PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Enero/2020

Teléfono: 3394055 -Código postal: 055422
Carrera 43 No. 38 Sur 35
Piso 2 Antiguo Palacio Municipal
Envigado- Colombia
www.concejoenvigado.gov.co

1. INTRODUCCIÓN

El presente Plan de Seguridad y Privacidad de La Información, da cuenta de una serie de tareas que el Concejo Municipal de Envigado realizará a fin de implementar la estrategia de gobierno digital alrededor del componente de seguridad y privacidad de la información, cuyo principal objetivo es proteger los derechos de los usuarios de la entidad y mejorar los niveles de confianza en los mismos a través de la identificación, valoración, tratamiento y mitigación de los riesgos de los sistemas de información.

2. OBJETIVO

Identificar, valorar, tratar y mitigar los riesgos de los sistemas de información con el fin de proteger los activos de información, el manejo de medios, el control de acceso y la gestión de los usuarios.

1. OBJETIVOS ESPECIFICOS

Elaborar un plan de trabajo para la del Plan de Seguridad y Privacidad de La Información.

2. RECURSOS

- Humano: Mesa Directiva, Secretaria General y Líderes de los Proceso
- Físico: PC y equipos de comunicación

3. RESPONSABLES

- Mesa directiva
- Secretaria General
- Líderes de proceso

4. TERMINOS Y DEFINICIONES

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elementos relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización1.

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.2

Acuerdo de Nivel de Servicio: Un Acuerdo de Nivel de Servicio (ANS) es un convenio entre un proveedor de servicios de TI y un cliente. Describe las características del servicio de TI, los niveles de cumplimiento y las sanciones, y especifica las responsabilidades del proveedor y del cliente. Un ANS puede cubrir múltiples servicios de TI o múltiples clientes.

Aplicaciones o aplicativos: Las aplicaciones son herramientas informáticas que permiten a los usuarios comunicarse, realizar trámites, entretenerse, orientarse, aprender, trabajar, informarse y realizar una serie de tareas de manera práctica y desde distintos tipos de terminales como computadores tabletas o celulares3.

Autenticación: Proceso utilizado entre un emisor y un receptor, con el fin de asegurar la integridad de los datos y proporcionar la autenticidad de los datos originales[4]

Backup: Operación que consiste en duplicar y asegurar datos e información contenida en un sistema informático. Es una copia de seguridad.

Clave de autenticación o Contraseñas: Clave criptográfica utilizada para la autenticación de usuario y que se utiliza para acceder a los recursos informáticos.

Copyright: Derecho exclusivo de un autor o editor a explotar una obra física o digital, literaria, científica o artística.

Dominio: Es un conjunto de computadores, conectados en una red, que confían a uno de los equipos de dicha red la administración de los usuarios y los privilegios que cada uno de los usuarios tiene en la red. Es la parte principal de una dirección en la Web, que usualmente indica la organización o compañía que administra dicha página

Internet: Herramienta de comunicación con decenas de miles de redes de computadoras unidas por el protocolo TCP/IP.

---

1 Definición ISO 27000:2009. Overview and Vocabulary. Traducción del autorEddy Pérez – UNEG 2006
2 http://www.microsoft.com/spain/technet/recursos/articulos/srsgch01.mspx
3 http://www.mintic.gov.co/portal/vivedigital/612/w3-channel.html
4 Norma Técnica Colombiana, NTC-ISO 3270

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos. [NTC 5411-1:2006]

Intranet: Es una red de ordenadores privados que utiliza tecnología Internet para compartir, dentro de una organización, parte de sus sistemas de información y sistemas operacionales.

Dirección IP: La dirección IP (IP es un acrónimo para Internet Protocol) es un número único e irrepetible con el cual se identifica una computadora conectada a una red que corre el protocolo IP.

Información personal: Es aquella suministrada por el usuario o el visitante para el registro o consulta de información, la cual incluye datos como nombre, identificación, edad, género, dirección, correo electrónico y teléfono, entre otros6.

Log: Uno o más ficheros de texto automáticamente creados y administrados por un servidor, en donde se almacena toda la actividad que se hace sobre éste7.

Cloud Computing: Es un nuevo concepto tecnológico que se basa en que las aplicaciones software y los equipos hardware con capacidad de proceso y almacenaje de datos que están ubicados en un Datacenter que permite a los usuarios acceder a las aplicaciones y servicios disponibles a través de Internet o como se conoce coloquialmente a través “la Nube” de Internet, de una forma sencilla y cómoda.

Clúster: Conjunto de servidores que trabajan como una única maquina mejorando el desempeño de las transacciones y operaciones implantadas en este sistema.

CPD: Centros de Procesamiento de Datos, ubicación física donde se concentran todos los equipos electrónicos necesarios para el procesamiento de la información de una organización.

CRM: “Customer Retationship Management”. Gestión de la Relación con el Cliente, son herramientas informáticas dedicadas a la gestión integrada de información sobre clientes. Estas aplicaciones permiten, desde almacenar y organizar esta información, hasta integrar, procesar y analizar la misma.

_____
6 http://www.personeriabogota.gov.co/politicas-de-privacidad-y-condiciones-de-uso
7 http://www.alegsa.com.ar/Dic/log%20de%20accesos.php

- **Medios de almacenamiento físico:** Se considera como medio de almacenamiento físico las cintas, los discos extraíbles, los DCs y los DVDs entre otros.

- **Nombres de Grupos:** Seudónimos utilizados para la clasificación de conjuntos de computadoras dentro del dominio.
- **Portal web**: Es un sitio compuesto por varias páginas web, el cual, permite al usuario el fácil acceso a diferentes recursos y servicios que tienen relación con un mismo tema. El portal web del Concejo Municipal de Envigado, se encuentra en la dirección: URL: https://www.concejoenvigado.gov.co/
- **Publicar:** Es la acción de hacer visible un contenido o documento desde un portal o sitio web.
- **Servidor:** Computadora central en un sistema de red que provee servicios a otras computadoras.
- **Sistema Informático o de Información:** Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna forma mensajes de datos.
- **Usuario:** Es un individuo que utiliza una computadora, sistema operativo, servicio o cualquier sistema informático. Por lo general es una única persona. Se autentica e ingresa a los sistemas y sus servicios mediante un nombre de usuario (cuenta) y una contraseña de autenticación.
- **Partes interesadas (Stakeholder**): Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- **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 en las entidades destinatarias del Manual de GEL la correlativa obligación
- **Procedimiento**: Sucesión cronológica de acciones concatenadas entre sí, para la realización de una actividad o tarea específica dentro del ámbito de los controles de Seguridad de la Información.
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- Confidencialidad: Propiedad que determina que la información está disponible ni sea revelada a quien no esté autorizado (2.13 ISO 27000)
- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado

como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- **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 (Ley 1712 de 2014, art 6).
- **Disponibilidad:** Propiedad que la información sea accesible y utilizable por solicitud de los autorizados (2.10 ISO 27000)
- 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. (ISO/IEC 27000).
- **Integridad:** Propiedad de salvaguardar la exactitud y el estado completo de los activos (2.36 ISO 27000)

5. METODOLOGÍA DE IMPLEMENTACIÓN

Para llevar a cabo la implementación del Plan de Seguridad y Privacidad de la Información en el Concejo Municipal de Envigado, toma referencia Modelo de Seguridad y Privacidad de la Información en su versión 3.0.2 publicado por el Ministerio de Tecnologías de la Información y las Comunicaciones.

En este punto es pertinente presentar el ciclo de funcionamiento del modelo de operación, a través de la descripción detallada de cada una de las cinco (5) fases que lo comprenden. Estas, contienen objetivos, metas y herramientas (guías) que permiten que la seguridad y privacidad de la información sea un sistema de gestión sostenible dentro del Concejo Municipal de Envigado.

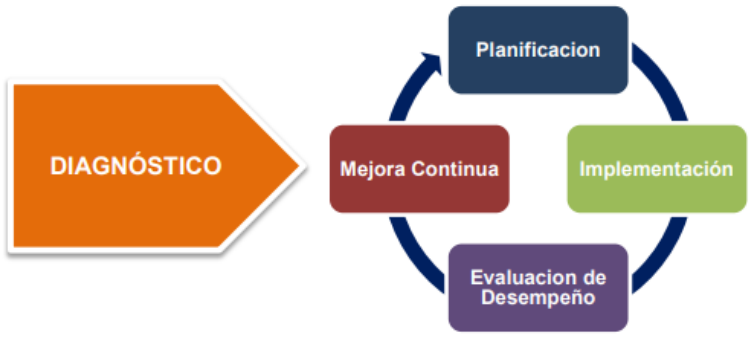

Figura 1 – Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

6. FASE DE DIAGNÓSTICO - ETAPAS PREVIAS A LA IMPLEMENTACIÓN

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.

Figura 2 – Etapas previas a la implementación

Tabla 1 - Metas, Resultados e Instrumentos de la fase etapas previas a la implementación:

Diagnostico			
Metas	**Resultados**	**Instrumentos MSPI**	**Alineación MRAE**
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.	Diligenciamiento de la herramienta.	Herramienta de diagnóstico.	LI.ES.01 LI.ES.02 LI.GO.01 LI.GO.04 LI.GO.05 LI.GO.07 LI.ST.14
Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad	Diligenciamiento de la herramienta e identificación del nivel de madurez de la entidad.	Herramienta de diagnóstico	
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Documento con los hallazgos encontrados en las pruebas de vulnerabilidad.	Herramienta de diagnóstico	

En la fase de diagnóstico del MSPI se pretende alcanzar las siguientes metas:

- Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior del Concejo Municipal de Envigado.
- Determinar el nivel de madurez de los controles de seguridad de la información.
- Identificar el avance de la implementación del ciclo de operación al interior de la entidad.

- Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.
- Identificación del uso de buenas prácticas en ciberseguridad.

Para ello se recomienda utilizar los siguientes instrumentos:

- Herramienta de diagnóstico.
- Instructivo para el diligenciamiento de la herramienta.
- Guía No 1 - Metodología de Pruebas de Efectividad.

Para realizar dicha fase el Concejo Municipal de Envigado 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.

7. 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 del MSPI permite a la Corporación definir los límites sobre los cuales se implementará la seguridad y privacidad. Este enfoque es por procesos y debe extenderse a todo el Concejo Municipal de Envigado.

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.

Figura 3 - Fase de planificación[1]

[1] El contenido de la figura 3 fue tomada de la Norma ISO IEC 27001 Capítulos 4, 5, 6, 7, que permite orientar como se desarrolla la planificación del MSPI.

8. FASE DE IMPLEMENTACIÓN

Esta fase le permitirá al Concejo Municipal de Envigado, llevar acabo la implementación de la planificación realizada en la fase anterior del MSPI.

Figura 4 - Fase de implementación[2]

[2] El contenido de la figura 4 fue tomada de la Norma ISO IEC 27001 Capítulo 8, que permite orientar como se desarrolla la implementación del MSPI.

9. FASE DE EVALUACIÓN DE DESEMPEÑO

El proceso de seguimiento y monitoreo del MSPI 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.

Figura 5 - Fase de Evaluación de desempeño[3]

[3] El contenido de la figura 5 fue tomada de la Norma ISO IEC 27001 Capítulo 9, que permite orientar como se desarrolla la evaluación de desempeño del MSPI.

Plan de revisión y seguimiento a la implementación del MSPI.

En esta actividad el Concejo Municipal de Envigado debe crear un plan que contemple las siguientes actividades:

- Revisión de la efectividad de los controles establecidos y su apoyo al cumplimiento de los objetivos de seguridad.
- Revisión de la evaluación de los niveles de riesgo y riesgo residual después de la aplicación de controles y medidas administrativas.
- Seguimiento a la programación y ejecución de las actividades de autorías internas y externas del MSPI.
- Seguimiento al alcance y a la implementación del MSPI.
- Seguimiento a los registros de acciones y eventos / incidentes que podrían tener impacto en la eficacia o desempeño de la seguridad de la información al interior de la entidad.
- Medición de los indicadores de gestión del MSPI
- Revisiones de acciones o planes de mejora (solo aplica en la segunda revisión del MSPI)

Este plan deberá permitir la consolidación de indicadores periódicamente y su evaluación frente a las metas esperadas; deben ser medibles permitiendo analizar causas de desviación y su impacto en el cumplimiento de las metas y objetivos del MSPI.

10. FASE DE MEJORA CONTINUA

En esta fase el Concejo Municipal de Envigado 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

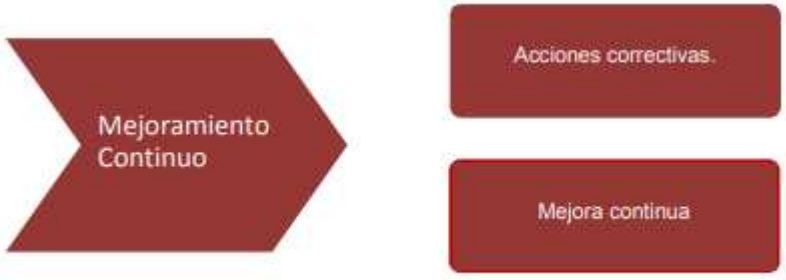

Figura 6 - Fase de mejoramiento continúo[4]

[4] El contenido de la figura 6 fue tomada de la Norma ISO IEC 27001 Capítulo 10, que permite orientar como se desarrolla la fase de Mejoramiento Continuo del MSPI.

En esta fase es importante que la Corporación defina y ejecute el plan de mejora continua con base en los resultados de la fase de evaluación del desempeño. Este plan incluye:

- Resultados de la ejecución del plan de seguimiento, evaluación y análisis para el MSPI.
- Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI.

Utilizando los insumos anteriores, la Corporación puede efectuar los ajustes a los entregables, controles y procedimientos dentro del MSPI. Estos insumos tendrán como resultado un plan de mejoramiento y un plan de comunicaciones de mejora continua, revisados y aprobados por la Alta Dirección de la entidad. La revisión por la Alta Dirección hace referencia a las decisiones, cambios, prioridades etc. tomadas en sus comités y que impacten el MSPI.

11. PROTECCION DE DATOS PERSONALES

EL CONCEJO MUNICIPAL DE ENVIGADO pone en conocimiento la Política de Privacidad y Protección de Datos Personales en virtud de lo consagrado en la Ley 1581 de 2012 y su Decreto reglamentario 1377 de 2013, aplicado a todo dato personal

que hayan sido suministrados o que se suministre al CONCEJO MUNICIPAL DE ENVIGADO

TENIENDO EN CUENTA QUE:

EL CONCEJO MUNICIPAL DE ENVIGADO en su proceso de implementación del Sistema de Gestión de Seguridad de la Información bajo el marco de la norma ISO 27001, aplica y da cumplimiento a la normatividad vigente en materia de protección de datos de carácter personal.

Como parte del Sistema de Gestión basado en ISO 27001, desarrolló las políticas de seguridad tendientes a proteger los activos de información entre ello la protección de datos personales.

Atendiendo la norma, el CONCEJO MUNICIPAL DE ENVIGADO en pro de mejorar su Sistema de Gestión de Seguridad de la Información, ha generado una política para aplicar al tratamiento y protección de datos de carácter personal.

Los funcionarios y contratistas del CONCEJO MUNICIPAL DE ENVIGADO deben, observar, acatar y cumplir las órdenes e instrucciones de carácter legal que aplica la entidad respecto al manejo de los datos de carácter personal cuya divulgación o indebido uso pueda generar un perjuicio a los usuarios, en cumplimiento de los derechos contenidos en el artículo 15 de la Constitución Política de Colombia, ley 1266 de 2008, ley 1273 de 2009, ley 1581 de 2012, Decreto Reglamentario 1377 de 2013, y demás disposiciones complementarias.

INFORMACIÓN PERSONAL RECOLECTADA

La Información Personal que el CONCEJO MUNICIPAL DE ENVIGADO. Puede recolectar y someter a tratamiento es la siguiente:

- Nombre completo del titular de la información;
- Identificación:
- Fecha de nacimiento;
- Domicilio;
- Dirección para notificación;
- Teléfonos de contacto;
- Correo electrónico;
- Identidad de género

TRATAMIENTO DE DATOS PERSONALES DE MENORES DE EDAD

- En aplicación de lo establecido en la ley, el CONCEJO MUNICIPAL DE ENVIGADO procederá a efectuar el Tratamiento de la Información personal; de niños, niñas y adolescentes, respetando el interés superior de los mismos y

asegurando, en todos los casos, el respeto de sus derechos fundamentales y garantías mínimas.

- En todos los eventos en los que se requiera darle tratamiento a la información personal de menores de edad, el CONCEJO MUNICIPAL DE ENVIGADO obtendrá la autorización de sus representantes legales, que para este efecto son el padre y/o madre o tutor.

MANEJO DE LA INFORMACIÓN

CLASIFICACIÓN DE LA INFORMACIÓN

La información resultante de los procesos misionales y de apoyo de la entidad se tratará conforme a los lineamientos y parámetros establecidos en el Manual de Gestión Documental de la entidad.

Los activos informáticos asociados a cada sistema de información, serán identificados y clasificados por su tipo y uso siguiendo lo establecido en las tablas de retención documental vigentes, de acuerdo con los siguientes criterios:

a) Pública: Datos misionales y críticos.
b) Interna: Aplicativos, archivos de software, archivos de usuarios, herramientas y programas de desarrollo. Manuales, procedimientos internos, guías y formatos.
c) Confidencial: Bases de Datos, Documentación, procedimientos operativos, configuraciones.

12. ACTIVIDADES PARA LA IMPLEMENTACIÓN.

- Realizar diagnóstico.
- Comparar el objetivo con lo identificado
- Realizar inventario de activos de información (Software, bases de datos) con los líderes de cada proceso
- Realizar la valoración de los activos de información con los líderes de cada proceso y emitir el plan
- Socializar el plan
- Ejecución del plan
- Realizar seguimiento del plan

13. CUMPLIMIENO DE IMPLEMENTACIÓN.

De acuerdo con las fases mencionadas anteriormente, se describe a continuación los dominios que se deben desarrollar y los plazos de implementación de acuerdo a lo establecido por el Concejo Municipal de Envigado.

- Implementar la Política de Seguridad de la información.
- Aspectos organizativos de la seguridad de la información
- Plan de tratamiento de riesgos de seguridad y privacidad de la información
- Seguridad de la Información enfocada a los recursos humanos
- Revisión de los Controles de acceso
- Seguridad en las telecomunicaciones
- Gestión de Incidentes de Seguridad de la Información
- Aspectos de seguridad de la información en la gestión de continuidad del plan.

14. CRONOGRAMA.

N°	ACTIVIVIDAD	RESPONSABLE	FECHA DE ENTREGA
1	Realizar diagnóstico.	Recurso Externo	01-04-2020
2	Realizar inventario de activos de información	Recurso Externo Líderes de los procesos	15-04-2020
3	Realizar la valoración de los activos de información	Recurso Externo Líderes de los procesos	30-04-2020
4	Comparar el objetivo con lo identificado	Recurso Externo Líderes de los procesos	05-05-2020
5	Construir el plan de seguridad y privacidad de la información para la corporación con los respectivos recursos.	Mesa Directiva Corporados - Funcionarios	15-05-2020
6	Socializar el plan	Mesa Directiva	16-05-2020
7	Ejecutar el plan de seguridad y privacidad de la información para la corporación.	Mesa Directiva Corporados - Funcionarios	16-05-2020 30-11-2020
8	Realizar seguimiento del plan	Recurso Externo	05-12-2020

15. ENTREGABLES

- Informe de avance a la Mesa Directiva y Secretaria General.
- Actas de Reunión.
- Plan aprobado por Mesa Directiva y la Secretaria General.
- Productos de cada etapa.