Empresas Públicas de La Ceja E.S.P
Tu empresa, nuestra empresa

Plan de Seguridad y Privacidad de la Información.

Nit: 811.009.329-0
Telefono: 604 553 77-88
Punto CIEM – Calle 20 # 22 – 05
Email: esplaceja@eeppdelaceja.gov.co
www.eeppdelaceja.gov.co
@eeppdelaceja

Introducción

El presente documento describe el Plan de Seguridad y Privacidad de la Información de Empresas Públicas de La Ceja E.S.P, alineado con los objetivos, metas, procesos, procedimientos y la estructura organizacional.

La Política de Gobierno Digital han definido dos (2) componentes: TIC para el Estado y TIC para la Sociedad, y tres (3) habilitadores transversales: Arquitectura, Seguridad y Servicios Ciudadanos Digitales, como se puede observar a continuación:

Ilustración 1 Política de Gobierno Digital - Fuente MINTIC

Donde los componentes permiten mejorar el funcionamiento de las entidades públicas, su relación con otras entidades y el fortalecimiento de su relación con la sociedad. Los habilitadores por su parte, contribuyen al logro de los objetivos definidos en los componentes.

El habilitador de Seguridad y Privacidad, permite a la Entidad garantizar la confidencialidad, disponibilidad e integridad de la información, para lo cual se hace indispensable diseñar el Plan de Seguridad y Privacidad de la Información que a continuación se detalla.

Marco Normativo

- Ley 1712 de 2014; Para la Implementación de la Estrategia de Gobierno en Línea, entidades del orden nacional; Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea.
- Decreto 2573 de 2014; Por medio de la cual se crea la Ley de Transparencia y del derecho de acceso a la Información pública nacional y se dictan otras disposiciones.
- Ley 1581 de 2012 Por la cual se dictan disposiciones generales para la protección de datos personales.

Conceptos

- **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados.
- **Activo de Información:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la Entidad.
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.
- **Bases de Datos Personales:** Conjunto organizado de datos personales que sea objeto de Tratamiento.
- **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.
- **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.

- **Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.
- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- **Datos Personales Públicos:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.
- **Datos Personales Privados:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.
- **Datos Personales Mixtos:** Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.
- **Datos Personales Sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.
- **Derecho a la Intimidad:** Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural.
- **Encargado del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del tratamiento.
- **Gestión de incidentes de seguridad de la información**: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.
- **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al

ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014.

- **Información Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014.
- **Ley de Habeas Data:** Se refiere a la Ley Estatutaria 1266 de 2008.
- **Ley de Transparencia y Acceso a la Información Pública:** Se refiere a la Ley Estatutaria 1712 de 2014.
- **Mecanismos de protección de datos personales:** Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.
- **Privacidad:** En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Objetivo

Definir la hoja de ruta de la estrategia de ciberseguridad, mediante la aplicación del habilitador de seguridad de la información de la política de gobierno digital, con el fin de proteger y preservar la integridad, disponibilidad y confidencialidad de la información Empresas Públicas de La Ceja E.S.P.

Objetivos específicos

• Implementar Proteger los activos de información de la Entidad, con base en los criterios de confidencialidad, integridad y disponibilidad.

• Administrar los riesgos de seguridad de la información para mantenerlos en niveles aceptables.

• Sensibilizar a los servidores públicos y contratistas de la Entidad acerca del Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información, fortaleciendo el nivel de conciencia de los mismos, en cuanto a la necesidad de salvaguardar los activos de información críticos de la Entidad.

• Monitorear el cumplimiento de los requisitos de seguridad de la información, mediante el uso de herramientas de diagnóstico.

• Implementar acciones correctivas y de mejora para el Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información de Gobierno Digital".

Modelo de Seguridad y Privacidad de la Información

El modelo de seguridad y privacidad de la información contempla un ciclo de operación que consta de cinco fases, las cuales permiten que Empresas Públicas de La Ceja E.S.P. pueda gestionar adecuadamente la seguridad y privacidad de sus activos de información.

1. **Fase de Diagnóstico**

En esta fase se pretende identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.

Para realizar dicha fase se debe efectuar la recolección de la información con la ayuda de la herramienta de diagnóstico y la metodología de pruebas de efectividad.

Una vez se tenga el resultado del diagnóstico inicial y se haya determinado el nivel de madurez de la Entidad se procede al desarrollo de la fase de Planificación.

Los resultados asociados a la fase de Diagnostico previas a la implementación deben ser revisados y socializados por las partes interesadas.

2. **Fase de Planificación**

Para el desarrollo de esta fase la entidad debe utilizar los resultados de la etapa anterior y proceder a elaborar el plan de seguridad y privacidad de la información alineado con el objetivo misional de la entidad, con el propósito de definir las

acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo.

El alcance permite a la Entidad definir los límites sobre los cuales se implementará la seguridad y privacidad en la Entidad.

Este enfoque es por procesos y debe extenderse a toda la Entidad. Para desarrollar el alcance y los límites del Modelo se deben tener en cuenta las siguientes recomendaciones: Procesos que impactan directamente la consecución de objetivos misionales, procesos, servicios, sistemas de información, ubicaciones físicas, terceros relacionados, e interrelaciones del Modelo con otros procesos.

3. **Fase de Implementación.**

Esta fase le permitirá a la Entidad, llevar a cabo la implementación de la planificación realizada.

4. **Fase de Evaluación de Desempeño**

El proceso de seguimiento y monitoreo se hace con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas.

5. **Fase de Mejora Continua**

En esta fase la Entidad debe consolidar los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.

SEBASTIAN ARBOLEDA CARDONA
Gerente General

YOLANDA VALLEJO TOBON
Directora Administrativa

VANESA OROZCO BENITEZ
P. U de las TIC

CONTROL DE CAMBIOS

VERSIÓN	FECHA	ELABORÓ	REVISÓ	APROBÓ	MODIFICACIONES
01					

Nit: 811.009.329-0
Telefono: 604 553 77-88
Punto CIEM – Calle 20 # 22 – 05
Email: esplaceja@eeppdelaceja.gov.co
www.eeppdelaceja.gov.co
@eeppdelaceja