POLÍTICA DE SEGURIDAD DIGITAL

EMPRESA INMOBILIARIA Y DE SERVICIOS LOGÍSTICOS DE CUNDINAMARCA

DIRECCIÓN TÉCNICA Y DE PROYECCTOS

INTRODUCCIÓN

La seguridad digital actualmente en un activo muy importante para el entorno de desarrollo a nivel mundial, debido a que el flujo constante de generación de información por medios digitales crece rápidamente, y más ahora con la atención puesta al manejo virtual de todos los procesos que se realizan en las entidades, medios empresariales, instituciones académicas y demás instituciones con las medidas contra el Covid-19.

Adicionalmente el continuo crecimiento y desarrollo de las actividades económicas que se visualizan en las entidades públicas, desarrolla incertidumbres y riesgos inherentes para los bienes tecnológicos por la seguridad digital, los cuales se deben afrontar y minimizar de manera adecuada, de lo contrario se podrían presentar riesgos materializados en amenazas o ataques cibernéticos, lo que afectaría la estructura económica, funcional, social, cultural a nivel nacional, departamental o municipal.

Con base en lo anterior, es que la Política de Seguridad Digital de la Empresa Inmobiliaria y de Servicios Logísticos de Cundinamarca, busca establecer unos lineamientos, políticas, reglas y demás mecanismos para asegurar la integridad, disponibilidad, confidencialidad y seguridad de todos los activos de información que se encuentran operativos tanto a nivel interno como externo de la entidad.

JUSTIFICACIÓN

Las entidades gubernamentales deben garantizar que el manejo y adecuado uso de los activos de información que reposan en sus infraestructuras, tengan todas las garantías de seguridad necesaria para salvaguardar toda la información pública que reposan en su custodia, de tal forma que se disminuyan las posibilidades de vulnerabilidades que puedan generar los delitos informáticos a los que diariamente se encuentran expuestos las infraestructuras tecnológicas que se integran a la red de internet. De esta manera se evita el uso indebido de la información, interceptación, robo o suplantación de identidad, secuestro entre otros delitos que se pueden presentar, haciendo uso y adecuada implementación de las políticas y normativas necesarias para disminuir estos hechos delictivos.

Es de vital importancia que se estructuren lineamientos para la implementación y adopción de la Política de Seguridad Digital de la Empresa Inmobiliaria y de Servicios Logísticos de Cundinamarca, con el fin de garantizar el adecuado funcionamiento y continuidad de las actividades que se desarrollan en la entidad, y de esta forma tener una atención adecuada a la ciudadanía.

OBJETIVO

Estructurar los lineamientos, políticas, procesos y procedimientos necesarios para garantizar la seguridad en los activos de información y sus herramientas tecnológicas operativas que se tienen en la entidad.

OBJETIVOS ESTRATEGICOS

- Generar pautas para la prestación de servicios a la comunidad de forma continua e interrumpida en la Empresa Inmobiliaria y de Servicios Logísticos de Cundinamarca.
- Fomentar el uso y apropiación de la Política de Seguridad vigente en los funcionarios y contratistas de la Empresa Inmobiliaria y de Servicios Logísticos de Cundinamarca.
- Reducir las brechas de seguridad, de forma ordenada y guiada por los parámetros dictaminados desde el Ministerio de las Tics.
- Proteger los recursos de información de la Empresa Inmobiliaria y de Servicios Logísticos de Cundinamarca y la tecnología utilizada para su operación, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.
- Establecer políticas que mejoren los servicios prestados mediante tecnologías de la información a las dependencias dentro de la entidad, procurando la mejora continua y optimización de los procesos.
- Fomentar la confianza necesaria para el entorno digital, estableciendo mecanismos de participación activa y permanente los cuales permitan promover en las diferentes dependencias comportamientos responsables en el entorno digital.
- Capacitar al personal de la Empresa Inmobiliaria y de Servicios Logísticos de Cundinamarca en buenas prácticas digitales y de seguridad.

ALCANCE

Suministrar procesos seguros, herramientas que respalden el funcionamiento de las actividades cotidianas, generando confiabilidad tanto a nivel interno como externo de los niveles de seguridad pertinentes, lo cual se vea reflejado en el buen funcionamiento y su oportuna solución de requerimientos de directivos, funcionarios, ciudadanos y entidades que lo requieran.

Lo anterior bajo el marco de la modalidad y excepciones que se han implementado para el trabajo presencial y virtual, en pro de dar continuidad a las actividades frenadas por la pandemia mundial del Covid-19. Ya que en pro de lo anterior, se ha requerido la implementación de procesos y procedimientos soportados en gestión de TI, lo que implica que se deben garantizar las medidas correspondientes para velar por la funcionabilidad y seguridad de todos los procesos.

VIGENCIA

Una vez se tenga aprobación por parte de la Junta Directiva de Copropietarios de la Empresa Inmobiliaria y de Servicios Logísticos de Cundinamarca, se procederá a realizar el acto administrativo que ordene su implementación y cumplimiento por la entidad para la vigencia 2021-2023.

RESPONSABLE

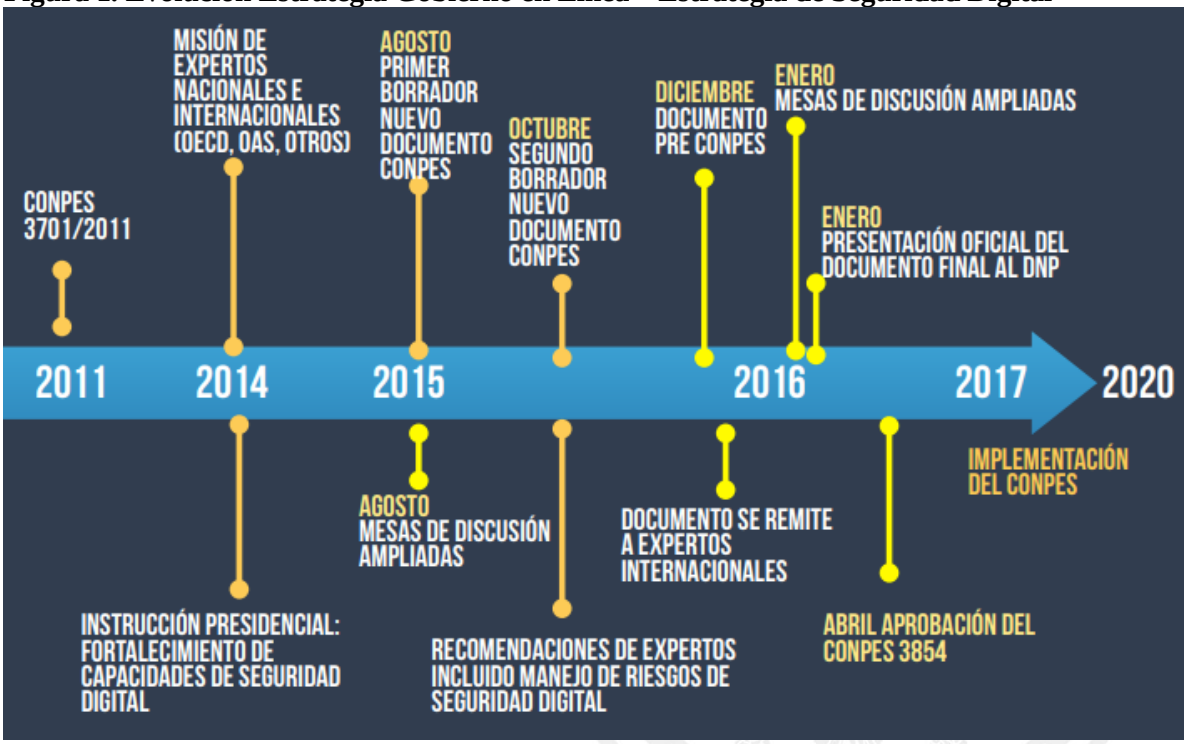
Para la implementación, seguimiento, control y actualización de la política estará como responsable la Dirección Técnica y de Proyectos con el apoyo del área de Tics, todo bajo el acompañamiento de la Gerencia General, los cuales deberán garantizar el adecuado desarrollo integral, teniendo en cuenta que el área de tics es un proceso transversal y de apoyo para toda la entidad.

MARCO LEGAL

- Constitución Política Nacional - art. 15.
- Decreto 1499 de 2017
- Decreto 2609 de 2012
- Decreto 2693 de 2012
- Decreto no. 44 del 19 diciembre de 2018
- ISO 27002:2005
- ISO/iec 27001:2005
- Ley 1266 de 2008
- Ley 1273 de 2009
- Ley 1341 de 2009
- Ley 1453 de 2011
- Ley 1480 de 2011
- Ley 527 de 1999
- Ley 599 de 2000
- Ley 679 de 2001
- NTC 27001:2006

A continuación, se muestra la línea de tiempo de la estrategia de orden nacional por el Ministerio de Tecnologías de la Información y Comunicaciones.

Figura 1. Evolución Estrategia Gobierno en Línea – Estrategia de Seguridad Digital



Fuente: Manual de Gobierno Digital – Recuperado de https://www.mintic.gov.co/portal/604/articles-15570_recurso_2.pdf

DEFINICIÓN Y ACRÓNIMOS

- **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**: Es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque en el equipo
- **Confidencialidad**: La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Copias de respaldo**: Es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.
- **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.
- **Gestión de riesgos de seguridad digital**: es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones, para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego.
- **Integridad**: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **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. • MSPI: Modelo de Seguridad y Privacidad de la Información.
- **Resiliencia**: es la capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido. (Documento CONPES 3854).
- **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.
- **Riesgo**: Es la posibilidad de que una amenaza se produzca, dando lugar a un ataque al equipo. Esto no es otra cosa que la probabilidad de que ocurra el ataque por parte de la amenaza.
- **Riesgo de seguridad digital**: es la expresión usada para describir una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital. Este riesgo puede resultar de la combinación de amenazas y vulnerabilidades en el ambiente digital.
- **Servidor**: Es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.
- **Vulnerabilidad**: Es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.

DIAGNOSTICO

De acuerdo al diligenciamiento del formato de Autodiagnóstico del modelo integrado de planeación y gestión (MIPG), el porcentaje de cumplimiento del Furag para la dimensión del modelo de Gestión con Valores para el Resultado, el cual integra las políticas entre las cuales se encuentra la Política Seguridad Digital (transformación estrategia Gobierno en Línea), se tiene un cumplimiento del 66.6% teniendo como máximo grupo par un porcentaje del 80.97%, lo que indica un avance continuo para dar cumplimiento a las lineamientos de orden nacional y departamental, pero dejando claridad de las acciones de mejora continua que se deben adoptar para incrementar el índice de cumplimiento.

LINEAMIENTOS GENERALES DE LA POLÍTICA

- La Empresa Inmobiliaria y de Servicios Logísticos de Cundinamarca, asignara responsabilidades frente a la seguridad de la información que serán definidas, compartidas, publicadas y aceptadas por cada uno de los proveedores, socios de la Entidad o terceros.
- La Empresa Inmobiliaria y de Servicios Logísticos de Cundinamarca, deberá garantizar que la seguridad que se encuentra en funcionamiento sea un activo primordial del ciclo de vida de los sistemas de información.
- La Empresa Inmobiliaria y de Servicios Logísticos de Cundinamarca, deberá establecer lineamientos que permitan garantizar la integridad de la información histórica, generada o adquirida, transmitida o resguardada en los procesos que se desarrollan en la entidad, con el objetivo de disminuir los daños que se puedan materializar de aspectos financieros, operativos, legales o procedimentales a razón de las amenazas que se tienen en la red.
- La Empresa Inmobiliaria y de Servicios Logísticos de Cundinamarca, deberá garantizar el adecuado análisis de información procedente de fuentes externas a la entidad, con el fin de disminuir los riesgos de afectaciones a la infraestructura de TI o información, haciendo uso de herramientas de análisis e identificación de amenazas (virus).
- Todo usuario de los recursos TIC, NO debe visitar sitios restringidos de manera explícita o implícita, o sitios que afecten la productividad de la Institución; como el acceso desde la Entidad a sitios relacionados con la pornografía, juegos, redes sociales no autorizadas, etc.
- Se deberá garantizar que los funcionarios que integran la planta de personal de la entidad, disminuyan el uso constante de dispositivos extraíbles para compartir archivos u información, con el fin de proteger la integridad de la información, lo anterior garantizando espacios colaborativos con las plataformas de tecnología que cuenta la entidad
- Todo usuario de los recursos TIC debe advertir e informar a la Dirección Técnica y de Proyectos y/o quien haga sus veces, de las restricciones específicas de protección para evitar el acceso a personal no autorizado, haciendo uso de los elemento de identificación, accesos con lectoras de proximidad y demás protocolos establecidos para este proceso.

POLÍTICAS DE SEGURIDAD DIGITAL

La Empresa inmobiliaria y de Servicios Logísticos de Cundinamarca, adopta como política de seguridad digital la administración de riesgos de seguridad y privacidad de la información, frente al control, implementación, monitoreo, lineamientos y demás procedimientos que proporcionan la integridad, disponibilidad y confidencialidad de toda la infraestructura de información y sus activos derivados.

Lo anterior con el fin de disminuir los impactos que se puedan generar y materializar sobre la infraestructura tecnológica de la entidad, de acuerdo a la matriz de gestión de riesgos que se deberá estructurar, modificar, actualizar, monitorear y controlar desde el aspecto tecnológico.

Para dar cumplimiento a la política de seguridad digital la entidad ha definido los siguientes parámetros:

1. Se deberá generar espacios de capacitación para los líderes de los procesos, con el fin de generar cultura tecnológica para lograr establecer planeas, estrategias y en general documentación necesaria para el fortalecimiento de lineamientos dirigidos a la disminución de riesgos.
2. Establecer resoluciones, actos administrativos u ordenanzas dirigidas al entorno digital, con el fin de generar normatividad interna para el cumplimientos de lineamientos que disminuyan y fortalezcan la gestión de riesgos.
3. Realizar la alineación correspondiente al modelo de gestión que se tenga implementado por el Gobierno Nacional, con el fin de identificar, gestionar, establecer planes de acción y mitigación.
4. Definir un documento frente a las responsabilidades que se generan al momento de participar en la entidad en la modalidad de funcionario, contratista, proveedor o cualquier interacción que requiera uso de herramientas tecnológicas de la entidad, mediante el cual se dé el conocimiento y aceptación.
5. Asegurar el adecuado respaldo y seguridad de la información que se genere, procese, transfiere o resguarda la entidad, como resultante del desarrollo de las actividades cotidianas, en pro de minimizar impacto financieros, operativos o legales debido a la materialización de algún riesgo.
6. La Empresa Inmobiliaria y de Servicios Logísticos de Cundinamarca garantizará el manejo de los riesgos originados por el personal con el que cuente la entidad.
7. La Empresa Inmobiliaria y de Servicios Logísticos de Cundinamarca deberá establecer un plan de contingencia frente a la materialización de riesgos que se tengan identificados.
8. Establecer parámetros para el uso de contraseñas, tanto para equipos, unidades de red, herramientas de Ti y demás sistemas que requieran autenticación personal.
9. Se deberá proteger la infraestructura de TI, realizando la restricción necesaria de navegación a los activos que tenga comunicación de red.
10. Los usuarios no deben modificar las configuraciones de seguridad de los dispositivos u aplicativos de gestión de TI bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.
11. Los usuarios deben evitar la instalación de programas desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales o con autorización del personal responsable.
12. El área de tics, deberá analizar y aprobar los métodos de conexión remota a la plataforma tecnológica de la entidad.
13. La Empresa Inmobiliaria y de Servicios Logísticos de Cundinamarca, garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

OPORTUNIDADES DE MEJORA Y RECOMENDACIONES

Una vez desarrollada la metodología de estructuración de la política de seguridad digital, para luego ser adaptada y ajustada a la entidad, se identifica las siguientes oportunidades de mejora:

- Gestionar acompañamiento y/o asesoramiento tanto del orden nacional con MinTic, como a nivel departamental con la Secretaría de Tics de la Gobernación de Cundinamarca, para tratar temas relacionados para el fortalecimiento de los procesos y procedimientos de la gestión de TI frente a la seguridad de toda la infraestructura de TI.
- Dar continuidad con el adecuado desarrollo de las actividades plasmadas para generar el uso y apropiación necesaria, con el fin de fomentar posteriormente herramientas de apoyo organizacional que faciliten la generación de nuevas políticas de funcionamiento en la gestión de TI y tenga una importancia directa frente a la seguridad de estos.
- Continuar con la estructuración, actualización y modificación de los documentos, lineamientos, planes, procesos, procedimientos y demás información que fortalezca la institucional de los objetivos estratégicos definidos en la Política de Seguridad Digital y de la entidad.
- Fortalecer la infraestructura de TI en harás de garantizar los niveles aceptables de seguridad de la información y de procesos que se maneja en la entidad.

CONCLUSIONES

De acuerdo al desarrollo, complemento y análisis de los requerimientos fundamentales que se contemplan en la política de seguridad digital, se concluye lo que se plasma a continuación:

- Se evidencia una aceptación por parte de la entidad al definir el área de tics como un proceso de apoyo transversal a todas las dependencias de la entidad.
- Se debe seguir trabajando para el fortalecimiento de la entidad y sobre todo estructurar proyectos que fomenten la capacidad tecnológica de la empresa y así lograr una mejor respuesta ante las responsabilidades y la seguridad de los procesos.
- Generar una cultura tecnológica tanto en los funcionarios como en los ciudadanos que requieran a la entidad de acuerdo a los lineamientos de seguridad que se tenga implementados.
- Se debe realizar actualizaciones necesarias de acuerdo al desarrollo organizacional o por cambio gubernamentales de orden nacional o departamental.

Elaborado por:	**Nombre:** German Darío Landinez González **Cargo:** Contratista – Profesional Universitario
Revisado por:	**Nombre:** **Cargo:**
Aprobado por:	**Nombre:** **Cargo**