

Para Bogotá Limpia S.A.S ESP, su Información, así como los sistemas que la contienen son activos de información de vital importancia. Por tal razón, la organización ha decidido mantener esquemas de protección, aseguramiento y gestión de dichos activos frente a las posibles amenazas que afecten la confidencialidad, integridad o disponibilidad en sus procesos de negocio, buscando protegerles 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 el talento humano, el cual debe 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 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. El incumplimiento de los compromisos conlleva a medidas disciplinarias según lo establecido en nuestro Reglamento Interno de Trabajo y los acuerdos comerciales, laborales y contractuales que puedan estar vigentes con los grupos de interés.

Los grupos de interés deben salvaguardar la Confidencialidad, Integridad y Disponibilidad de la Información que administre y/o maneje durante la vigencia de acuerdos comerciales y/o laborales, así como realizar la respectiva devolución de la información digital y/o física que le fue entregada al momento de iniciar el acuerdo y durante la vigencia del mismo.

**Protección de Datos Personales:** 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.

**Privacidad y Confidencialidad:** Los grupos de interés deben tratar la información originada dentro de la organización, protegiendo dicha información, así como evitar su divulgación no autorizada a terceros, que pudiera poner el riesgo los objetivos de la organización.

**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 y/o laborales.

**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.

Todos los usuarios con acceso a recursos tecnológicos e información de la organización deben poseer un identificador único. Todos los sistemas y computadores deben soportar un usuario con privilegios superiores a un usuario normal con el fin de poder ejercer las correspondientes labores administrativas y por lo cual estos privilegios deben ser asignados únicamente al Director y/o Líder de Gestión Tecnología, o quien ellos designen. 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 de intercambio de la información 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 o laborales, asociados con el grupo de interés, debe asegurarse que la información entregada sea destruida, o en su debido defecto devuelta.

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; la pérdida, robo, daño e interferencia a la información de la empresa, que pueda comprometer la continuidad de las operaciones.

**Gestión de Comunicaciones y Operaciones:** Toda conexión o tráfico de datos hacia los servidores 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 componentes tecnológicos que permitan el bloqueo a sitios de Internet que se consideren cuestionables o cuyo propósito no sea el estrictamente de su función.

**Gestión de Contraseñas:** Las contraseñas iniciales otorgadas a un usuario, deben servir únicamente para el primer ingreso del usuario al sistema, en ese momento el sistema debe obligar al usuario a cambiar su contraseña.

Se limita el número de intentos consecutivos de introducir una contraseña válida, permitiendo el bloqueo posterior.

Todos los sistemas de información de la organización o cualquier recurso tecnológico que involucre un sistema de control de acceso basado en credenciales (usuario y contraseña), deben validar una vigencia de la contraseña. Una vez vencida, la contraseña debe expirar y bloquear la cuenta del usuario.

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 "Batch", 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.

No está permitido a un usuario, revelar la contraseña a otros usuarios o grupos de interés. La contraseña personal no debe ser digitada en presencia de terceras personas, así sean trabajadores de la organización. Ningún usuario deberá intentar obtener contraseñas de otros usuarios.

Todas las estaciones de trabajo de los usuarios deben tener activado el bloqueo de pantalla por contraseña, luego de un tiempo específico de inactividad, adicional a que no se debe instalar un papel tapiz diferente a los especificados.

Para la definición de contraseña, se implementará un esquema de complejidad de la misma.

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

Todo usuario es responsable por todas las actividades o interacción con procesos donde se vea involucrada su identificación, siendo personal e intransferible.

Los usuarios no deben permitir que otros usuarios realicen labores bajo su identidad, y tampoco deben realizar actividades bajo la identidad de alguien más. La utilización de los recursos informáticos por parte de terceras personas con conocimiento o consentimiento del usuario, o por su descuido o negligencia, lo hace responsable de posibles pérdidas o, daños que estas personas ocasionen a los equipos e información de propiedad de la empresa.

La organización usa controles de acceso y otras medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información manejada por computadores y sistemas de información. Para cumplir con estos objetivos, Bogotá Limpia S.A.S. ESP se reserva el derecho y la autoridad de restringir o revocar los privilegios de cualquier usuario para inspeccionar, copiar, remover cualquier dato, programa u otro recurso que vaya en contra de los objetivos antes planteados; y, tomar cualquier medida necesaria para utilizar proteger los sistemas de información de la organización. Esta autoridad se puede ejercer con o sin conocimiento de los usuarios.

Los usuarios tienen la prohibición de capturar contraseñas o utilizar otros mecanismos que le puedan permitir obtener acceso a sistemas no autorizados.

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

**Gestión de Eventos e Incidentes / Vulnerabilidades:** Los usuarios no deben explotar las deficiencias de seguridad de los sistemas de información para dañarlos o acceder a la información contenida en ellos,

En el caso de encontrar eventos, incidentes o vulnerabilidades, estos deben ser reportados de inmediato al proceso de Sistemas.

**Sistemas Desatendidos / Escritorio y Pantalla Limpia:** Los usuarios no deben dejar su computador desatendido sin cerrar primero la sesión activa. Se debe mantener el escritorio del computador 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 sin custodia. Mantener puestos de trabajo ordenados y limpios, dejando al final de la jornada los puestos libres de información reservada.

**Sistemas y aplicaciones:** Está prohibido copiar cualquiera de los aplicativos y/o programas que se aloja en los computadores 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.

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 instalación de hardware o software, la reparación o retiro de cualquier parte o elemento en los equipos de computación o demás recursos informáticos solo puede ser realizada por el personal del área de sistemas 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 jefe inmediato y del personal del área de sistemas.

**Dispositivos Móviles / Medios Removibles:** Está prohibido el uso de medios removibles sin autorización del jefe inmediato del área y sin conocimiento del personal de Gestión Tecnología. Es responsabilidad de los usuarios revisar cualquier medio extraíble, como: memorias USB, CD's, DVD's, teléfonos móviles, USB's, 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 contagios de infección electrónica. Los grupos de interés internos de la organización no deben almacenar información de la organización en ningún medio removible (Diskette, USB, Discos Externos) sin autorización del jefe inmediato del área y sin conocimiento del personal de Gestión Tecnología.

El esquema de protección de los equipos informáticos utilizados dentro de las instalaciones de la organización tiene su correspondencia en el nivel de protección de los equipos portátiles, en aspectos tales como antivirus, parches, 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 dispositivos de computación móvil como equipos portátiles, teléfonos móviles, tabletas, entre otros definidos por el área de Sistemas, 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:** Se asigna para propósitos laborales y/o comerciales. 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 está permitido siempre y cuando este no afecte de ninguna forma la productividad del personal y no cause conflictos con las actividades propias de la organización.

Los usuarios de la organización deben abstenerse de descargar a través de Internet: videos, audio, imágenes de gran tamaño, a menos que estas descargas estén debidamente justificadas para propósitos laborales y/o comerciales y estén autorizadas por el jefe inmediato del área. 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 o demás reglas que rigen a la organización.

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) Internet contratado(s).

**Uso de Correo Electrónico:** El correo electrónico debe ser usado únicamente con prioridad para los propósitos del trabajo. Se recomienda usar términos y expresiones adecuadas como en otros medios de comunicación formal de la organización, para que no sean interpretados al relacionarse con los grupos de interés externos como la postura oficial de la organización.

La cuenta de correo asignada es preferentemente de carácter individual por lo cual ningún trabajador no debe usar la cuenta de otro trabajador. Para la creación de buzones compartidos, deberá ser autorizado por el jefe del área respectiva.

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 solicitado no deben abrirlo, ni dar respuesta a quien envía el mensaje.

Todas las direcciones de correo electrónico asignados a los usuarios internos de la organización deben corresponder con la función que desempeñan. No deben asignarse direcciones de dominio externas de carácter personal. 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:** La información y los datos almacenados en los computadores o portátiles se le deben realizar un respaldo de información con cierta periodicidad. Es responsabilidad del usuario estar pendiente de la ejecución de este procedimiento.

El área de Sistemas no es responsable, ni dueño de ninguna de la información de la organización, a excepción de los documentos e información producidas en dicha área.

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 área de sistemas.

**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 del riesgo que se genera de los accesos otorgados a sus grupos de interés externos, o como resultado de un servicio o proceso interno tercerizado.

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

**Teletrabajo:** En caso de formalizarse y definirse el Teletrabajo para los colaboradores con responsabilidades dentro de Bogotá Limpia ESP SAS, 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), sensibilidad de la información a la que se tendrá acceso y que pasará a través del enlace de comunicación, sensibilidad del sistema interno, la amenaza de acceso no autorizado a información o a recursos, por parte de otras personas que usan el mismo alojamiento (ej. familia y amigos), 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.