BENEFICENCIA
DE CUNDINAMARCA

Resolución No. 529

"Por medio de la cual se adopta la Política General de Seguridad y Privacidad de la Información, dando cumplimiento a los requerimientos dictados por el Ministerio de las Tecnologías de la Información y Comunicaciones"

EL GERENTE GENERAL DE LA BENEFICENCIA DE CUNDINAMARCA

En uso de las atribuciones constitucionales y legales en especial las conferidas en el CONPES 3650 del 15 de marzo de 2010, CONPES 3785 del 9 de diciembre de 2013, Ley 1341 de 2009, Decreto-ley 019 de 2012, Decreto 2573 de 2014, el decreto 1078 de 2015, ARTÍCULO 2.2.9.1.3.4. decreto ordenanzal 430 del 25 de septiembre del 2020.

CONSIDERANDO:

Que la Constitución Política, en su artículo 113 señala que los diferentes órganos del Estado tienen funciones separadas, pero colaboran armónicamente para la realización de sus funciones.

Que el documento CONPES 3650 del 15 de marzo de 2010 declara la importancia estructural la implementación de la Estrategia de Gobierno en Línea en Colombia y exhorta al ministerio de las comunicaciones, con el apoyo del Departamento Nacional de Planeación, a formular los lineamientos de política que contribuyan a la sostenibilidad de la Estrategia de Gobierno en Línea;

Que el documento CONPES 3785 del 9 de diciembre de 2013 enmarca los lineamientos de la Política Nacional de Eficiencia Administrativa al Servicio del Ciudadano y adopta el modelo de Gestión Publica Eficiente, dirigido a mejorar la calidad de la gestión, como la prestación de los servicios provistos por las entidades de la Administración Pública.

Que la ley 1341 de 2009 estableció el marco general del sector de las Tecnologías de la Información y las Comunicaciones, incorporando principios, conceptos y competencias sobre su organización y desarrollo e igualmente señalo que las tecnologías de la información y comunicaciones deben servir al interés general y, por tanto, es deber del estado promover su acceso eficiente y la igualdad de oportunidades a todos los habitantes del territorio nacional;

Qué, asimismo, la anotada Ley determinó que es función del Estado intervenir en el sector de las TIC con el fin de promover condiciones de seguridad del servicio al usuario final, incentivar acciones preventivas y de seguridad informática y de redes para el desarrollo de dicho sector;

Que el Decreto-ley 019 de 2012, por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública, hace referencia al uso de medios electrónicos como elemento necesario en la optimización de los trámites ante la Administración Pública y establece en el articulo 4º que las autoridades deben incentivar el uso de las tecnologías de la información y las comunicaciones a efectos de que los procesos administrativos se adelanten con diligencia, dentro de los términos legales y sin dilaciones injustificadas;

Que, de igual manera, el articulo 38 del Decreto - Ley 019 de 2012 establece que la formulación de la política de racionalización de trámites estará a cargo del Departamento Administrativo de la Función Pública con el apoyo del Departamento Administrativo de la Presidencia de la República y del Ministerio de Tecnologías de la Información y las Comunicaciones;

Que el Decreto número 2482 de 2012, en su artículo 3º, establece los lineamientos generales para la integración de la planeación y la gestión e indica que para el desarrollo de las políticas de Desarrollo y Administrativo se deberá tener en cuenta la Estrategia de Gobierno en Línea que formula el Ministerio de Tecnologías de Información y Comunicaciones;

Que en el mismo decreto se contempla la Gestión de tecnologías de información y Comunicaciones, dentro. de la política de eficiencia administrativa;

Que Colombia aceptó las recomendaciones de la Organización para la Cooperación y el desarrollo Económico (OCDE) en Estrategias de Gobierno Digital, que insta a los gobiernos a adoptar enfoques más estratégicos para un uso de la tecnología que los impulse a ser más abiertos, participativos e innovadores, a través de acciones tales como el diseño de lineamientos para permitir, orientar y fomentar: el uso y reúso de la información pública, aumentar la apertura y la transparencia, incentivar la participación del público en la elaboración de políticas, proporcionar datos oficiales oportunos y confiables, y gestionar. los riesgos de uso indebido de datos, así como aumentar la disponibilidad de los datos en formatos abiertos; ·

Que Colombia suscribió la Alianza para el Gobierno Abierto declarando su compromiso de realizar acciones para el aprovechamiento de las tecnologías, facilitando mayor apertura en el gobierno, mejorando la prestación de los servicios y la participación ciudadana en los asuntos públicos, y promoviendo la innovación y la creación de comunidades más seguras con el propósito de que el gobierno sea más transparente, sensible, responsable y eficaz;

Que, con base en las consideraciones previamente expuestas, el Gobierno Nacional expidió el Decreto 2573 de 2014, "Por el cual se establecen lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones, compilado el decreto único reglamentario 1078 de 2015;

Que con base ARTÍCULO 2.2.9.1.3.4. del decreto 1078 de 2015, Responsable de liderar la implementación la Política de Gobierno Digital, el director, jefe de Oficina o Coordinador de Tecnologías y Sistemas de la Información y las Comunicaciones, o quien haga sus veces, de la respectiva entidad, tendrá la responsabilidad de liderar la implementación de la Política de Gobierno Digital. Las demás áreas de la respectiva entidad serán corresponsables de la implementación de la Política de Gobierno Digital en los temas de su competencia.

Que el director, jefe de Oficina o Coordinador de Tecnologías y Sistemas de la Información y las Comunicaciones, o quien haga sus veces, hará parte del Comité Institucional de Gestión y Desempeño y responderá directamente al representante legal de la entidad, de acuerdo a lo establecido en el artículo 2.2.3.5.4. del Decreto Único Reglamentario de Función Pública 1083 de 2015.

Que el artículo 2 Ibidem, estipula que las disposiciones de esa norma son de aplicación obligatoria para las entidades que conforman la Administración Pública en los términos del artículo 39 de la ley 489 de 1998 y los particulares que cumplen funciones administrativas;

Que el artículo 7 del Decreto 2573 de 2014, estipula que, el representante legal de cada sujeto obligado, será el responsable de coordinar, hacer seguimiento y verificación de la implementación y desarrollo de la Estrategia de Gobierno en Línea.

Que al definir el órgano interno responsable de orientar la implementación de la ·estrategia de Gobierno en Línea, el artículo 8 Ibidem, establece:

"Artículo 8º. responsable de orientar la implementación de la Estrategia de Gobierno en Línea. En las entidades del orden nacional y territorial, el Comité Institucional de Desarrollo Administrativo de que trata el artículo 6º del Decreto número 2482 de 2012 será la instancia orientadora de la implementación de la Estrategia de Gobierno en Línea al interior de cada entidad. Los sujetos obligados deberán incluir la estrategia de Gobierno en Línea de forma transversal dentro de sus planes estratégicos sectoriales e institucionales, y anualmente dentro de los planes de acción de acuerdo con el Modelo Integrado de Planeación y Gestión de qué trata el Decreto número 2482 de 2012 o las normas que lo modifiquen, adicionen o sustituyan. En estos documentos se deben definir las actividades, responsables, metas y recursos presupuestales que les permita dar cumplimiento a los lineamientos que se establecen.

En las entidades del orden territorial y demás sujetos obligados, la instancia orientadora de la implementación de la estrategia GEL será el consejo de Gobierno o quien haga sus veces. En caso que no existan estas instancias en el sujeto obligado, será la instancia o dependencia de mayor nivel jerárquico de la entidad.

En las materias relacionadas con tramites adelantados por medios electrónicos, la instancia orientadora deberá articularse con el Comité Anti tramites o con el responsable de esta materia al interior de los sujetos obligados.

Que el articulo 17 Numeral 17.5 del decreto ordenanzal 430 del 25 de septiembre de 2020 establece qué dentro de las funciones del gerente Qué son las funciones del gerente se encuentra la de expedir los actos administrativos para la adopción de los manuales de procedimientos, la implementación de los sistemas de MIPG, gestión de calidad y ambiental, el sistema de gestión en salud y seguridad en el trabajo y demás reglamentos administrativos de aplicación general.

En merito de lo expuesto,

RESUELVE:

ARTÍCULO PRIMERO - OBJETO. Adoptar en la Beneficencia de Cundinamarca la política general de seguridad de la información, en el marco de los lineamientos del Modelo Integrado de Planeación y Gestión – MIPG.

ARTICULO SEGUNDO - OBJETIVO GENERAL Establecer las reglas, lineamientos y principios para la gestión de la seguridad de los activos de información, con el fin de preservar la confidencialidad, integridad y disponibilidad durante todo el ciclo de vida de la información en la Beneficencia de Cundinamarca.

ARTICULO TERCERO - OBJETIVOS ESPECÍFICOS

- Gestionar y mantener la seguridad de la información que se gestiona y procesa dentro de la entidad y de los servicios y trámites dispuestos para los grupos de interés externos.
- Establecer, implementar y mantener la protección adecuada de los activos de información de la entidad.

- Asegurar que los funcionarios, contratistas, y empresas prestadoras de servicios en la entidad, conozcan sus responsabilidades y deberes, además que estén informados de las amenazas respecto a la seguridad de la información con el fin de reducir los riesgos de seguridad.
- Evitar el acceso no autorizado a los sistemas de información, servicios de información e infraestructura tecnológica de la entidad, así como el daño o interceptación no autorizada a la información de la entidad.
- Impedir pérdida, daño, robo o puesta en riesgo de los activos de información y la interrupción de las actividades de la entidad.
- Asegurar la operación correcta y segura de los servicios de almacenamiento y de procesamiento de la información.
- Establecer la inclusión de controles de seguridad en los sistemas de información desarrollados por la entidad o por terceros, o adquiridos.
- Dar directrices para contrarrestar las interrupciones en las actividades de la entidad y proteger los procesos más críticos en caso de fallas importantes de los sistemas de información o la infraestructura tecnológica y asegurar su recuperación oportuna.
- Definir los roles y perfiles dentro de la entidad para la gestión y seguridad de la información.

ARTICULO CUARTO - ALCANCE

- La política de seguridad y privacidad de la información aplica a todas las áreas y dependencias de la Beneficencia de Cundinamarca y la deben cumplir todos sus funcionarios, contratistas y terceros que presten algún servicio a la entidad.
- La política de seguridad y privacidad de la información estará alineada al marco de referencia de Arquitectura TI y a la Política de Gobierno Digital, así mismo contribuirá en el desarrollo del Plan Estratégico Institucional y del Plan Estratégico de Tecnologías de la Información y de las Comunicaciones.
- La política de seguridad y privacidad de la información estará alineada a la política de tratamiento de datos personales que defina la entidad, mas no da lineamientos en esta materia.
- La política de seguridad y privacidad de la información deberá estar articulada con la política de administración del riesgo, en lo relacionado con los riesgos de seguridad digital.
- De acuerdo a lo anterior, la información que genera y gestiona la Beneficencia de Cundinamarca constituye un activo estratégico clave para asegurar la continuidad del negocio, por lo que la Seguridad de la Información es una herramienta para garantizar su integridad, disponibilidad y confidencialidad.

ARTICULO QUINTO - DEFINICIONES

- **Activo**: Aquello que tenga valor para la organización. (Base de datos, sistemas de información, servicios, documentos, personas). Los activos los podemos separar en dos grandes grupos: tangibles e intangibles. Los activos tangibles son aquellos activos materiales que contienen información. Los activos intangibles son aquellos que soportan la información dentro de un activo material, y pueden inutilizar la información, pese a que el activo físico no haya sufrido daño alguno.
- **Activos de información:** es: "algo que una organización valora y por lo tanto debe proteger". Se puede considerar como un activo de información a: los datos creados o utilizados por un proceso de la organización en medio digital, en papel o en otros medios. Es importante precisar que el concepto de activos de información definido en la ley 1712 de 2014 es diferente al concepto que maneja el MSPI – ISO 27001.

- **Acuerdo de confidencialidad:** es el mecanismo mediante el cual regulamos los aspectos relativos a la seguridad de la información en una prestación de servicios, acorde a las funciones a desempeñar en la entidad.
- **Arquitectura empresarial:** es un marco conceptual que explica la estructuración y funcionamiento de una organización e incluye los siguientes elementos: Mapa de organización, Mapa de procesos de negocio, Mapa de sistemas, Mapa de Información
- **Backup de la información:** se refiere a la copia y archivo de datos de modo que se puede utilizar para restaurar la información original después de una eventual pérdida de datos.
- **Cadena de mensajes**: consiste en un mensaje que intenta inducir al receptor a realizar algún número de copias de este para luego pasarlos o propagarlos a nuevos receptores.
- **Centro de datos:** es la ubicación física donde se concentran los recursos necesarios de computación de una organización o proveedor de servicios.
- **Ciberataques**: es un intento de exponer, alterar, desestabilizar, destruir, eliminar para obtener acceso sin autorización o utilizar información, se intenta obtener el control de un sistema informático para utilizarlo con fines maliciosos o robo de información.
- **Ciberamenazas**: Una amenaza digital es un acto malicioso que busca hacer daño a datos, robar datos, o afecta la vida digital en general. Los ciber ataques incluyen amenazas cómo virus.
- **Ciberdelincuente**: Persona que realiza actividades delictivas en internet como robar información, acceder a redes privadas, estafas, y todo lo que tiene que ver con los delitos e ilegalidad.
- **Ciberseguridad**: Es la práctica de defender las computadoras y los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos.
- **CIO**: (Chief Information Officer) Líder de la gestión estratégica de Tecnologías de Información, encargado de planificar, organizar, coordinar, gestionar y controlar la estrategia de uso y apropiación de TI.
- **Código quemado**: Hace referencia a una mala práctica en el desarrollo de software que consiste en incrustar datos directamente en el código fuente del programa como usuario, contraseña, dirección ip, entre otros.
- **ColCERT**: Grupo de Respuesta a Emergencias Cibernéticas de Colombia.
- **Confidencialidad:** asegura que el acceso a la información está adecuadamente autorizado. prevenir la divulgación no autorizada de la información sobre nuestra organización.
- **Cortafuego**: conocido en inglés como firewall, es un sistema que bloquea cualquier intento de uso y acceso no autorizado a equipos de cómputo o portátiles. Los cortafuegos pueden ser de software, hardware, o una combinación de ambos.
- **Correos masivos:** Es él envió simultaneo de correo a varias personas a través de un solo buzón de correo.
- **Custodio de la información**: Es un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado. intenta obtener el control de un sistema informático para utilizarlo con fines maliciosos, robo de información.
- **Disponibilidad**: Asegura que los usuarios autorizados pueden acceder a la información cuando la necesitan.
- **Información sensible**: se usa este término para designar datos privados relacionados con Internet o informática, como contraseñas de correo electrónico, conexión a Internet, IP privada, así como la información personal privada de un individuo como datos personales y bancarios.
- **Integridad:** Supone que la información se mantenga inalterada ante accidentes o intentos maliciosos. Sólo se podrá modificar la información mediante autorización.
- **Malware:** Es un término general para referirse a cualquier tipo de software malicioso, diseñado para infiltrarse en un dispositivo (PC, móviles, tabletas) sin conocimiento, del que hace uso de este.

- **Modelo Integrado de Planeación y gestión- MIPG:** el Sistema de Gestión, integra los Sistemas de Desarrollo Administrativo y de Gestión de la Calidad y lo articula con el Sistema de Control Interno, siendo MIPG el mecanismo que facilitará dicha integración y articulación.
- **NCSI**: Índice Nacional de Seguridad Cibernética.
- **OTIC:** Oficina de las Tecnologías de la Información y las Comunicaciones.
- **Perfiles**: Permite definir los permisos a que tiene derecho un grupo de usuarios.
- **Phishing:** es un método para suplantación de Identidad, que recopila información personal utilizando una llamada telefónica, correos electrónicos y sitios web engañosos, logrando que un usuario comparta contraseñas, números de tarjeta de crédito, y cualquier otra información confidencial.
- **Ransomware**: Es un software malicioso que al infectar un equipo le da al ciberdelincuente la capacidad de bloquear un dispositivo desde una ubicación remota y encriptar los archivos quitando el control de toda la información y datos almacenados. El atacante a cambio de desencriptar la información solicita una cantidad de dinero.
- **Roles:** es una colección de permisos definida para todo el sistema que Usted puede asignar a usuarios específicos.
- **Seguridad de la información:** es el conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos.
- **Seguridad Digital:** es la dependencia de una empresa u organización enfocada en procesos informáticos y telemáticos para proteger toda la infraestructura física y digital relacionada con la tecnología computacional.
- **Servicios Ciudadanos Digitales:** son un conjunto de soluciones tecnológicas que buscan facilitar a los usuarios, y en específico a los ciudadanos, su interacción con las entidades públicas y optimizar la labor del Estado.
- **Sistema de Seguridad Digital SGDI**: busca contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad Digital.
- **TIC**: Tecnologías de la Información y de la Comunicación.
- **TI:** Tecnologías de la información
- **TOGAF**: Es un marco de trabajo de arquitectura empresarial desarrollado por el Open Group que proporciona un enfoque para el diseño, planificación, implementación y gobierno de una arquitectura empresarial. Este marco plantea la estructuración de la arquitectura cuatro dominios o dimensiones: Negocio, Tecnología (TI), Datos y Aplicaciones.

ARTICULO SEXTO – RESPONSABILIDADES: A fin de ejecutar la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, así como la política de seguridad y privacidad de la Información, se establecen los diferentes roles, asignación de responsabilidades y principales actividades a ejecutar así:

ACTIVIDADES	GERENTE	SECRETARIA GENERAL	DIRECTORES O DEPENDENCIAS	CONTRATISTAS
Estructurar la política de seguridad y privacidad de la Información	A - I	R	C	C
Aprobar la política de seguridad y privacidad de la información	A	I	I	I
Implementar y socializar la política de seguridad y privacidad de La Información	I	R	R	R
Actualizar la política de seguridad y privacidad de la Información	I	R	C	C
Efectuar diagnóstico y estado actual del MSPI	I	R	R	C
Identificar vulnerabilidades de los activos de información de la entidad.	I	R	R	C
Identificar avance y efectividad de los controles para la gestión de riesgos de seguridad de la información	I	R	R	C
Documentar, socializar y ejecutar los procedimientos de seguridad de la información	I	R	R	C
Identificar y actualizar los activos de información		R	R	C
Efectuar la valoración y tratamiento de los riesgos de seguridad de la información.	I	R	R	C
Estructurar y ejecutar el plan de sensibilización y capacitación.	I	R	R	C
Establecer los indicadores de Gestión del MSPI para la entidad.	I	R	R	C

Responsable (R): es la persona que realiza el trabajo hasta completar la tarea.

Aprobador (A): es el encargado de designar a la persona responsable de la tarea, además será el responsable de que la tarea se realice con éxito.

Consultado (C): se refiere a las personas que expresan su opinión sobre una actividad en concreto.

Informado (I): designa a aquellos que buscan mantenerse al día sobre el progreso de la actividad

ARTICULO SEPTIMO- MARCO NORMATIVO Y REGULATORIO

La Beneficencia de Cundinamarca por ser una entidad pública del orden territorial, debe cumplir con la regulación y la normativa que establece el Estado colombiano en materia de Tecnologías de la Información. En ese sentido y para dar cumplimiento de la Política pública de Gobierno Digital, la cual hace parte de las 18 políticas de gestión y desempeño institucional, que se establecen en el Modelo Integrado de Planeación y Gestión MIPG, se requiere trabajar e implementar los tres habilitadores transversales de la Política de Gobierno Digital: Arquitectura empresarial, Seguridad de información y Servicios ciudadanos Digitales.

Para implementar el habilitador de seguridad de la información, así como el SGSI y la Política se seguridad y privacidad la Información se requiere dar cumplimiento a los decretos, leyes, normas que se enuncian a continuación:

ARTICULO OCTAVO - NORMAS REGULATORIAS

- **Conpes 3995 de 2020**, Política Nacional De Confianza y Seguridad Digital.
- **Conpes 3975 de 2019**, Política Nacional Para la Transformación Digital e Inteligencia Artificial.
- **Conpes 3920 de 2018**, Política Nacional De Explotación De Datos (Big Data).
- **Conpes 3701 de 2011**, Lineamientos de política para la Ciberseguridad y Ciberdefensa.
- **Resolución 1519** "Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos"
- **Decreto 620 de 2020**, "Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 Y 64 de la Ley 1437 de 2011, los literales e, j y literal a del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9 del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
- **Decreto 1008 de 2018**, por el cual se establecen los lineamientos generales de la Política de Gobierno Digital.
- **Decreto 1499 de 2017**, Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema *de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.* Modelo Integrado de Planeación y gestión- cap 3.
- **Decreto 1078 de 2015**, Reglamenta el Sector de Tecnologías de la Información y las Comunicaciones.
- **Decreto 1377 de 2013**, Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- **Ley 1955 de 2019**, Por el cual se expide el Plan Nacional de Desarrollo 2018-2022.
- **Ley 1712 de 2014**, por medio de la cual se crea la Ley de Transparencia y del Derecho de acceso a la Información Pública Nacional.
- **Ley 1581 de 2012**, Por la cual se dictan disposiciones generales para la protección de datos personales. Protección de datos y privacidad de la información.
- **Ley 1266 de 2008**, Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones, es decir, regula el manejo de la información contenida en bases de datos personales.
- **Ley 594 de 2000**, Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.

- **Ley 527 de 1999**, Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
- **Resolución 3564 de 2015** expedida por MinTIC, Por la cual se reglamentan aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública.
- **Resolución 500 de 2021 de Mintic** – "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital".

Normas Técnicas

- Norma NTC ISO IEC 27001-2013, Técnicas de Seguridad, Sistemas de Gestión de la Seguridad de la Información – SGSI.
- Norma NTC ISO IEC 27002-2013, Técnicas de Seguridad, Código de practica para la gestión de la seguridad de la Información.
- Norma NTC ISO IEC 27005–2009, Técnicas de Seguridad, Gestión del Riesgo en la Seguridad de la Información.

ARTÍCULO NOVENO - POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. Declaración de la política de seguridad y privacidad de la información

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración La Beneficencia de Cundinamarca con respecto a la protección de los activos de información, (procesos, personas y tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apalancan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

La Beneficencia de Cundinamarca, para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Minimizar el riesgo en los procesos de la entidad frente a la seguridad de la información.
- Cumplir con los principios de seguridad de la información.
- Mantener la confianza de los funcionarios y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de La Beneficencia de Cundinamarca de Cundinamarca
- Garantizar la continuidad del negocio frente a incidentes.

Nivel de cumplimiento:

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento al 100% de la política.

A continuación, se establecen los hitos de seguridad que soportan la política del Sistema de Gestión de Seguridad de la Información - SGSI de la Beneficencia de Cundinamarca, en ese sentido la Beneficencia de Cundinamarca se compromete a implementar el SGSI en cada uno de sus procesos a fin de identificar y gestionar la seguridad de los activos de información y adicionalmente a:

- Divulgar y verificar el cumplimiento de la Política de seguridad y privacidad de la información a los funcionarios y contratistas de la entidad.
- Promover la cultura en Ciberseguridad y privacidad de la información al interior de la Beneficencia de Cundinamarca
- Definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio y a los requerimientos regulatorios que le aplican a su naturaleza.
- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los funcionarios y contratistas.
- Aprobar la asignación de funciones, roles y responsabilidades de cada dependencia en el sistema de gestión de seguridad de la información.
- Asignar los recursos para la implementación y mejora continua del sistema de gestión de seguridad de la información.
- Apoyar la innovación tecnológica acorde con los lineamientos del Ministerio de las Tecnologías y las Comunicaciones MINTIC, con el fin de contribuir en la implementación de la Política de Gobierno Digital.
- Minimizar y mitigar los riesgos de seguridad digital, acorde con lo establecido en la política de administración del riesgo de la entidad.
- Protegerá la información generada, procesada y resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.
- Proteger la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información, de su propiedad o en custodia.
- Proteger su información de las amenazas originadas por parte del personal.
- Controlar la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- Implementar controles de acceso a la información, sistemas y recursos de red.
- Garantizar que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- Garantizar a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- Proteger la información en busca de disminuir el impacto generado por las amenazas informáticas sobre sus activos, permitiendo preservar la integridad, salvaguardando la precisión y completitud de la información, confidencialidad, restringiendo el acceso de la información a solo aquellas personas o entidades autorizadas y garantizando la disponibilidad, que es la condición de la información de encontrarse a disposición de quienes deben acceder a ella.
- El incumplimiento a la presente política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

ARTÍCULO DECIMO - SEGUIMIENTO Y REVISIÓN - La secretaría general de la Beneficencia de Cundinamarca será la dependencia encargada de liderar el proceso de seguridad digital y por lo tanto la política de general de seguridad y privacidad de la información será revisada cada que se requiera para que se mantenga oportuna y eficaz.

ARTÍCULO ONCE - VIGENCIA - La presente resolución rige a partir de su expedición y publicación.

PUBLIQUESE Y CÚMPLASE,

Dada en Bogotá D.C., a los 13 días del mes de diciembre de 2021.

SALOMON SAID ARIAS
Gerente General

Revisó y Aprobó: Nestor Armando Castañeda Castañeda
Secretaria General (E)
Revisó y aprobó: Erika Constanza González Rubio
Jefe Oficina Asesora de Planeación
Revisó: Diana Carolina Zambrano Cruz
Jefe Oficina Asesora Jurídica.
Proyectó: Jonhattan Andreis Raquejo Romero
Contratista Beneficencia
Reviso: Jaime Omar Garcia Bautista
Jefe Oficina Control Interno