POLÍTICA NACIONAL DE CIBERSEGURIDAD

Objetivo

Proteger la infraestructura de información, los datos e información del Estado y la tecnología utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Asegurar la implementación de las propuestas legislativas, y en general la normatividad relacionada con la seguridad de la información o ciberseguridad comprendida en esta Política, identificando los recursos involucrados y las partidas presupuestales correspondientes.

Mantener la Política Nacional de Ciberseguridad actualizada, a efectos de asegurar su vigencia y por ende su eficacia, promoviendo la participación de las entidades de sector público y privado, así como representantes de la sociedad civil y la academia.

I. Alcance

La presente Política se aplica a todas las entidades de la Administración Pública a que hace referencia el Artículo I del Título Preliminar de la Ley N° 27444, así como a todos sus recursos y procesos sean estos internos o externos.

II. Referencias Internacionales

La presente Política cuenta con los siguientes marcos de referencia:

- Resolución Ministerial N° 246-2007-PCM, que aprueba la Norma Técnica Peruana "NTP-ISO/ IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2a. Edición" en todas las entidades integrantes del Sistema Nacional de Informática, o la que haga sus veces.
- Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de 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 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática, o la que haga sus veces.
- Resolución Ministerial N° 166-2017-PCM, que modifica el artículo 5 de la R.M. N° 004-2016-PCM referente al Comité de Gestión de Seguridad de la Información.

III. Marco Normativo

- Constitución Política del Perú.
- Decreto Legislativo N° 604.
- Ley N° 29158: Ley Orgánica del Poder Ejecutivo.

- Ley Nº 27658: Ley Marco de Modernización de la Gestión del Estado.
- Ley Nº 27806: Ley Transparencia y Acceso a la Información Pública.
- Ley N° 27444: Ley de Procedimiento Administrativo General.
- Ley N° 27269: Ley de Firmas y Certificados Digitales.
- Ley N° 27291: Ley que modifica el código civil permitiendo la utilización de los medios electrónicos para la comunicación de la manifestación de voluntad y la utilización de la firma electrónica.
- Ley N° 28493: Ley que regula el uso del Correo Electrónico comercial no solicitado (SPAM).
- Ley N° 29733: Ley de Protección de Datos Personales.
- Ley N° 28530: Ley de Promoción de Acceso a Internet para personas con discapacidad y adecuación del espacio físico en cabinas públicas de internet.
- Ley N° 29904: Ley de Promoción de la Banda Ancha y Construcción de la Red Dorsal Nacional de Fibra Óptica.
- Ley N° 30096 y su modificatoria Ley 30171: Ley de Delitos Informáticos.
- Decreto Legislativo N° 1353, que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el régimen de protección de datos personales y la regulación de la gestión de intereses.
- Decreto Supremo N° 022-2017-PCM, que aprueba el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros.
- Decreto Supremo N° 066-2011-PCM: Aprueba el “Plan de Desarrollo de la Sociedad de la Información en el Perú – La Agenda Digital Peruana 2.0”.
- Decreto Supremo N° 004-2013-PCM: Aprueba la Política Nacional de Modernización de la Gestión Pública.
- Decreto Supremo N° 081-2013-PCM: Aprueba la Política Nacional de Gobierno Electrónico 2013-2017.
- Resolución Ministerial N° 179-2004-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana “NTP-ISO/IEC 12207:2004 Tecnología de la Información. "Procesos del Ciclo de Vida del Software, 1ª Edición” en entidades del Sistema Nacional de Informática.
- Resolución Ministerial N° 246-2007-PCM, que aprueba la Norma Técnica Peruana “NTP-ISO/ IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2a. Edición” en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución Ministerial N° 197-2011-PCM, que establece fecha límite para que diversas entidades de la Administración Pública implementen el plan de seguridad de la información dispuesto en la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de Buenas Prácticas para la Gestión de la Seguridad de la Información".
- Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de 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 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.

- Resolución Ministerial N° 166-2017-PCM, que modifica el artículo 5 de la R.M. N° 004-2016-PCM referente al Comité de Gestión de Seguridad de la Información.

IV. Términos y Definiciones

a) Seguridad de la Información

La seguridad de la información se entiende como la preservación de las siguientes características:

- *Confidencialidad*: Garantizar que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- *Integridad*: Salvaguardar la exactitud y totalidad de la información y los métodos de procesamiento.
- *Disponibilidad*: Garantizar que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, deben considerarse los conceptos de:

- *Autenticidad*: Asegurar que la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- *Auditabilidad*: Definir que todos los eventos de un sistema puedan ser registrados para su control posterior.
- *Protección a la duplicación*: Asegurar que una transacción sólo se realice una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
- *No repudio*: Evitar que una entidad que haya enviado o recibido información o intercambiado datos, alegue ante terceros que no los envió o no los recibió.
- *Legalidad*: Cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.
- *Confiabilidad de la Información*: Que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

A los efectos de una correcta interpretación de la presente Política, se realizan las siguientes definiciones:

- *Información*: Toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
- *Sistema de Información*: Conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

- *Tecnología de la Información*: Hardware y software operados por la entidad o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la entidad, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.
- *Propietario de la Información*: Persona responsable de la integridad, confidencialidad y disponibilidad de una cierta información.

b) Evaluación de Riesgos

Evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma; la probabilidad de que ocurran y su potencial impacto en la operatoria del Organismo.

c) Tratamiento de Riesgos

Proceso de selección e implementación de medidas para modificar el riesgo.

d) Gestión de Riesgos

Actividades coordinadas para dirigir y controlar una organización en lo que concierne al riesgo.

NOTA. La gestión de riesgos usualmente incluye la evaluación de riesgos, el tratamiento de riesgos, la aceptación de riesgos y la comunicación de riesgos.

e) Comité de Seguridad de la Información

Colegiado integrado por representantes de todas las áreas sustantivas de la entidad, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

f) Responsable de Seguridad de la Información

Persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes de la entidad que así lo requieran.

g) Incidente de Seguridad

Evento adverso en un sistema de computadoras, o red de computadoras, que puede comprometer o compromete la confidencialidad, integridad y/o disponibilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de quebrar los mecanismos de seguridad existentes.

h) Riesgo

Combinación de la probabilidad de ocurrencia de un evento y sus consecuencias o impacto.

i) Amenaza

Causa potencial de un incidente no deseado, el cual puede ocasionar daños a un sistema u organización.

j) Vulnerabilidad

Debilidad de un activo o grupo de activos que puede ser aprovechada por una amenaza.

k) Control

Medio para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras organizacionales, las cuales pueden ser de naturaleza administrativa, técnica, de gestión, o legal.

V. Política Nacional de Ciberseguridad

1. ***Fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el de la ciberseguridad, creando un entorno y las condiciones necesarias que permitan brindar protección en el ciberespacio.***

   Para lograr este objetivo es necesario involucrar a todos los sectores y entidades del Estado con responsabilidad en el campo de ciberseguridad y ciberdefensa, creando un ambiente participativo en el que participen representantes del sector privado, sociedad y la academia, donde cada quien aporte y actúe a propósitos comunes, estrategias concertadas y esfuerzos coordinados. Asimismo, es de vital importancia crear conciencia y sensibilizar a la población respecto de la importancia de la seguridad de la información (ciberseguridad); así como, fortalecer los niveles de cooperación y colaboración internacional en aspectos de ciberseguridad y ciberdefensa; apoyar investigaciones relacionadas con ataques informáticos y proteger a la ciudadanía de las consecuencias de estos ataques.

2. ***Brindar capacitación especializada en seguridad de la información y ampliar las líneas de investigación en materia de ciberseguridad dentro de la Administración Pública.***

   Este objetivo permitirá generar y fortalecer las capacidades existentes en materia de seguridad cibernética, con el propósito de afrontar las amenazas que atentan contra los propósitos planteados.

   Inicialmente, se capacitará a los funcionarios y servidores que estén directamente involucrados en la atención y manejo de incidentes cibernéticos. Gradualmente se extenderá esta capacitación a las demás entidades del Estado. Entre los planes de capacitación, el Pe-CERT con el apoyo del Comité Interamericano Contra el Terrorismo (CICTE) de la OEA, entre otros, elaborará un Plan de Capacitación para los demás funcionarios y servidores del Estado, así como programas de sensibilización y concienciación para los ciudadanos en general. De la misma forma, el Ministerio del Interior (MININTER) buscará la implementación gradual de asignaturas en seguridad de la información, ciberseguridad y ciberdefensa (teórico-prácticas) en las escuelas de formación y de capacitación de oficiales y suboficiales.

3. ***Desarrollar un Plan de sensibilización y capacitación a todos los ciudadanos respecto a la Ciberseguridad.***

   Se busca que la sociedad civil tome consciencia sobre la ciber-seguridad, identificar posibles vulnerabilidades o amenazas y tomar acciones oportunas para su seguridad.

   El Plan contará con una Estrategia de difusión que incluya la organización de conferencias para instituciones educativas (de nivel primario a universitario), y tareas de divulgación entre ciudadanos y otras entidades públicas y privadas del país.

   Así mismo, se realizarán foros que permitan intercambiar opiniones y experiencias entre todas las entidades públicas y privadas, sociedad civil y academia, con el objeto de compartir las mejores prácticas en Ciberseguridad y Ciberdefensa.

   Parte de la sensibilización en temas de Seguridad de la Información, radica en socializar la Normatividad vigente, como la Ley N° 27933 de Protección de Datos Personales, que ampara a todos los ciudadanos y la Ley N° 30096 modificada por la Ley N° 30171 – Ley de Delitos Informáticos, entre otros.

4. ***Fortalecer la legislación en materia de ciberseguridad, la cooperación internacional y propiciar la adhesión del Perú a los diferentes organismos internacionales en esta temática.***

   Este objetivo busca desarrollar las herramientas jurídicas necesarias para una efectiva y eficiente prevención, investigación y judicialización de los delitos informáticos.

   Así, se propenderá por la expedición de la normatividad necesaria para dar cumplimiento a los tratados internacionales sobre ciberseguridad, ciberdelincuencia, en la medida que hagan parte del bloque de constitucionalidad, así como por la debida reglamentación de lo dispuesto en la legislación nacional. Las entidades responsables de la ciberseguridad y ciberdefensa deberán buscar y evaluar la participación en diferentes redes y mecanismos internacionales de cooperación (Consejo de Europa, OEA y Forum Of Incident Response Security Teams - FIRST), que permitan preparar al país para afrontar los crecientes desafíos del entorno internacional en el área de ciber-seguridad, así como responder de una forma más eficiente a incidentes y delitos de seguridad cibernética.

   De manera especial el Perú deberá gestionar la adhesión al Convenio de Ciberdelincuencia suscrito en Budapest el 23 de noviembre del 2001, adhesión que permitirá combatir la ciber-delincuencia de manera coordinada y globalizada, lo cual a su vez, se orienta al cumplimiento del Compromiso al que se arribó en la Cumbre Mundial sobre Sociedad de la información en Túnez 2005, enmarcados dentro de los Objetivos de Desarrollo del Milenio, (ahora denominados Objetivos de Desarrollo Sostenible), que disponen incrementar la confianza y la seguridad en cuanto a la utilización de las Tecnologías de la Información y de la Comunicación (TIC), y a su vez, se encuentra dentro de los alcances de lo establecido en el Política Nacional de Gobierno Electrónico 2013-2017, aprobada mediante Decreto Supremo N° 081-2013-PCM , y en plena concordancia con la Ley de Delitos Informáticos aprobada mediante Ley N° 30096, modificada mediante Ley N° 30171.

5. ***Afianzar la integración y coordinación eficaz, entre las diversas Coordinadoras de Respuestas a Emergencias en Redes Teleinformáticas de la Administración Pública y el sector privado.***

   Según lo establecido en la Resolución Ministerial N° 360-2009-PCM, se hace necesario que cada Ministerio o la que haga sus veces, coordine con el Pe-CERT, para hacer cumplir sus objetivos.

   Es importante que dicha coordinación se realice permanentemente y que la misma tenga un carácter de prioridad ante cualquier amenaza que vulnere la seguridad de la Nación.

6. **Elaborar un Plan de Acción Nacional en Ciberseguridad**

   Este Plan deberá realizarse de forma multisectorial y multidisciplinaria, entre representantes de las entidades del sector público, sector privado, sociedad y la academia.

7. **Crear el Comité Nacional de Ciberseguridad**

   Este Comité tendrá como parte de sus funciones, el velar por el fiel cumplimiento de las políticas y lineamientos que se establezcan respecto a la Ciberseguridad.

   El Comité está conformado por las siguientes entidades:

   1. Presidencia del Consejo de Ministros a través de la Secretaría de Gobierno Digital (SEGDI)
   2. Poder Judicial
   3. Dirección Nacional de Inteligencia (DINI)
   4. Ministerio de Defensa (MINDEF)
   5. Ministerio del Interior (MININTER)
   6. Policía Nacional del Perú (PNP)
   7. Asociación de Gobiernos Regionales
   8. Sociedad Nacional de Industrias (SNI)
   9. Cámara de Comercio de Lima (CCL) (OBS)
   10. Cámara Nacional de Comercio, Producción, Turismo y Servicios – PERUCÁMARAS
   11. Colegio de Abogados de Lima (CAL)
   12. Colegio de Ingenieros del Perú (CIP)
   13. NAP (Network Access Point) Peru
   14. Confederación Nacional de Institucionales Empresariales Privadas (CONFIEP)
   15. Asociación de Bancos del Perú (ASBANC)
   16. Asociación para el Fomento de la Infraestructura Nacional (AFIN)
   17. Red Científica Peruana (RCP)
   18. Otros (Definir)