ANEXO 6
CONSIDERACIONES DE SEGURIDAD DE LA INFORMACIÓN
GRUPO 1 CONTACT CENTER

El siguiente documento contiene las consideraciones de seguridad que deben ser cumplidas por terceras partes. El contratista debe conocer la intención de la entidad en materia de seguridad y protección de la información de la entidad, por tal motivo se presenta la Política de Seguridad de la Información.

Política de Seguridad de la Información

Para la Cámara de Comercio de Bogotá, 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.

El Comité Ejecutivo de la Cámara de Comercio de Bogotá dispondrá de los recursos y acciones necesarias para garantizar la seguridad de los activos de información que la organización utiliza en pro de la prestación de los servicios que ofrece a sus clientes, atendiendo siempre los requerimientos legales y manteniendo su compromiso de calidad y seguridad frente a sus empleados, asociados y clientes.

Como elemento estratégico, la organización cuenta con una guía de gestión de riesgos en la cual se declaran los niveles de aceptación al interior de la Cámara de Comercio; con el propósito de disminuir la probabilidad de que alguna de las amenazas presentes afecte de manera significativa la operación del negocio.

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.

Cumplimiento con la seguridad de la información: Todos los colaboradores de la organización deben cumplir y acatar la Política General de Seguridad de la Información, Política de Protección de Datos Personales así como sus documentos relacionados en materia de protección y seguridad de la información. Corresponde velar por su estricto cumplimiento a la Oficina de Gestión de Riesgos, Vicepresidencia de Tecnología y Contraloría Interna.

Efectos por incumplimiento de La Política de Seguridad de la Información, Política de Protección de Datos Personales y sus documentos relacionados: El incumplimiento de La Política de Seguridad de la Información, Política de Protección de Datos Personales así podrá ser sancionado, salvo lo señalado sobre comparendos pedagógicos, conforme lo establece el reglamento interno de trabajo.

1. El contratista debe salvaguardar la Confidencialidad, Integridad, Disponibilidad de la Información que administre y/o maneje dentro de la CCB durante la vigencia del contrato, así como realizar la respectiva devolución de la información digital y/o física que le fue entregada al momento de iniciar el contrato y durante la vigencia del mismo hasta su finalización. Adicional a lo anterior, debe: "Remitirse o ver el documento interno Política General de Seguridad de la Información".

2. En las prácticas de seguridad se debe incluir lo siguiente:

    a. "El contratista debe cumplir con las siguientes prácticas de seguridad de la información establecidas al interior de la CCB a través del documento: PRÁCTICAS EN SEGURIDAD DE LA INFORMACIÓN – DOCUMENTO INTERNO:

        i. **SEGURIDAD DEL RECURSO HUMANO Acuerdo y aceptación de la política y prácticas de seguridad de la información:** Todo usuario debe firmar el formato **INF-SPI-F-001** Cláusula de autorización de tratamiento y cumplimiento de la seguridad de la información y la protección de datos personales., antes de otorgarle cualquier tipo de información sin importar el medio en el que se maneje, o su identificación de usuario y contraseña y sus respectivos privilegios para el uso de los recursos tecnológicos de la CCB, este acuerdo de confidencialidad también cubre a empleados temporales, consultores y toda aquella persona o empresa que de una u otra manera tenga acceso a la información de la organización, para facilidad de todos los colaboradores sea de planta, consultores, temporales se facilita la guía rápida de seguridad de la información, la cual debe ser leída antes de firmar dicho acuerdo de confidencialidad.

        ii. **Organización Seguridad de la información:**

            1. **Definición clara de las responsabilidades de seguridad de la información en relación con terceros:** Socios de negocios,

proveedores, clientes y otros asociados a los negocios de la CCB deben tener conocimiento de sus responsabilidades relacionadas con la seguridad de la información y esta responsabilidad se debe ver reflejada en los contratos con la CCB y verificada por la Vicepresidencia de Operaciones e Informática.

2. **Acceso por parte de terceros:** Cualquier acceso por parte de un tercero a los recursos tecnológicos o a la información de la organización, debe haber cumplido con las autorizaciones respectivas y además estén debidamente firmados los acuerdos de confidencialidad respectivos.

3. **Manejo de información con terceros:** Al momento de terminar relaciones con un tercero el cual maneje información de la organización, el tercero debe destruir de una manera adecuada la información o en su debido defecto devolver la información.

4. **Acuerdos con terceras partes:** Dentro de los acuerdos de servicios con terceras partes se debe incluir una cláusula, la cual autorice a la CCB a realizar auditoria para validar los controles utilizados por los terceros para el manejo de la información de la organización.

iii. SEGURIDAD FISICA Y AMBIENTAL

1. **Manejo de privilegios y remoción de los mismos:** Todos los empleados, contratistas y terceras partes deben tener asignados privilegios de acceso a las instalaciones de la entidad, es responsabilidad del área de seguridad física, su manejo y control. En caso de finalización de contratos se deben eliminar inmediatamente los privilegios de acceso físico.

iv. GESTIÓN DE COMUNICACIONES Y OPERACIONES

1. **Sistemas de protección perimetral:** Toda conexión a los servidores de la CCB proveniente del exterior, sea Internet, acceso telefónico o redes externas debe pasar primero por un sistema de protección perimetral (Firewall), con el fin de limitar y controlar el tráfico de red a los activos de información de la entidad.

2. **Toda conexión hacia Internet debe pasar por el sistema de protección de perímetro:** El sistema de protección de perímetro (firewall) debe ser el único elemento conectado directamente a

Internet por lo cual toda conexión desde la red interna hacia Internet debe pasar por dicho componente tecnológico.

v. CONTROL DE ACCESO

1. **Revisión periódica y reautorización de privilegios de usuarios:** Los derechos de acceso a los usuarios serán revisados al menos una vez al año con el fin de mantener un control eficaz de acceso a los datos y a los servicios de información, labor que será realizada por el propietario o responsable del Sistema de Información en acompañamiento de la Dirección de Sistemas a través del procedimiento definido para tal fin.

2. **Identificación de usuarios:** Todos los usuarios de recursos tecnológicos e información deben poseer un identificador único.

3. **Identificación de usuarios estándar:** Los identificadores de usuarios genéricos en cualquier sistema operacional, base de datos, o aplicación, deben estar debidamente documentados en caso de ser utilizados.

4. **Soporte para usuarios con privilegios especiales:** 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 a los administradores. Se brindarán permisos de administrador a los usuarios que lo requieran, siempre y cuando exista una previa validación por parte de la Infraestructura de Tecnología a cargo del Coordinador de Soporte Técnico, en donde se valide que se requieren este tipo de permisos especiales para la administración de Software que no permite la misma bajo el tipo de usuario estándar.

5. **Gestión de Privilegios**: Los privilegios asignados a los usuarios deben estar asociados a/o los Sistemas de Información que corresponda de acuerdo al rol del funcionario en la Entidad. Es responsabilidad del propietario del o los Sistemas de Información definir los privilegios y notificar a los administradores respectivos para su adecuada asignación.

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

7. **Límite de intentos consecutivos de ingreso al sistema:** El sistema debe limitar el número de intentos consecutivos de introducir una contraseña valida. Después de tres (3) intentos fallidos el identificador del usuario debe ser bloqueado hasta nueva reactivación por parte del administrador, después que se compruebe la identidad del usuario.

8. **Longitud mínima de las contraseñas:** Todos los sistemas de información de la organización deben validar que las contraseñas deben tener como longitud mínima 7 caracteres, de igual manera deben validar que no se involucren contraseñas en blanco.

9. **Historia de las contraseñas:** Los sistemas de información, o componentes tecnológicos que involucren un proceso de autenticación de usuarios debe mantener historia de al menos las últimas 5 contraseñas utilizadas por parte de los usuarios, de tal manera que no puedan ser reutilizadas.

10. **Vigencia de las contraseñas:** Todos los sistemas de información de la organización o cualquier recurso tecnológico que involucre un sistema de control de acceso basado en credenciales (login, contraseña), deben validar como vigencia de la contraseña un periodo de 30 días hábiles, pasado este tiempo la contraseña debe expirar y bloquear la cuenta del usuario.

11. **Notificación de cambio de contraseñas:** Todos los sistemas de información de la organización o cualquier recurso tecnológico que involucre un sistema de control de acceso basado en credenciales (login, contraseña), deben notificar al usuario 10 días antes que su contraseña debe ser cambiada, por el vencimiento de la misma.

12. **Sesión:** Todos los sistemas y computadores de la organización, debe tener involucrado un sistema de control de acceso, así como un conjunto de credenciales que lo habiliten para utilizar los recursos de la organización.

13. **Permisos por defecto en sistemas de archivos:** Los accesos a los sistemas de archivos de red de la organización deben bloquear por defecto el acceso de usuarios no autorizados. Se excluyen las carpetas que hayan sido definidas de propósito PÚBLICO a la cual pueden tener acceso todos los usuarios para intercambio de archivos.

vi. CUMPLIMIENTO

1. **Uso personal de los recursos informáticos:** Los recursos informáticos de la CCB deben ser usados para fines laborales. 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.

2. **Responsabilidad de la Identificación del usuario:** Todo usuario es responsable por todas las actividades relacionadas con su identificación. La identificación no puede ser usada por otro individuo diferente a quien fue otorgada dicha identificación. Los usuarios no deben permitir que otros usuarios realicen labores bajo su identidad. De forma similar, los usuarios no 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 los posibles daños que estas personas ocasionen a los equipos o a la propiedad de la Cámara de Comercio de Bogotá (CCB).

3. **Uso del software entregado:** Cuando la CCB realiza contratos de licenciamiento de software, la entidad subscribe con los fabricantes un contrato de "LICENCIA DE USO" para los aplicativos que utiliza. Está terminantemente prohibido copiar cualquiera de los aplicativos que se aloja en los computadores de la Entidad.

4. **Declaración de reserva de derechos de la CCB:** La CCB 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 mantener estos objetivos la CCB se reserva el derecho y la autoridad de: 1. Restringir o revocar los privilegios de cualquier usuario; 2. Inspeccionar, copiar, remover cualquier dato, programa u otro recurso que vaya en contra de los objetivos antes planteados; y, 3. Tomar cualquier medida necesaria para manejar y proteger los sistemas de información de la CCB. Esta autoridad se puede ejercer con o sin conocimiento de los usuarios, con conocimiento del jefe inmediato, siempre con el concurso del Vicepresidente de Operaciones e Informática o de quién él delegue esta función.

5. **Acceso no autorizado a los sistemas de información de la Entidad**: Los usuarios tienen la prohibición de obtener acceso a sistemas de información a los que no se tiene privilegios e igualmente se prohíbe cualquier modificación o consulta de la información contenida en el sistema. Esto implica la prohibición de capturar contraseñas, llaves de cifrado y otros mecanismos de

control de acceso que le puedan permitir obtener acceso a sistemas no autorizados.

6. **Posibilidad de acceso no implica permiso de uso**: Los usuarios no deben leer, modificar, copiar o borrar información perteneciente a otro usuario.

7. **Prohibición a la explotación de vulnerabilidades de seguridad de los recursos informáticos**: Los usuarios no deben explotar las deficiencias de seguridad de los sistemas de información para dañar los sistemas o la información contenida en ellos, obtener acceso a recursos a los cuales no se le ha dado acceso. En el caso de encontrar vulnerabilidades, estas deben ser reportadas de inmediato al área de seguridad de la información. Para garantizar la seguridad de los sistemas y canales de comunicación entre el proveedor y la CCB, debe existir además de la cláusula de privacidad y cumplimiento, un análisis de vulnerabilidades que el proveedor ejecute al menos 4 veces al año y de la cual pueda garantizar a través de un informe con reporte de análisis que está llevando a cabo las mitigaciones que requiere para el tratamiento de vulnerabilidades, disminuyendo la posibilidad de cualquier amenaza que pueda derivarse de las anomalías encontradas o que existan en sus sistemas de información y plataforma tecnológica.

8. **Dejar sistemas desatendidos:** Los usuarios no deben dejar el computador desatendido sin cerrar primero la sesión iniciada.

9. **Protección por Defecto de Copyright:** Todos los colaboradores de la organización deben revisar, e investigar los derechos de propiedad intelectual para todo material, software y/o sitio Web encontrado en Internet antes de ser usado para cualquier propósito que esté relacionado con la entidad.

10. **Prohibición de instalación de software y hardware en los computadores de la organización:** 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 los funcionarios autorizados de la Dirección de Sistemas de información. Solamente bajo la autorización del área de Infraestructura Tecnológica se permitirá la instalación de software no contemplado al momento inicial de configurada la estación.

11. **Esquemas de licenciamiento de fuente abierta y/o libre distribución:** La instalación de software que posee algún tipo de esquema de licenciamiento diferente al que posee la

organización (Dominio Público, Shareware, Freeware, entre otros), no podrá ser instalada, hasta el momento que se solicite la autorización respectiva por parte al área de Infraestructura Tecnológica.

12. **Juegos no pueden estar almacenados sobre un computador:** Bajo ninguna circunstancia es posible almacenar o usar cualquier juego en los recursos computacionales suministrados por la Cámara de Comercio de Bogotá.

13. **Uso de dispositivos móviles:** Es responsabilidad de los usuarios revisar cualquier medio extraíble (memorias USB, CDs, DVDs, teléfonos móviles USBs, cámaras con memoria con conexión a USB y en general cualquier dispositivo que almacene archivos y que se pueda conectar al computador a través de puerto USB), que sea conectado al computador de tal manera que se eviten posibles contagios de malware o infección electrónica.

14. **Confidencialidad de las contraseñas:** La contraseña que a cada usuario se le asigna para el acceso a los sistemas de información, debe ser personal, confidencial e intransferible, cada usuario debe velar porque sus contraseñas no sean vistas y aprendidas por otras personas.

15. **Identificación única para cada usuario:** Cada usuario tendrá una identificación única, acompañado de un elemento para su autenticación (contraseña) de carácter personal y confidencial para la utilización de los recursos tecnológicos necesarios para sus labores.

16. **Almacenamiento de contraseñas:** Ninguna contraseña debe ser guardada de forma legible en archivos “Bach”, 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.

17. **Sospechas de compromiso deben forzar cambios de contraseña:** Toda contraseña deberá ser cambiada por el usuario de forma inmediata si se sospecha o se conoce que ha perdido su confidencialidad.

18. **Revelación de contraseñas:** Bajo ninguna circunstancia está permitido revelar la contraseña a empleados o a terceras personas. La contraseña personal no debe ser digitada en presencia de terceras personas, así sean funcionarios de la

Entidad. Ningún usuario deberá intentar obtener contraseñas de otros usuarios.

19. **Auditoria periódica a las contraseñas de los usuarios:** Solamente la auditoria de Sistemas ó el área de seguridad de la información realizarán auditorías a las bases de datos de las contraseñas de los usuarios, con el objetivo de dar cumplimiento a las labores de monitoreo de cumplimiento a las políticas de seguridad de la información.

20. **Uso obligatorio de contraseña en el protector de pantalla:** Todas las estaciones de trabajo de los usuarios deben tener activado el protector de pantalla institucional protegida por contraseña, adicional a que no se debe instalar un papel tapiz diferente a los especificados.

21. **Manejo, Acceso y Uso de la Información:** La Información de la Cámara de Comercio de Bogotá debe ser usada única y exclusivamente para los propósitos de la función que desempeña el colaborador dentro de su entorno laboral. De igual manera el uso y acceso de la información de la organización debe ser consistente con las políticas que existan.

22. **Propiedad legal de los archivos de los sistemas de información y mensajes:** La Cámara de Comercio de Bogotá tiene la propiedad legal del contenido de todos los archivos almacenados en cualquier sistema informático suministrado por la organización, así como cualquier mensaje de datos transmitido vía estos sistemas. La Cámara de Comercio de Bogotá se reserva el derecho de utilizar la información para el desarrollo de sus actividades

23. **Medios Removibles**: Los colaboradores de la organización no deben almacenar información de la entidad en ningún medio removible (Diskette, USB, Discos Externos).

24. **Uso de Internet para propósitos personales:** El uso de Internet se asigna para propósitos laborales. Los usuarios de Internet deben ser advertidos sobre la existencia de recursos tecnológicos que generan registros sobre las actividades realizadas. 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.

25. **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 clientes o terceros como la postura oficial de la organización. Todo mensaje de correo electrónico (e-mail) deberá contener en la parte inferior el siguiente mensaje: “Este es un mensaje de carácter confidencial de la Cámara de Comercio de Bogotá. Si usted no es el destinatario del mismo o no está autorizado para recibir este mensaje en nombre del destinatario, absténgase de usar, copiar, divulgar o en cualquier otra forma esta información. Las opiniones o información de tipo personal o no directamente relacionadas con los asuntos de la Cámara de Comercio de Bogotá que contenga este mensaje no se deben entender como respaldadas por esta. Si recibió este mensaje por error por favor comuníquese en forma inmediata con su remitente “.

26. **Formalidad del correo electrónico:** Toda comunicación a través del correo electrónico interno se considera una comunicación de tipo laboral y formal, por tanto podrá ser supervisada por el superior inmediato del empleado.

27. **Preferencia por el uso del correo electrónico**: Debe preferirse el uso del correo electrónico al envío de documentos físicos siempre que las circunstancias lo permitan.

28. **Propietarios del buzón de correo:** La cuenta de correo asignada es de carácter individual por lo cual ningún empleado bajo ninguna circunstancia debe usar la cuenta de otro empleado.

29. **Mensajes prohibidos:** Se prohíbe el uso del correo electrónico con fines religiosos, políticos, lúdicos o que vulnere los derechos fundamentales de las personas. Por tanto, está prohibido el envío, reenvío o en general cualquier otra conducta tendiente a la transmisión de mensajes humorísticos, pornográficos, en cadena, publicitarios y en general cualquier otro mensaje ajeno a los fines laborales sin importar si son de solo texto, audio, video o una combinación de los tres.

30. **Respuestas a correo electrónico no solicitado:** Bajo ninguna circunstancia los usuarios que reciban correo no solicitado deben responder a quien envía el mensaje.

31. **Bloqueo de Acceso:** La organización puede utilizar componentes tecnológicos que permitan el bloqueo a sitios de Internet que se consideren cuestionables o cuyo propósito no sea el estrictamente de su función.

32. **Visitas y Descargas de Internet:** 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, de la misma manera 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, la presente normatividad o demás reglas que rigen a la entidad.

33. **Direcciones de correos institucionales:** Todas las direcciones de correo electrónico externo asignados a los usuarios internos de la CCB, deben corresponder con la función que desempeñan. No deben asignarse direcciones externas de carácter personal. Se exceptúan los miembros del Comité Directivo y aquellas solicitudes justificadas por un miembro del Comité Directivo.

34. **Todo buzón de correo debe tener un responsable:** 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

35. **Control de Tráfico en Internet**: La organización está en todo su derecho de monitorear de manera continua y constante el tráfico que circula hacia o de Internet.

36. **Monitoreo del correo electrónico**: La organización se reserva el derecho de monitorear y/o revisar los mensajes de correo electrónico corporativo sin notificar al usuario de la acción a realizar.

37. **Manejo de archivos adjuntos:** Los usuarios deben abstenerse de abrir archivos adjuntos de mensajes los cuales desconozcan el remitente.

38. **Foros públicos:** Los colaboradores de la organización deben abstenerse de participar en comunidades, foros, blog y demás medios electrónicos de intercambio de información, con información relevante de la organización, a menos que está esté debidamente autorizada.

39. **Responsabilidad de las copias de respaldo de los usuarios:** La información y los datos almacenados sobre computadores o portátiles se le deben realizar un Backups con regularidad. Es responsabilidad del usuario que se realice el procedimiento.

40. **Revisiones de sistemas de información:** El área de seguridad de la información debe tener autorización para revisar la configuración, programación,

41. mantenimiento, entrenamiento, y monitorear los sistemas de información de la organización.

42. **Responsabilidad y propiedad:** Tanto el área de seguridad de la información, Infraestructura Tecnológica, así como Desarrollo de Sistemas de Información, no son los responsables, ni dueño de ninguna de la información de la organización, a excepción de los documentos e información producidas en las respectivas áreas.

43. **Deshabilitar controles de seguridad:** A menos que exista una autorización de la Vicepresidencia de Operaciones e Informática, ningún sistema de control de la infraestructura de seguridad debe ser desactivado, inhabilitado, desconectado, apagado, o sobrepasado.

Nota:

Todo funcionario que trabaje para la campaña de la CCB debe firmar el formato :

INF-SPI-F-001 Cláusula de autorización de tratamiento y cumplimiento de la seguridad de la información y la protección de datos personales sea temporal o indefinido. El contratista debe garantizar la firma del documento por cada uno de los funcionarios asignado de forma temporal o permanente y allegarlos a la CBB para su respectiva custodia. Para tal efecto se adjunta formato correspondiente.

Conozco y acepto:

Firma Representante Legal