entre los años 2016 y 2020, se ha visto una marea de cambios en lo que concierne a los temas de gobierno y transformación digital, desde el enfoque con el que se asumen de una manera mejor estructurada los conceptos de datos, información y las tecnologías de la información en la administración pública y, por ende, también desde la seguridad de la información, como en el marco regulatorio. Estos son, en mi opinión, los cambios más trascendentales:

- En el 2018 la publicación de la Ley de Gobierno Digital, aprobada por Decreto Legislativo 1412, donde "se establece el marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos. Asimismo, define el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno" (PCM, 2020).
- Y en el 2020, la publicación del Decreto de Urgencia 006-2020, Decreto de Urgencia que crea el Sistema de Transformación Digital, que según su artículo 4 es de aplicación para todo el aparato estatal y según una de sus disposiciones complementarias dicho sistema reemplaza al Sistema Nacional de Informática. Indica también que el ente rector de este sistema es la Secretaría de Gobierno Digital.

¿Por qué son importantes estos cambios? En definitiva, porque el Estado, a través de los órganos que corresponden, comienza a establecer cuáles son las bases sustantivas para su funcionamiento y su interacción en referencia al tratamiento de la información y más aún en

un escenario donde la tecnología y lo digital es el principal participante. Este escenario nos plantea también nuevos retos, ya que el Estado depende solo de él mismo para poder avanzar en la dirección correcta, pues como se muestra a continuación, si bien el Estado promueve el cambio y la seguridad de la información, es este mismo ente quien no ha logrado cumplir con sus propios objetivos.

Como todo proceso requiere ser medido, todos los años la Secretaría de Gobierno Digital (antes ONGEI), ente rector del Sistema de Transformación Digital, lleva a cabo la Encuesta Nacional de Recursos Informáticos en la Administración Pública, donde se tiene como objetivo "mantener actualizada la información técnica sobre los recursos informáticos y tecnológicos de las entidades de la administración pública, a efecto de medir sus capacidades y potencialidades en materia tecnológica de información y comunicaciones (TIC), analizar la capacidad tecnológica instalada del Estado en los diversos departamentos del país" (PCM, 2013).

En el año 2020, según los datos recabados por la Secretaría de Gobierno Digital (PCM, 2020), respondieron a la encuesta 445 entidades públicas, que representan el 15 % del total de estas organizaciones, y de este universo se tiene que el 42 % cuenta con políticas de seguridad de la información, el 65 % refiere tener un área o persona asignada de manera exclusiva a la seguridad de la información, el 36 % de las entidades que contestaron la encuesta indican que han realizado la clasificación de sus activos informáticos y el 53 % señala que sus usuarios están preparados para reportar incidentes de seguridad en sus sistemas de información. Estos datos pueden ser expresados de la siguiente manera:

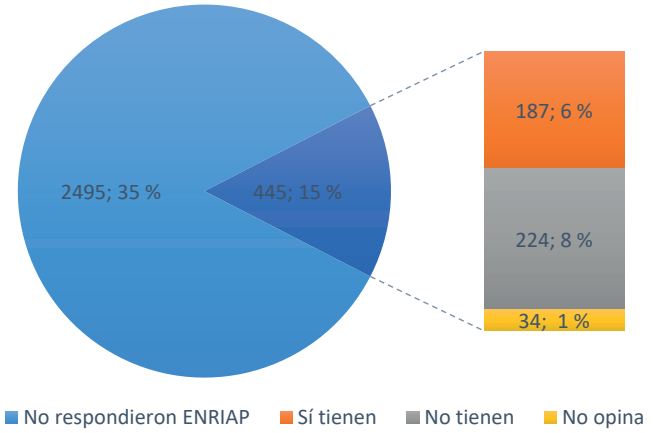

Figura 5. Cantidad de entidades públicas, respecto del total, que tienen políticas de seguridad de la información
Elaboración propia

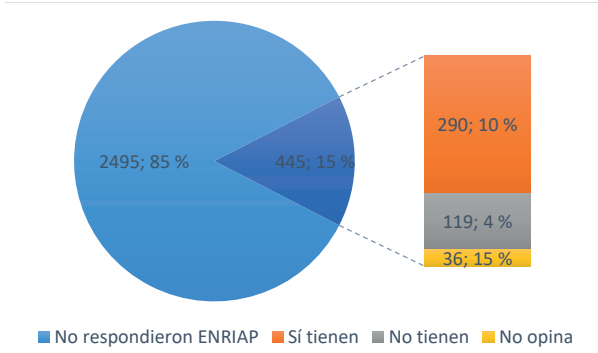

Figura 6. Cantidad de entidades públicas, respecto del total, que tienen un encargado exclusivo de seguridad de la información
Elaboración propia

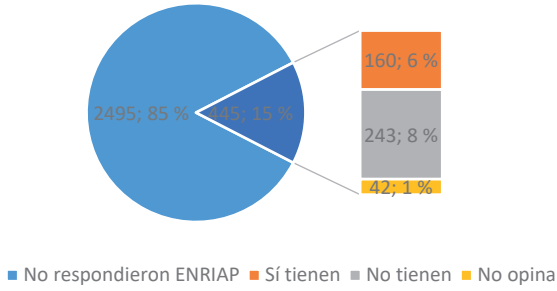

Figura 7. Cantidad de entidades públicas, respecto del total, que han clasificado sus activos informáticos
Elaboración propia

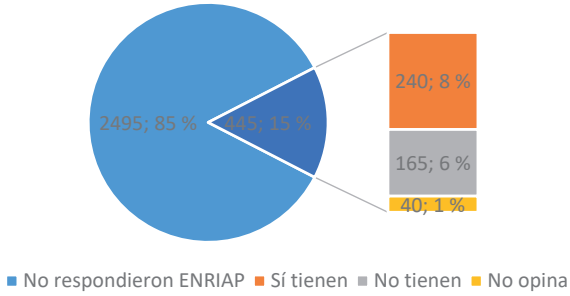

Figura 8. Cantidad de entidades públicas, respecto del total, cuyos usuarios están preparados para reportar incidentes sobre seguridad de la información
Elaboración propia

De lo antes señalado, se puede sostener que el panorama referente a la seguridad de la información en el aparato público es de por sí preocupante, ya que para el año 2020, de las 2940 entidades que lo conforman, solo el 6 % tendría definida su política de seguridad de la información y solo el 6 % habría hecho la clasificación de sus activos informáticos, ambos, requisitos indispensables. Ocurre del mismo modo con la base de los sistemas de gestión de seguridad de la información y lo que llama aún más la atención es que solo el 8 % de los usuarios de los sistemas informáticos del aparato público está preparado para reportar algún incidente referente a este aspecto, que en términos de personas y siguiendo la premisa de que todos los servidores públicos son usuarios de los sistemas informáticos de sus entidades, representan aproximadamente ciento doce mil usuarios, ya que según SERVIR en el 2016 la planilla estatal la conformaban aproximadamente 1 400 000 personas. Ahora bien, es importante recalcar que se está asumiendo que todas las entidades que no respondieron la ENRIAP tienen respuestas negativas a las interrogantes planteadas.

Este escenario nos muestra que la seguridad de la información en el aparato público no es una prioridad o no tiene la importancia que debe y, por tanto, la información no está debidamente protegida, situación que por añadidura hace que este derecho por parte de la ciudadanía no se pueda cumplir a cabalidad. Sin embargo, es importante resaltar que si bien la seguridad de la información en el escenario actual no es "relevante" para el Estado y a pesar de los problemas que enfrenta su implementación (Seclén Arana, 2016) se tienen las bases para poder hacerlo, esto viene más que todo como consecuencia del cumplimiento de la Ley de Transparencia que data del año 2002, dado que su puesta en ejecución exige que las entidades del ámbito público hayan puesto (*de facto*) en marcha una especie de "Sistema de Gestión de Seguridad de la Información", ya que el cumplimiento de la ley logra establecer todos los procedimientos necesarios para gestionar el acceso a la información asegurando los tres pilares de la seguridad de la información. ¿Cómo así? Básicamente por lo siguiente:

a. *Respecto a la confidencialidad*. La ley tiene como principio básico la "publicidad"; este es descrito en el artículo 3, en el cual se indica que "Toda información que posea el Estado se presume pública, salvo las excepciones expresamente previstas por el Artículo 15 de la presente Ley" (Ley 27806), es decir, la ley nos propone y manda una clasificación de la información; esto en la práctica significa otorgar las autorizaciones que correspondan según la información, lo que nos lleva a decir que se cumple con la confidencialidad.

b. *Respecto a la disponibilidad*. La ley y su reglamento exigen que las entidades cumplan los plazos establecidos para poder entregar la información, ya sea a los entes gubernamentales que correspondan o a los ciudadanos que hacen uso de su derecho al acceso a la información, por lo cual dicha información debe estar "disponible" en tiempo y forma para quien lo requiera.

c. *Respecto a la integridad.* En el reglamento de la ley (Decreto Supremo 072-2003-PCM) en el artículo 6, inciso d, se pone de manifiesto que la entidad debe garantizar la autenticidad de la información que entrega, de esta manera se garantiza la "integridad" de la misma.

11. ¿LA SEGURIDAD DE LA INFORMACIÓN ES SOLO DIGITAL?

Actualmente, debido a la adopción de la tecnología en la vida diaria y por su crecimiento acelerado, la información ha encontrado en este medio un nuevo espacio donde desarrollar su ciclo de vida. Este medio da lugar a un nuevo ecosistema que es el "ciberespacio" y que, según la norma ISO/IEC 27032, "es un entorno complejo resultante de la interacción de personas, *software* y servicios en internet por medio de dispositivos tecnológicos y redes conectadas a dichos dispositivos, y el cual no existe de una forma física". Entonces, surge la siguiente pregunta: ¿la seguridad de la información es solo para los medios tecnológicos? La respuesta es no; como se ha mencionado antes, la seguridad de la información sirve para proteger toda la información, es decir, en todas sus formas, representaciones y contenedores donde es procesada y almacenada. Pero, teniendo en cuenta el concepto de ciberespacio, se puede determinar que hay dos clases macro de información: la física y la digital (Alegsa, 2018), donde la principal diferencia entre ambas es la representación y medio donde se desarrolla; por ejemplo, un texto en un libro es una información en forma física, un texto en una computadora es una información en forma digital, ya que esta está representada y almacenada en un sistema binario. Es en este sentido que se hizo necesario generar una materia especializada, derivada y relacionada estrechamente con la seguridad de la información, mas no dependiente para su implementación como tal; sino que se enfoque en este entorno, lo que a partir de ahora llamaremos "ciberseguridad", que no es más que —según la norma ISO/IEC 27032— la preservación en el ciberespacio de los principios de confidencialidad, integridad y disponibilidad.

En el Perú, basados en la información recabada por la ENRIAP, se tiene que en las preguntas acerca de la implementación de políticas, controles, entre otros aspectos relacionados a la ciberseguridad, en promedio 217 entidades han dado una respuesta afirmativa, lo que se puede entender como que el 49 % de entidades públicas que contestaron a la ENRIAP cumple con lo dispuesto por la normativa o buenas prácticas, ya sea de manera completa o de forma parcial. Y respecto al número total de entidades públicas solo representa al 7 %.

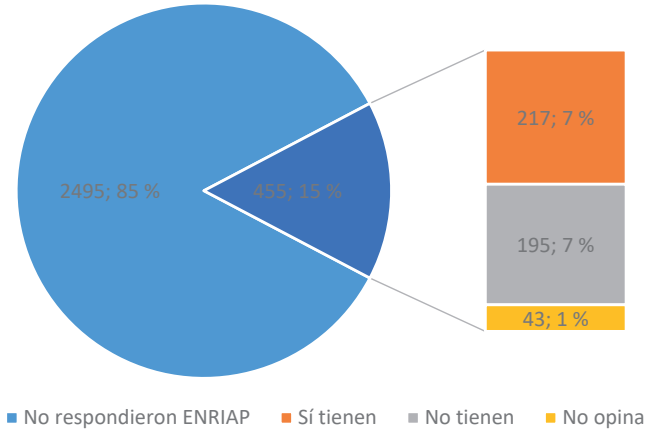

Figura 9. Cantidad de entidades públicas, respecto del total, que tienen políticas, controles y otros aspectos relacionados con la ciberseguridad
Elaboración propia

12. CONCLUSIONES

Con base en lo expuesto en los párrafos precedentes, podemos llegar a ciertas conclusiones en referencia a cómo se trata la seguridad de la información en la administración pública:

En primer lugar, la información generada en el ámbito público adquiere un matiz único, ya que este es producto de la administración y transformación de otra información que tiene un efecto directo en la ciudadanía. Por tanto, esta última no puede ser privada del acceso a esta información, a no ser que se tenga un argumento específico en el cual el interés sobre el ocultamiento de esa información sea mayor al interés del acceso a ella.

En segundo lugar, se puede sostener que el Estado es responsable desde sus diversos frentes de proteger la información asegurando la confidencialidad, integridad y disponibilidad, teniendo siempre presentes los principios del derecho de acceso a ella por parte de los ciudadanos.

En tercer lugar, es importante resaltar que el Estado se encuentra en una situación preocupante en lo que respecta a la implementación de sus sistemas de gestión de seguridad de la información, ya que, aproximadamente, solo el 6 % de organismos públicos ha cumplido con implementar lo dispuesto por la normativa vigente en referencia a este tema. Sin embargo, se debe tener en cuenta que ya se tienen las bases para poder cambiar esta situación teniendo en cuenta que el cumplimiento de la Ley de Transparencia ya hizo el trabajo de armar la estructura inicial del sistema en mención. Se hace patente también que el Estado requiere redoblar los esfuerzos para proteger su información, ya que los nuevos escenarios referentes a la tecnología, a la información y a la interacción entre Estado y ciudadanía así lo requieren.

En cuarto lugar, se debe mencionar que es tarea del Estado en su conjunto poder hacer el uso debido de las herramientas y recursos de diagnóstico como la ENRIAP; de esta manera, se podría y se debería tener una mejor imagen de la situación actual respecto a la seguridad de la información para luego establecer de manera más acertada las pautas y el camino a seguir con el objetivo de lograr cambios significativos en la protección de la información pública en beneficio de la población en general. Esto porque con solo la información del 15 % de entidades del Estado no se pueden realizar diagnósticos o análisis que se acerquen al conocimiento de la situación actual.

Por último, pero no menos importante, se debe considerar que la seguridad de la información no es solo la "seguridad digital". Si bien en razón de la realidad pueden parecer lo mismo, es importante tener en cuenta que la segunda es parte de la primera, pero a su vez no es dependiente de esta.

REFERENCIAS

Alegsa, L. (2018). *Definición de información digital.* http://www.alegsa.com.ar/Dic/informacion_digital.php

Autoridad Nacional del Servicio Civil (2016). *Características del Servicio Civil Peruano.* https://storage.servir.gob.pe/biblioteca/SERVIR-El_servicio_civil_peruano-Anx1.PDF

BCRP (2020). *Organismos públicos*. https://www.bcrp.gob.pe/sitios-de-interes/organismos-publicos.html

Castro, J. (2013). *Definición de Ley*. https://inoponible.cl/definicion-de-ley/

Cleveland, H. (1986). Government is Information (but Not Vice Versa). *Public Administration Review*, *46*, 605-607.

Correa, P. (2010). *La estructura del Estado peruano*. http://files.uladech.edu.pe/docente/06507071/CONSTITUCIONAL_ESPECIAL/SESION_06/LECTURA%20CENTRAL%2006.pdf.pdf

Decreto Legislativo 1412. [Presidencia del Consejo de Ministros]. Decreto Legislativo que aprueba la Ley de Gobierno Digital. 13 de septiembre del 2018. https://www.gob.pe/institucion/pcm/normas-legales/289706-1412

Decreto de Urgencia 006-2020. [Presidencia del Consejo de Ministros]. Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital. 8 de enero del 2020. https://busquedas.elperuano.pe/normaslegales/decreto-de-urgencia-que-crea-el-sistema-nacional-de-transfor-decreto-de-urgencia-n-006-2020-1844001-1/

Decreto Supremo 072-2003-PCM. [Presidencia del Consejo de Ministros]. Aprueban el Reglamento de la Ley de Transparencia y Acceso a la Información Pública. 7 de agosto del 2003. https://www.peru.gob.pe/normas/docs/DS-072-2003-PCM.pdf

Frayssinet M. (2016). *Taller de implementación de la norma ISO 27001*. https://www.slideshare.net/zerobar/si-semana11-iso27001v011

Instituto Nacional de Calidad. (2016). *¿Qué son las NTP?* https://www.inacal.gob.pe/principal/categoria/qslntp

Instituto Nacional de Estadística e Informática. (2018). *Perú: Número de Municipalidades y Población Total Proyectada al 30 de Junio, según Departamento, 2017*. https://www.inei.gob.pe/media/MenuRecursivo/publicaciones_digitales/Est/Lib1420/resumen.pdf

Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual. (2014). *Norma Técnica Peruana NTP-ISO/IEC 27001:2014*; 2.ª edición.

ISO. (2012). *ISO/IEC 27032:2012(en) Information technology — Security techniques — Guidelines for cybersecurity*. https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en

Ley 27806. [Ministerio de Economía y Finanzas]. Ley de Transparencia y Acceso a la Información Pública. 13 de julio del 2002. https://www.mef.gob.pe/es/normas-legales/298-portal-de-transparencia-economica/normas-legales/830-ley-nd-27806#:~:text=La%20presente%20Ley%20tiene%20por,la%20Constituci%C3%B3n%20Pol%C3%ADtica%20del%20Per%C3%BA

Martínez, C. (2010). El valor de la información, su administración y alcance en las organizaciones. *Revista Mexicana de Ciencias de la Información*, *1*(2), 10-20.

Mendel, T. (1999). *The Public's Right to Know: Principles on Freedom of Information Legislation*. Article 19.

Mogull, R. (2011). *Introducing the Data Security Lifecycle 2.0.* https://www.securosis.com/blog/introducing-the-data-security-lifecycle-2.0

Muñoz, A. (2001). Una aproximación a la información del sector público: la información de las administraciones públicas. *Revista General de Información y Documentación*, *11*(1), 33-47.

Novoa, Y. (2016). *El derecho de acceso a la información pública: contenido e importancia*. http://forseti.pe/revista/derecho-constitucional-y-derechos-humanos/articulo/el-derecho-de-acceso-a-la-informacion-publica-contenido-e-importancia

Oficina Nacional de Gobierno Electrónico e Informática. (2010). *Guía para elaborar la formulación y evaluación del plan operativo informático de las entidades de la administración pública para el año 2010.* http://spij.minjus.gob.pe/graficos/peru/2010/enero/05/RM-545-2009-PCM.pdf

Presidencia del Consejo de Ministros. (2013). *Autorizan ejecución de la "Encuesta Nacional de Recursos Informáticos en la Administración Pública (ENRIAP)"*. https://cdn.www.gob.pe/uploads/document/file/357258/RM_310-2013-PCM.pdf

Presidencia del Consejo de Ministros. (2017). Lista de entidades del Estado peruano. https://www.datosabiertos.gob.pe/dataset/lista-de-entidades-del-estado-peruano

Presidencia del Consejo de Ministros. (2020). Oficio N.° D000532-2020-PCM-OPII. Solicitud de información en el marco de la Ley N.° 27806, realizada por Kadú Josep Altamirano de la Borda.

Presidencia del Consejo de Ministros. (2020). Oficio N.° D000750-2020-PCM-OPII. Solicitud de información en el marco de la Ley 27806, realizada por Kadú Josep Altamirano de la Borda.

Presidencia del Consejo de Ministros. (2020). *Secretaría de Gobierno Digital*. https://www.gob.pe/7025-presidencia-del-consejo-de-ministros-secretaria-de-gobierno-digital/

Seclén Arana, J. A. (2016). *Factores que afectan la implementación del Sistema de Gestión de Seguridad de la Información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001*. Universidad Nacional Mayor de San Marcos.