AREA METROPOLITANA DE BUCARAMANGA

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. PRESENTACION

El siguiente plan estratégico se realiza con el objetivo de ser un indicador de la forma en que se llevara a cabo la implementación y posterior socialización de lo que será la estructura de la estrategia de seguridad y privacidad de la información dando cumplimiento a las directrices establecidas por el programa de gobierno en línea cuyo fin en este aspecto es garantizar ampliamente los niveles de seguridad de la información que por ser entidades de índole publico posee componentes de alta sensibilidad.

2. DEFINICIONES

***Acceso a la información pública.**

Durante los últimos años ha ganado importancia la concientización de todas las personas de que tienen como un derecho fundamental dado por las leyes que rigen nuestra nación (Ley 1712 de 2014, art 4) el acceso a toda clase de información que sea catalogada como publica.

***Activo**

Con referencia al termino de seguridad de la información la palabra activo indica todo elemento de información que se encuentre inmerso en el tratamiento de seguridad de la misma y que puede tener relación con datos de sistemas de información, dé lugares, plantas físicas, documentos y / o personas es decir todos los datos que tengan valor para la entidad.

***Activo de la información**

Para nuestro tema en cuestión este hace referencia específicamente al activo compuesto de información que el funcionario público genera a partir de los datos que recolecta, controla y transforma en el desarrollo de sus funciones.

***Archivo**

Se refiere al conjunto de documentos sin importar su cronología, forma y tipos de soportes que se han logrado reunir mediante procesos establecidos por entidades llámense públicas o privadas durante periodos específicos y que dan como resultado información de relevancia para entidades o personas.

***Amenazas**

Hace referencia específicamente al origen de potenciales incidentes o eventos no deseados y que pueden provocar daños a la estructura de la información que maneja una organización.

Análisis de riesgos
Este hace referencia el proceso mediante el cual se examinan y comprenden los orígenes y los niveles del riesgo. (ISO/IEC 27000).

Auditoria
Se refiere al sistema de procesos independientes y documentados por medio de los cuales se quiere conseguir evidencias de auditoria y posteriormente determinar los niveles de cumplimiento de dichos lineamientos de auditoria. (ISO/IEC 27000).

Autorización

Es el consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales (ley 1581 de 2012, art 3).

Bases de Datos Personales

Conjunto organizado de datos personales que sea objeto de tratamiento (ley 1581 de 2012, art 3).

ciberseguridad

Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

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

Control

Se refiere a todas las políticas, prácticas y estructuras organizativas diseñadas con el fin de mantener en los niveles más bajos los índices de riesgo de seguridad de la información o por lo menos hasta los niveles de riesgo proyectado.
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)

Datos Personales

Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

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. (Decreto 1377 de 2013, art 3).

Datos Personales Privados

Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

Datos Personales Mixtos

Para todo lo que concierne a este documento; 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. (Decreto 1377 de 2013, art 3).

Declaración de aplicabilidad

Documento que establece y enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

***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 (Jurisprudencia Corte Constitucional).

***Encargado del Tratamiento de Datos**

Hace referencia a la 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. (Ley 1581 de 2012, art 3)

***Gestión de incidentes de seguridad de la información**

Son los Procesos mediante los cuales se puede detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

***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. (Ley 1712 de 2014, art 6).

***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 1712 de 2014, art 6)

***Plan de continuidad del negocio**

Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

***Plan de tratamiento de riesgos**

Documento que define y establece el conjunto de 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 de proteger dicha información en observancia del marco legal vigente.

Responsabilidad

Demostrada Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

Responsable del Tratamiento de Datos

Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

Riesgo

Hace referencia a la 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).

Sistema de Gestión de Seguridad de la Información SGSI

Es el Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Titulares de la información

Son las Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).

Trazabilidad

Es la Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

3 OBJETIVOS

3.1 Objetivo General

Establecer y Controlar los niveles de riesgos que se encuentran asociados a cada uno de los procesos tecnológicos existentes, en el Área Metropolitana de Bucaramanga con el objetivo de salvaguardar los activos de información, el manejo de medios, control de acceso y gestión de usuarios.

3.2 Objetivos Específicos

*Diseñar un plan de trabajo específico en donde se validen los recursos con los que se cuenta actualmente en el Área Metropolitana de Bucaramanga para tener establecido un plan de tratamiento de riesgo de seguridad y privacidad de la información.

* Aplicar las metodologías del DAPF e ISO respectivamente en seguridad y riesgo de la información, para que el Área Metropolitana de Bucaramanga de cumplimiento a lo establecido en el programa de gobierno en línea.

4 RECURSOS

*Humano: director, Subdirectores, Profesional 3 Tecnología, Personal Externo
* Físico: Firewall físico, PCS y equipos de telecomunicaciones.
* Financieros: $200.000.000 (doscientos Millones)

5. RESPONSABLES

Gerente General • Líderes del Proceso • Profesional 3 Tecnología 6. METODOLOGÍA DE IMPLEMENTACIÓN Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información en el Área Metropolitana de Bucaramanga, se toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – Min TIC, a través de los decretos emitidos.

De acuerdo con esto, se definen las siguientes fases de implementación del MSPI:

1. Identificación

2. Planeación

3. Ejecución

4. Verificación

5. Puesta en marcha

7. ACTIVIDADES

1. Realizar Diagnóstico

2. Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información

3. Realizar la Identificación de los Riesgos con los líderes del Proceso.

3.1. Entrevistar con los líderes del Proceso

4. Valorar del riesgo y del riesgo residual

5. Realizar Mapas de calor donde se ubican los riesgos

6. Plantear al plan de tratamiento de riego aprobado por los lideres

8. CUMPLIMIENTO DE IMPLEMENTACIÓN

De acuerdo a 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 Área Metropolitana de Bucaramanga.

- Revisión y/o Modificación de la actual Política de Seguridad.
- Aspectos organizativos de la seguridad de la información
- Seguridad Ligada a los recursos humanos
- Revisión del Control de acceso
- Seguridad en la operativa
- Seguridad en las telecomunicaciones
- Gestión de Incidentes de Seguridad de la Información

- Aspectos de seguridad de la información en la gestión de continuidad del negocio.

9. Se establece una cláusula de habeas data y confidencialidad de la información para funcionarios del área metropolitana de Bucaramanga.

CLÁUSULAS DE HABEAS DATA -CONTRATO LABORAL

CLÁUSULA DE AUTORIZACIÓN DE TRATAMIENTO DE DATOS PERSONALES.
El Trabajador/Aprendiz o contratista autoriza el tratamiento de sus datos personales recolectados por EL AREA METROPOLITANA DE BUCARAMANGA. en desarrollo de la relación laboral/funcional que les vincula, y consiente que sean compartidos con organismos aliados y/o empresas con las cuales se tengan relaciones contractuales o legales. Las finalidades para las cuales se utilizarán sus datos, serán: 1. Vinculación y elaboración de contrato laboral, 2. Afiliación al Sistema de Seguridad Social cuando fuere el caso; 3. Actualización de hoja de vida, 4. Registro de asistencia: 5. Registro de capacitaciones; 6. Registro de ingreso; 7. Cumplimiento de obligaciones y actividades relacionadas con el Sistema General de Seguridad y Salud en el Trabajo (SG-SST); 8. Las demás contempladas en la Política de Tratamiento de la Información de EL AREA METROPOLITANA DE BUCARAMANGA.

CLÁUSULA DE OBLIGACIÓN DE CUMPLIMIENTO DE HÁBEAS DATA.
El Trabajador/Aprendiz o contratista se obliga a tratar los datos personales de los Titulares (Clientes, Prospectos, Contactos, Proveedores, Empleados directos, Empleados indirectos, Aspirantes a empleados, Familiares de empleados, Referenciadores, Accionistas, Visitantes, Miembros de Junta Directiva, Contratistas, Vecinos y Terceros, Empleados de contratistas, Oferentes, etc.) a los que tenga acceso en virtud de la relación jurídica que se constituye por el presente documento, en estricto cumplimiento de las normas de protección de Datos Personales que la ley señala y a las directrices contenidas en la Política de Tratamiento de la Información adoptada por EL AREA METROPOLITANA DE BUCARAMANGA., la cual declara habérsele puesto en conocimiento y que tiene a su disposición en la página web www.amb.gov.co. **PARÁGRAFO:** El incumplimiento de las obligaciones aquí estipuladas en materia de Hábeas Data y seguridad de la información, constituirá falta grave y por tanto justa causa para dar por terminado el contrato laboral, sin perjuicio de las sanciones judiciales a que haya lugar.

CLÁUSULA DE OBLIGACIÓN DE REPORTE DE INCIDENTES.
El Trabajador/Aprendiz o contratista se obliga a comunicar inmediatamente al superior jerárquico, por escrito, cualquier pérdida, vulneración, modificación o incidencia sufrida en la información en general y de los datos personales en particular, que se traten en virtud del ejercicio de sus funciones. **PARÁGRAFO:** La omisión del reporte a que haya lugar, constituirá falta grave conforme lo estipulado en el artículo xxx del Reglamento Interno de Trabajo de la organización.

CLÁUSULA DE AUTORIZACIÓN DE ACCESO A MEDIOS TECNOLÓGICOS.
Permitir al jefe inmediato o a quien ésta delegue la revisión física o virtual de los medios tecnológicos que le han sido puestos a disposición para la ejecución de las labores encomendadas, con el único fin de que se supervise el correcto manejo a las estaciones de trabajo, los perfiles de usuario, los correos corporativos y cuentas dispuestas por el superior jerárquico, con miras a garantizar, entre otros, los derechos de los Titulares de datos personales tratados por EL AREA METROPOLITANA DE BUCARAMANGA.

CLÁUSULA DE NOTIFICACIÓN DE CANALES PARA DERECHOS COMO TITULAR DE LOS DATOS. El mecanismo para que el Trabajador/Aprendiz o contratista ejerza sus derechos de acceso, rectificación, cancelación y oposición será a través del correo electrónico quejasyreclamos@amb.gov.co , el buzón de sugerencias ubicado en la oficina principal de EL AREA METROPOLITANA DE BUCARAMANGA o en nuestra página web www.amb.gov.co a través del formulario de contacto.

CLÁUSULA DE RECONOCIMIENTO DE PTI Y PROTOCOLOS.
El Trabajador/Aprendiz o contratista reconoce la prohibición que le asiste para tratar datos personales sin el debido cumplimiento de las normas de protección de seguridad o en desatención de los lineamientos fijados en la Política de Tratamiento de la Información de la organización, así como en los manuales, protocolos, formatos, documentos, normas, reglamentos, circulares y disposiciones que la desarrollen.

CLÁUSULA DE CONFIDENCIALIDAD.
El Trabajador/Aprendiz o contratista se obliga a no revelar la información que reciba durante el desempeño del cargo. Esta condición aplica aun después de la vigencia de la relación laboral/funcional y, en consecuencia, se obliga a mantenerla de manera confidencial o de uso interno y privada a nivel interno y externo, y a proteger dicha información para evitar su divulgación no autorizada, ejerciendo el mismo grado de cuidado que utiliza aquel para proteger información confidencial o de uso interno de su propiedad, de naturaleza similar, si se dan las siguientes condiciones: (i) que al momento de ser recibida esté marcada claramente como confidencial o de uso interno, reservada o con otra leyenda similar; (ii) si se trata de información verbal que se resuma en un escrito que debe entregarse con una marca o leyenda de confidencial o de uso interno, dentro de los treinta (30) días calendario vigentes a su revelación a la parte receptora; (iii) si se trata de datos personales de especial protección, que se conocieron con ocasión del cargo desempeñado, aun si no se encuentra marcada con la leyenda de confidencial o de uso interno. En adelante, la información así marcada se llamará la información confidencial o de uso interno.

CLÁUSULA DE CONFIDENCIALIDAD DE CREDENCIALES DE ACCESO.
EL AREA METROPOLITANA DE BUCARAMANGA entregará al Trabajador/Aprendiz o contratista claves de acceso a los servicios de red y aplicaciones de la organización, para uso exclusivo de acuerdo a las funciones propias de su cargo o labor encomendada. Por tanto, el Trabajador/Aprendiz o contratista se obliga a conservar en total reserva y

confidencialidad las claves suministradas, así como toda la información que llegare a conocer a través de los accesos que le sean habilitados a los servicios de red y las demás aplicaciones. Lo aquí dispuesto regirá aun después de la vigencia de la relación laboral. Así mismo, el Trabajador/Aprendiz o contratista se obliga a reportar al área o funcionario encargado, cuando tenga conocimiento de la ocurrencia de cualquier incidente con sus claves de acceso, que ponga en peligro la seguridad, integridad o confidencialidad de la información a la que se pueda acceder.

CLÁUSULA DE ANTECEDENTES POR MAL MANEJO DE HÁBEAS DATA Y DATOS PERSONALES.

Bajo gravedad de juramento el Trabajador/Aprendiz o contratista declara no haber sido sancionado por mal manejo de información ni datos personales.

CLÁUSULA DE SECION DE DERECHOS DE AUTOR SOBRE LA CREACION Y DESARROLLO DE HERRAMIENTAS Y SOLUCIONES DE INDOLE INTELECTUAL.

El trabajador, aprendiz o contratista se obliga a ceder sus derechos sobre las creaciones de índole intelectual que realice para EL AREA METROPOLITANA DE BUCARAMANGA en el desarrollo de las actividades propias de su objeto contractual y se obliga a dejar a la entidad los respetivos manuales de usuario, código fuente en el caso del desarrollo de software y programación de estructuras basadas en aplicaciones de software; estará obligado a entregar a la entidad todo el material en donde se describa de manera pormenorizada la creación, la estructura ,documentación, claves, nombres de usuarios y demás información necesaria para su correcto funcionamiento ; lo anterior inclusive posterior a la terminación del vínculo generado por el tipo de contrato laboral.