Para Bogotá Limpia S.A.S ESP, sus activos de información son de vital importancia, por tal razón, la organización ha decidido mantener esquemas de protección, aseguramiento y gestión de estos frente a las posibles amenazas que afecten la confidencialidad, integridad o disponibilidad en sus procesos de negocio, buscando protegerlos de la manera más adecuada.

Como pieza fundamental para alcanzar una debida protección de todos y cada uno de los activos de información, la organización se apoya en los grupos de interés el talento humano, quienes deben de cumplir de manera oportuna todos y cada uno de los lineamientos propuestos en materia de seguridad de la información.

Todos los grupos de interés identificados deben de tener conocimiento, cumplir y acatar la **(D-SGI-001) Política del Sistema de Gestión Integrado** y las siguientes **Políticas Específicas de Seguridad de la Información** detalladas en el presente documento.

Los grupos de interés deben salvaguardar la Confidencialidad, Integridad y Disponibilidad de la Información que genere, administre y/o maneje según lo especificado en los acuerdos comerciales y/o laborales, así como realizar la respectiva devolución de la información digital, física u otro formato que le fue entregada al momento de iniciar el acuerdo y durante la vigencia de este.

Protección de Datos Personales: La organización ha establecido su **(D-SGI-002) Política de Protección de Datos Personales**, la cual se encuentra publicada y podrá ser consultada en su página web https://www.bogotalimpia.com. Todo grupo de interés debe autorizar el tratamiento de datos personales y cumplir con los controles de seguridad de la información de acuerdo con las normas vigentes relacionadas.

Bogotá Limpia SAS ESP establece medidas para evitar la pérdida, mal uso (diferente a la(s) finalidad(es) definidas para los grupos de interés), alteración, acceso no autorizado y robo de los datos facilitados por los grupos de interés.

Bogotá Limpia SAS ESP comunica a los grupos de interés las finalidades establecidas en la **(D-SGI-002) Política de Protección de Datos Personales** que determinan el uso que se dará a la información personal suministrada, que de manera general se definen como:

- El uso como medio de soporte para el cumplimiento de las obligaciones contractuales durante y después de la relación laboral. (Trabajadores)
- Mantener una comunicación eficaz con el usuario mediante el trámite de Peticiones Quejas y Reclamos (Usuarios), y,
- Garantizar la adecuada vinculación y relación comercial con nuestra empresa (Proveedores).

En ninguna circunstancia se utilizarán los datos recopilados para otra acción diferente a su misionalidad y al objeto de recolección, previa autorización informada del titular de los datos a excepción de los terceros autorizados por el titular o por la ley.

Privacidad y Confidencialidad: Los grupos de interés se obligan a guardar absoluta reserva, salvo autorización expresa de Bogotá Limpia SAS ESP, de todas aquellas informaciones que lleguen a su conocimiento en razón de su trabajo y que sean de cualquier naturaleza, por lo tanto se compromete a no revelar, difundir, comentar, analizar, evaluar, copiar o realizar un uso diferente del previsto, ni utilizará dicha información para el ejercicio de su propia actividad, ni la duplicará o compartirá con terceras personas, salvo autorización previa y escrita de Bogotá Limpia SAS ESP, so pena de incurrir en contravenciones de la normativa legal establecida. Todo ello será sin perjuicio de las sanciones legales, laborales y comerciales que la ley contempla. Así mismo, los grupos de interés deberán manejar la información con el mismo sigilo empleado por Bogotá Limpia SAS ESP y sólo podrán obtenerla y utilizarla para el cabal cumplimiento de sus funciones.

Etiquetado de la Información: Según la clasificación de la información (clasificada, reservada y pública), los grupos de interés manejan, preparan, copian y entregan los activos de información sólo al personal autorizado. La utilización de equipos de reproducción tales como fotocopiadoras, impresoras, escáneres para información con calificación reservada serán debidamente autorizada por el líder del proceso correspondiente.

Organización de la Seguridad de la Información: Los grupos de interés deben de tener conocimiento de sus responsabilidades relacionadas con la seguridad de la información, las cuales quedarán reflejadas en acuerdos comerciales, laborales o de cualquier otra índole, donde se indique su relación con la empresa.

Gestión de Acceso: Cualquier acceso por parte de los grupos de interés que lo requieran, a los recursos tecnológicos o a la información de la organización debe haber cumplido con las autorizaciones respectivas del líder de proceso correspondiente. Los privilegios asignados a los usuarios estarán asociados a los Sistemas de Información o recursos que corresponda de acuerdo con el rol del grupo de interés.

Manejo, Acceso, Uso y Transferencia de la Información: La Información de la organización debe ser usada única y exclusivamente para los propósitos de la función/rol o actividades que desempeña el grupo de interés. De igual manera el uso y acceso de la información de la organización debe ser consistente con los lineamientos que existan.

Bogotá Limpia S.A.S ESP tiene la propiedad legal del contenido de todos los datos almacenados en cualquier sistema informático suministrado por la organización, así como cualquier mensaje de datos transmitido vía estos sistemas. La organización se reserva el derecho de brindar acceso a la información para el desarrollo de las actividades y uso por parte de los grupos de interés.

Para la transferencia e intercambio de información con grupos de interés se debe seguir lo indicado en los acuerdos contractuales, comerciales, laborales, o de cualquier otra índole, donde se indique su relación con la empresa, para la prestación del servicio público domiciliario de aseo en la ciudad de Bogotá

Al momento de terminar relaciones con un grupo de interés que manejó información de la organización, el responsable del seguimiento de los acuerdos contractuales, comerciales, laborales o de cualquier otra índole, asociados con el grupo de interés, debe asegurarse que la información entregada sea destruida o en su debido defecto devuelta, y se validará la gestión de accesos que se hayan podido habilitar.

Los grupos de interés externos a la organización autorizan a Bogotá Limpia S.A.S ESP a realizar auditoria para validar los controles utilizados para el manejo de la información de la organización por parte de ellos.

Seguridad Física y del Entorno: Todos los grupos de interés deben tener asignados privilegios de acceso a las instalaciones de la organización, para prevenir el acceso físico no autorizado a áreas restringidas y la pérdida, robo, daño e interferencia de los activos de la información de la empresa, que pueda comprometer la continuidad de las operaciones.

Gestión de Comunicaciones: Toda conexión o tráfico de datos hacia los servidores o equipos de trabajo de la organización proveniente del exterior, debe pasar primero por un sistema de protección perimetral, de igual forma las conexiones hacia Internet.

La organización utilizará diversos mecanismos que permitan restringir el acceso a sitios de Internet que se consideren cuestionables o cuyo propósito no sea el estrictamente definido para su función.

Gestión de Contraseñas: Todos los sistemas de información de la organización o cualquier recurso tecnológico incorporan un sistema de control de acceso basado en credenciales (usuario y contraseña).

La contraseña asignada al usuario para el acceso a los sistemas de información es de carácter personal, confidencial e intransferible. El usuario no debe permitir que sus contraseñas sean vistas y aprendidas por otras personas. En caso el usuario sospeche que su acceso puede ser vulnerado, deberá cambiar su contraseña de acceso de manera inmediata.

Ninguna contraseña debe ser guardada de forma legible en archivos ejecutables, scripts, macros, teclas de función de terminal, archivos de texto, en computadores o en otras ubicaciones en donde personas no autorizadas puedan descubrirlas o usarlas. Se recomienda no tener su contraseña en cualquier medio impreso.

Todas las estaciones de trabajo de los usuarios deben tener activado el bloqueo de pantalla por tiempo de inactividad.

Recursos Informáticos: Los recursos informáticos de la organización deben ser usados para fines laborales. Cualquier otro uso, debe ser autorizado previamente y realizado de manera moderada de tal forma que no interfiera con la productividad de la persona o con las actividades propias de la organización.

La organización usa controles de acceso y otras medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información manejada por estaciones de trabajo y sistemas de información, que puedan ser utilizados por los grupos de interés. Para cumplir con estos objetivos, Bogotá Limpia S.A.S. ESP se reserva el derecho de restringir o revocar los privilegios de cualquier usuario, así como para inspeccionar, copiar, remover cualquier dato, programa u otro recurso que vaya en contra del alcance de la relación con los grupos de interés; y, tomar cualquier medida necesaria para utilizar proteger los sistemas de información de la organización. Esta autoridad se puede ejercer con o sin conocimiento, o previo aviso a los grupos de interés.

Los usuarios no deben leer, modificar, copiar, borrar o extraer información perteneciente a otro usuario o la organización.

Gestión de Eventos e Incidentes / Vulnerabilidades: Queda prohibido a los usuarios, explotar las deficiencias de seguridad o vulnerabilidades de los sistemas de información para acceder a la información contenida en ellos.

En el caso de encontrar eventos, incidentes o vulnerabilidades de seguridad de la información, estos deben ser reportados de inmediato al proceso de Gestión Tecnología.

Sistemas Desatendidos / Escritorio y Pantalla Limpia: Los usuarios no deben dejar su estación de trabajo desatendido sin bloquear o cerrar primero la sesión activa. Se debe mantener el escritorio de la estación de trabajo sin documentos de carácter "reservado".

Los documentos de carácter "reservado" que se encuentran en papel y/o medios removibles no deben dejarse encima del escritorio. Asimismo, mantener los puestos de trabajo ordenados y limpios, dejando al final de la jornada los puestos libres de información reservada.

Sistemas y aplicaciones: Está prohibido copiar o duplicar, bajo cualquier medio, cualquiera de los aplicativos y/o programas que se aloja en las estaciones de trabajo de la organización, los cuales tienen "Licencia de uso". Los grupos de interés de la organización, con acceso a aplicativos y/o programas desde sus estaciones de trabajo, deben revisar e investigar sobre los derechos de

propiedad intelectual para todo material o software antes de ser usado para cualquier propósito que esté relacionado con la organización.

La instalación de hardware o software, la reparación o retiro de cualquier parte o elemento en las estaciones de trabajo o demás recursos informáticos solo puede ser realizada ´por el personal del proceso de Gestión Tecnología de la empresa. La instalación de software que posee algún tipo de esquema de licenciamiento diferente al que posee la organización no podrá ser instalada sin previa autorización del líder del proceso correspondiente y del personal del proceso de Gestión Tecnología.

Dispositivos Móviles / Medios Removibles: Está prohibido el uso de medios removibles sin autorización del Líder del Proceso y sin conocimiento del personal de Gestión Tecnología. Es responsabilidad de los usuarios revisar cualquier medio extraíble como: memorias o discos USB, teléfonos móviles, cámaras con memoria y en general cualquier dispositivo que almacene archivos y que se pueda conectar al computador de manera directa o inalámbrica, que sea conectado al computador de tal manera que se eviten posibles incidentes con malware. Los grupos de interés internos de la organización no deben almacenar información de la organización en ningún medio removible (USB y Discos Externos) sin autorización del líder del proceso y sin conocimiento del personal de Gestión Tecnología.

El esquema de protección para las estaciones de trabajo utilizados dentro de las instalaciones de la organización deben considerar aspectos tales como agente antimalware, aplicación de parches y actualizaciones, software cortafuegos, entre otros programas que se utilicen para asegurar la confidencialidad e integridad de la información contenida en los equipos.

Para el uso de equipos portátiles, teléfonos móviles, tabletas, entre otros definidos por el proceso de Gestión Tecnología, se deben implementar controles de acceso y mecanismos de respaldo de la información que se consideren necesarios y pertinentes para garantizar la seguridad de la información.

Uso de Internet: El acceso a navegación de páginas o servicios de internet, se asigna para propósitos laborales. Los usuarios deben ser advertidos sobre la existencia de recursos tecnológicos que realizan un seguimiento sobre las actividades realizadas con el servicio internet. El uso de Internet con propósitos personales será evaluado y permitido siempre y cuando esté autorizado por el director o líder de proceso y que no afecte de ninguna forma la productividad del personal y no cause conflictos con las actividades o seguridad de la información de la organización.

Los usuarios de la organización deben abstenerse de descargar a través de Internet: videos, audio, imágenes, a menos que estas descargas estén debidamente justificadas para propósitos laborales y estén autorizadas por el líder del proceso que corresponda. Del mismo modo, queda prohibido el acceso, observación o cualquier forma de utilización de sitios Web que en su contenido contemple pornografía, juegos, racismo o que de alguna forma atenten contra los derechos fundamentales, normatividades de ley, reglamento interno de trabajo, los presentes lineamientos de seguridad o demás reglas que rigen a la organización.

Con relación a la navegación por sitios web, de preferencia deben acceder a sitios seguros, los cuales se identifican por la nomenclatura "https" al inicio de la dirección web; en caso la página no cuente con este nivel de seguridad, es necesario que el usuario se asegure que la página a la que está accediendo es la verdadera para el desarrollo de sus funciones.

La organización está en todo su derecho de monitorear de manera continua y constante el tráfico de entrada o salida que circula por el (los) servicio(s) de Internet contratado(s).

Uso de Correo Electrónico: El correo electrónico debe ser usado únicamente para los propósitos del trabajo.

La cuenta de correo asignada es preferentemente de carácter individual, por lo cual está prohibido el acceso a una cuenta de correo que no sea la asignada. Para la creación de buzones compartidos, deberá ser autorizado por el líder del proceso que corresponda.

Se prohíbe el uso del correo electrónico con fines religiosos, políticos, lúdicos o cualquier forma que vulnere los derechos fundamentales de las personas.

En ninguna circunstancia los usuarios que reciban correo no habitual o desconocido, o identifique un remitente no válido, deberán abrirlo ni dar respuesta a quien envía el mensaje.

No deben asignarse o utilizarse direcciones de correo cuyo dominio pertenezca a plataformas públicas. Todo buzón de correo asignado debe tener una persona responsable de su administración, incluidos los buzones que se utilizan en los sistemas de información de la organización.

La organización se reserva el derecho de monitorear y/o revisar los buzones de correo electrónico o servicios asociados, sin notificar al usuario de la acción a realizar.

Respaldo de la Información: Para la información y los datos almacenados en las estaciones de trabajo, se realizará un respaldo de información con cierta periodicidad. Es responsabilidad del usuario estar al pendiente de la ejecución de este procedimiento.

El proceso de Gestión Tecnología no es responsable, ni dueño de ninguna de la información o dato de la organización, a excepción de los documentos e información producidas o procesadas en dicho proceso.

A menos que exista una autorización previa de la alta dirección, ningún sistema de control de la infraestructura de seguridad debe ser desactivado, inhabilitado, desconectado o apagado, sin conocimiento del personal del proceso de Gestión Tecnología.

Relaciones con Terceros: Bogotá Limpia S.A.S ESP protege la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos de la información que se generan como resultado de un servicio o proceso interno tercerizado con un grupo de interés externo.

Criptografía: La empresa ha definido reglas para el uso efectivo de la criptografía, incluyendo la gestión de claves criptográficas, en los casos de la trasmisión de información con software y de las transacciones financieras, para proteger la confidencialidad e integridad de la información.

Teletrabajo: Para el caso de trabajadores de la empresa que realicen actividades o funciones, bajo el esquema de teletrabajo, se dará cumplimiento a la legislación vigente en Colombia en materia de teletrabajo, teniendo en cuenta los controles establecidos por la organización tales como: la seguridad física existente en el sitio (incluye edificación y entorno local), entorno físico, requisitos de seguridad de las comunicaciones (necesidad de acceso remoto a los sistemas internos de la empresa), gestión de la información a la que se tendrá acceso y que pasará a través del enlace de comunicación, la gestión de amenazas de acceso no autorizado a información o a recursos tecnológicos de la empresa, uso de redes domésticas y requisitos o restricciones sobre la configuración de servicios de red inalámbrica, acuerdos para evitar disputas acerca de derechos de propiedad intelectual desarrollados en equipos de propiedad privada, requisitos de firewall y de protección contra software malicioso.

Cumplimiento: El incumplimiento de estos compromisos y cualquier violación de los lineamientos de la seguridad de la información conlleva la aplicación de medidas legales, disciplinarias y/o sanciones según lo establecido en nuestro Reglamento Interno de Trabajo, los acuerdos comerciales, laborales y contractuales, así como normatividad legal, que puedan estar vigentes con los grupos de interés.

Bogotá Limpia SAS ESP velará por el cumplimiento de la legislación relacionada y aplicable con la gestión de seguridad de la información, entre ella la referente a derechos de autor y propiedad intelectual, protección de datos personales y delitos informáticos. Todo grupo de interés es responsable de registrar y reportar las violaciones a la seguridad de la información, confirmadas o sospechadas al Director SGI y/o Director Gestión Tecnología, o quienes designen.

Jairo Antonio Cordero Hernández
Gerente General