POLÍTICA DE SEGURIDAD DIGITAL

1. Introducción

Como efecto de los procesos de apertura de las instituciones, entidades y propias dinámicas globales y globalizantes hacia el uso de las herramientas y tecnologías digitales y de transmisión de datos e información, se hace indispensable por parte de las entidades e instituciones gubernamentales principalmente la adopción de esquemas y políticas que disminuyan la incertidumbre y riesgo asociado a las amenazas que suponen el mundo digital y cibernético con miras a garantizar la integridad de los ciudadanos y sus organizaciones posiblemente afectados por ataques y filtraciones cada vez más constantes en el mundo tal y como lo han evidenciado en eventos como el de los Panamá Papers, Watergate, Wikileaks y otros múltiples de organizaciones como la de Anonymous a nivel mundial que aumentan la incertidumbre y riesgo frente a la seguridad digital de manera permanente.

Es ante ello que, la Política de seguridad digital está enfocada a contrarrestar las amenazas cibernéticas, siendo la gestión del riesgo la parte fundamental de esta política, la seguridad digital por ser la información el activo más importante de la organización, es necesario protegerla frente a los posibles riesgos derivados del uso de las nuevas tecnologías, por lo que el INDERBUENAVENTURA en cumplimiento pleno de su objetivo misional de

> "Generar y brindar a la comunidad oportunidades de participación en procesos de iniciación, formación, fomento y práctica del deporte, la recreación y el aprovechamiento del tiempo libre, la Educación Física y la Educación extraescolar como contribución al desarrollo integral del individuo y la integración comunitaria, para el mejoramiento de la calidad de vida de los habitantes del Distrito de Buenaventura en sus áreas urbana y rural."

En el marco del Modelo Integrado de Planeación y Gestión -MIPG- por medio de esta política realizara actividades de mitigación y eliminación de cualquier tipo de riesgo digital que pueda afectar la confianza de los ciudadanos digitales y la calidad de datos que se gestionan por ambas partes, encaminando todas las acciones en materia de seguridad digital para contrarrestar cualquier amenaza cibernética y mitigue todo tipo de riesgo, teniendo presente directrices y recomendaciones en el CONPES 3854 de Seguridad Digital, adicionando aspectos del Decreto Nacional 1078 de 2015 y del Modelo de Privacidad de la Información (MSPI) expedido por el MinTIC.

2. Objetivos y alcance

2.1. Objetivos

Objetivo general:

Diseñar el marco de política institucional orientada a la identificación, gestión y mitigación de riesgos de seguridad digital para la generación de confianza de los ciudadanos digitales del Instituto.

Objetivos Específicos:

- Establecer lineamientos para una correcta gestión del riesgo de seguridad digital en actividades propias de la entidad.
- Capacitar a los funcionarios del INDERBUENAVENTURA en buenas prácticas digitales.
- Desarrollar confianza digital a través de la mejora de la seguridad digital en la entidad.
- Fortalecer la capacidad del INDERBUENAVENTURA en materia de prevención de riesgos digitales.

2.2. Alcance

La política e Seguridad digital del INDERBUENAVENTURA busca garantizar que la entidad identifique el peligro de los riesgos de su entorno digital y tenga un empoderamiento de la aplicación de ciberseguridad con el fin de desarrollar nuevas capacidades frente a sistemas de seguridad digital que permiten un manejo confiable y seguro de la información de la entidad.

3. Principios

La Política nacional de gobierno digital recomienda que se debe tener en cuenta dos tipos de principios que son: generales y operativos. Los principios generales están dirigidos a las múltiples partes interesadas quienes, directa o indirectamente, desarrollan algunas o todas sus actividades socioeconómicas en el entorno digital. Los principios operativos están dirigidos a los líderes o tomadores de decisiones, quienes por su alto nivel en las organizaciones deben enfocar sus acciones hacia la adopción del marco general de gestión del riesgo de seguridad digital.

3.1. Principios generales:

- *Conocimiento, capacidades y empoderamiento:* Las múltiples partes interesadas deben entender los riesgos de seguridad digital. Deben ser

conscientes de que el riesgo de seguridad digital puede afectar el logro de sus objetivos económicos y sociales, y el de otros. Deben estar educados al respecto, poseer las habilidades necesarias para entender el riesgo, administrarlo y evaluar su impacto.

- *Responsabilidad:* Las múltiples partes interesadas deben asumir la responsabilidad de la gestión del riesgo de seguridad digital. Deben rendir cuentas sobre la base de sus funciones y su capacidad para actuar, teniendo en cuenta el posible impacto de sus decisiones sobre los demás. Deben también reconocer que un cierto nivel de riesgo de seguridad digital tiene que ser aceptado para lograr los objetivos económicos y sociales.

- *Derechos humanos y valores fundamentales:* Las múltiples partes interesadas deben gestionar los riesgos de seguridad digital de manera transparente y compatible con los derechos humanos y los valores fundamentales. La implementación de la gestión de riesgos de seguridad digital debe ser compatible con la libertad de expresión, el libre flujo de la información, la confidencialidad de la información, la protección de la privacidad y los datos personales. Las organizaciones deben tener una política general de transparencia acerca de sus prácticas y procedimientos para la gestión de riesgos de seguridad digital.

- *Cooperación:* Las múltiples partes interesadas deben cooperar, incluso más allá de sus fronteras, a nivel regional e internacional.

- *Gobernanza de la seguridad digital:* Articulación y armonización de las múltiples partes interesadas, bajo un marco institucional adecuado, con el fin de gestionar la seguridad digital, bajo el liderazgo del Gobierno nacional.

3.2. *Principios operativos:*

- *Evaluación de riesgos y ciclo de tratamiento:* La evaluación de riesgos debe llevarse a cabo de manera sistemática y continua, evaluando las posibles consecuencias de las amenazas y las vulnerabilidades digitales en las actividades económicas y sociales en juego. El tratamiento del riesgo debería tener como objetivo reducir el riesgo a un nivel aceptable en relación con los beneficios económicos y sociales.

- *Medidas de seguridad:* Los líderes y tomadores de decisiones deben asegurarse de que las medidas de seguridad sean apropiadas y proporcionales al riesgo, y

deben tener en cuenta su potencial impacto, negativo o positivo, sobre las actividades económicas y sociales que tienen por objeto proteger. La evaluación de riesgos de seguridad digital debe guiar la selección, operación y mejora de las medidas de seguridad para reducir el riesgo a niveles aceptables Innovación: los líderes y tomadores de decisiones deben asegurarse de que la innovación sea considerada como parte integral de la reducción del riesgo de seguridad digital. Esta debe fomentarse tanto en el diseño y funcionamiento de la economía, y de las actividades sociales basadas en el entorno digital, como en el diseño y el desarrollo de las medidas de seguridad.

- *Preparación y continuidad:* con el fin de reducir los efectos adversos de los incidentes de seguridad, y apoyar la continuidad y la capacidad de recuperación de las actividades económicas y sociales, deben adoptarse preparaciones y planes de continuidad. El plan debe identificar las medidas para prevenir, detectar, responder y recuperarse de los incidentes y proporcionar mecanismos claros de escalamiento.

4. Glosario

La mayoría de las definiciones se toman de la Política Nacional de Confianza y Seguridad Digital – CONPES 3995.

- **Activo de Información:** Es todo aquello que en la entidad es considerado importante o de alta validez para la misma ya que puede contener información importante como son en las Bases de Datos con usuarios, contraseñas, números de cuentas, etc.
- **Amenaza:** Posible violación de la seguridad digital que tiene el potencial de ocurrir total o parcialmente en el entorno digital. Se caracteriza por la aparición de una situación donde uno o más actores (externos o internos) adelantan una o varias acciones con la capacidad de alterar una infraestructura física, un sistema de información o la integridad de la información en sí.
- **Ataque:** amenaza intencional que se concreta.
- **Confidencialidad:** La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Ciberdefensa:** Capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales. La ciberdefensa implica el empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética.

- **Ciberdelincuencia:** Conjunto de acciones y actividades ilícitas que son cometidas total o parcialmente en el entorno digital, asociadas con el uso de las Tecnologías de la Información y las Comunicaciones o la utilización de un bien o servicio informático con el fin de causar daño, generar problemas o adelantar una agresión cibernética con el objetivo del propio beneficio o para desestabilizar la población, el territorio y la organización política del Estado.
- **Ciberdelito / Delito cibernético:** Actividad delictiva o abusiva relacionada con los ordenadores y las redes de comunicaciones, bien porque se utilice el ordenador como herramienta del delito, bien porque sea el sistema informático (o sus datos) el objetivo del delito. (Ministerio de Defensa de Colombia)
- **Ciberespacio:** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
- **Ciberseguridad:** Se entiende como la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética, buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio de las interacciones digitales. La ciberseguridad tiene el fin de proteger a los usuarios y los activos de Estado en el Ciberespacio y comprende el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para dicho fin.
- **Dato:** Es una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.
- **Disponibilidad:** Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
- **Entorno digital:** Ambiente, tanto físico como virtual sobre el cual se soportan las interacciones del futuro digital, tales como la economía digital.
- **Incidente:** Cualquier evento adverso real o sospechado, intencionado o no intencionado, que puede cambiar el curso esperado de una actividad en el entorno digital.
- **Información:** Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.
- **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

- **Riesgo:** Es el efecto de incertidumbres sobre objetivos y puede resultar de eventos en donde las amenazas cibernéticas se combinan con vulnerabilidades generando consecuencias económicas.
- **Riesgo informático:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. (ISO Guía 73:2002)
- **Seguridad digital:** Es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante la gestión del riesgo de seguridad digital; la implementación efectiva de medidas de ciberseguridad; y el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país.
- **Vulnerabilidad:** Es una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada, los servicios y recursos que la soportan.

5. Marco normativo

- Ley 1150 de 2007
- Ley 1341 de 2009
- Ley 1273 de 2009
- Ley 1474 de 2011
- Ley 1581 de 2012
- Ley 1712 de 2014
- Ley 2052 de 2020
- Resolución 3564 de 2015
- Resolución 2710 de 2017
- Resolución 1519 del 2020
- Resolución 1126 de 2021
- Directiva No. 02 de abril de 2019 Decreto 612 del 4 de abril de 2018
- Decreto 1413 de 2017
- Decreto 2693 de 2012
- Decreto 212 de 2014
- Decreto 1078 de 2015
- Decreto 612 de 2018
- Decreto 2106 de 2019
- Decreto 620 de 2020
- Decreto 1692 de 2020
- Acuerdo 03 de 2015 del AGN CONPES 3995

6. Institucionalidad

Es obligatorio de las entidades del Estado de orden territorial dar cumplimiento a la normatividad que expida el gobierno nacional a través del Ministerio de Tecnologías de la Información y las Comunicaciones MTIC mediante la Política Nacional de Seguridad digital sus decretos y demás normas reglamentarias, y su articulación con el MIPG.

De otro lado, en el Comité Institucional de Gestión y Desempeño se debe articular los esfuerzos, recursos, metodologías y estrategias para asegurar la implementación de la política. Para ello, se debe designar un responsable de Seguridad Digital que también es el responsable de la Seguridad de la Información en la entidad, el cual debe pertenecer a un área que haga parte de la Alta Dirección.

En el orden territorial, MinTIC definirá los lineamientos para que las entidades territoriales definan la figura del enlace territorial para la implementación de la política de Seguridad Digital, así como las instancias respectivas para la articulación con el Coordinador Nacional de Seguridad Digital.

7. Marco Estratégico de la Política

7.1. Plan de Acción.

Para el INDERBUENAVENTURA, se define plan de acción con base al autodiagnóstico de la Política de Seguridad digital para dar cumplimiento con el fin de que la entidad cuente con una buena gestión y desempeño frente a la implementación de la Política.

El Plan de acción forma parte integral de la presente política y se encuentra en la oficina de la secretaria general.

7.2. Seguimiento y evaluación

En primera instancia el Ministerio de Tecnologías de la Información y las Comunicaciones definirá el procedimiento para el seguimiento y evaluación de la Política de seguridad digital en el marco de los lineamientos nacionales

El Área de control interno del INDERBUENAVENTURA o quien haga sus veces será la responsable de realizar seguimiento y evaluación a la Política de seguridad digital de acuerdo al plan de acción definido y aprobado.