1. JUSTIFICACIÓN

La adopción de políticas, normas y procedimientos de seguridad de la información obedece a una decisión estratégica de BE CALL OUTSOURCING S.A.S., con el fin de definir el SGSI, a través del análisis, diseño e implementación de los objetivos, requisitos de seguridad, procesos, procedimientos, planes, políticas, controles con formatos, el tamaño, la tecnología y estructura de la misma.

Se ha definido que las políticas de seguridad de la información deben identificar responsabilidades y establecer los objetivos para una protección apropiada de los activos de información de la entidad, contando además con manuales para usuarios finales. La implementación de las políticas busca reducir el riesgo de que en forma accidental o intencional se divulgue, modifique, destruya o use en forma indebida la información de la entidad.

La organización desde sus directivas pretende mantener un esquema de seguridad que permita asegurar constantemente la confidencialidad, integridad y disponibilidad de la información, siendo esta, su activo más valioso; Para ello adopta, establece, implementa, opera, verifica y mejora un Sistema de Gestión de Seguridad de la Información (SGSI).

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Establecer los lineamientos que permitan proteger, asegurar y salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información de la organización teniendo en cuenta los procesos, la operación, los objetivos de negocio y los requisitos legales vigentes en la entidad.

2.2 OBJETIVOS ESPECIFICOS

- ✓ Definir la política de seguridad y privacidad de la información de la organización.
- ✓ Definir los lineamientos a ser considerados para diseñar e implementar el Sistema de Gestión de Seguridad de la Información alineado con las necesidades, los procesos, los objetivos y la operación de la organización.
- ✓ Dar conformidad y cumplimiento a las leyes, regulaciones y normativas que aplican a la organización en el desarrollo de su misión.

- ✓ Proteger los activos de información de la organización
- ✓ Mantener un sistema de políticas, manuales, procedimientos y estándares actualizados, a efectos de asegurar su vigencia y un nivel de eficacia, que permitan minimizar el nivel de riesgo de los activos de información de la organización
- ✓ Fortalecer la cultura de seguridad de la información en funcionarios, terceros y clientes de la organización, mediante la definición de una estrategia de uso y apropiación de la política.
- ✓ Garantizar la continuidad de negocio frente a la materialización de incidentes de seguridad basados en la norma ISO 27035.
- ✓ Definir una estrategia de continuidad de los procesos de la entidad frente a incidentes de seguridad de la información.

3. ALCANCE

La política de seguridad de la información es aplicable en todo el ciclo de vida de los activos de información de la organización, incluyendo creación, distribución, almacenamiento y destrucción.

De igual forma para todos los funcionarios, contratistas y terceros que desempeñen alguna labor en la entidad. El alcance abarca desde el enunciado de la política, pasando por los lineamientos para la implementación del Sistema Seguridad y Privacidad de la información, la matriz de riesgo, la definición de los indicadores para el monitoreo de cumplimiento de la política hasta la definición de una estrategia para la adopción de la política en la entidad.

4. DOCUMENTOS DE REFERENCIA

A continuación, se relacionan las normas, leyes, decretos y resoluciones que aplican para el establecimiento, implementación y operación del SGSI:

4.1. Constitución Política

4.1.1. **Artículo 15:** Establece el derecho de todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos.

4.2. Leyes

4.2.1. **Ley 1581 de 2012**: Por la cual se dictan disposiciones generales para la protección de datos personales. Es la ley principal que regula el tratamiento de datos personales en Colombia, estableciendo principios, derechos y procedimientos.

4.2.2. **Ley 1266 de 2008**: Por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información personal contenida en bases de datos, especialmente la financiera, crediticia, comercial y de servicios.

4.2.3. **Ley 1273 de 2009**: Modifica el Código Penal para crear nuevos delitos informáticos y proteger la información y los datos.

4.2.4. **Ley 1712 de 2014:** Por la cual se crea la ley de transparencia y el derecho de acceso a la información pública nacional y se dictan otras disposiciones.

4.2.5. **Ley 527 de 1999**: Define y reglamenta el acceso y uso de los mensajes de datos, el comercio electrónico y las firmas digitales, estableciendo un marco legal para las transacciones electrónicas.

4.2.6. **Ley 1336 de 2009**: Fortalece las medidas de protección contra la explotación, la pornografía y el turismo sexual con menores, incluyendo aspectos relacionados con contenidos en línea.

4.2.7. **Ley 1712 de 2014**: Ley de Transparencia y Acceso a la Información Pública Nacional, que garantiza el derecho de acceso a la información pública y establece procedimientos para su divulgación.

4.2.8. **Ley 1928 de 2018**: Establece disposiciones para fortalecer la ciberseguridad y ciberdefensa en Colombia, incluyendo directrices sobre la protección de la información y la infraestructura crítica.

4.2.9. **Ley 1978 de 2019**: Ley de modernización del sector TIC, que incluye disposiciones sobre gestión de información, seguridad digital y protección de datos.

4.2.10. **Ley 2300 de 2024**: Ley Dejen de Fregar. Tiene como objetivo proteger el derecho a la intimidad de los consumidores y deudores.

4.3. Decretos

4.3.1. **Decreto 2952 de 2010:** Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008.

4.3.2. **Decreto 1377 de 2013**: Reglamenta parcialmente la Ley 1581 de 2012, en relación con los aspectos relacionados con las políticas de tratamiento de información y el consentimiento de los titulares.

4.3.3. **Decreto 886 de 2014**: Por el cual se reglamenta lo relativo al Registro Nacional de Bases de Datos.

4.3.4. **Decreto 1074 de 2015**: Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, que en su Capítulo 25 reglamenta aspectos de protección de datos personales.

4.3.5. **Decreto 1078 de 2015**: Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, incluye normas sobre seguridad digital.

4.3.6. **Decreto 090 de 2018**: Proporciona un marco detallado para el registro y manejo de las bases de datos.

4.3.7. **Decreto 1078 de 2015**: Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, incluye normas sobre seguridad digital.

4.3.8. **Decreto 338 de 2022**: Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital.

4.4. Circulares y Resoluciones

4.4.1. **Circular 02 de 2015**, les imparte las instrucciones a los responsables de tratamiento de datos personales, personas jurídicas de naturaleza privadas inscritas en las cámaras de comercio y sociedades de economía mixta, para efectos de realizar la inscripción de sus bases de datos en el Registro Nacional de bases de Datos – RNBD

4.4.2. **Circular Externa 003 del 22 de agosto de 2024:** presenta una serie de lineamientos que deberán tener en cuenta los administradores societarios, sobre el alcance de sus funciones en relación con el tratamiento de datos personales.

4.4.3. **Guía oficial de Protección de Datos Personales SIC:** https://www.sic.gov.co/sites/default/files/files/2023/Guia%20de%20datos%202023%20(2).pdf

4.4.4. **Circular Externa 006 de 2022 SIC**: Se imparten instrucciones para la efectiva protección y el adecuado tratamiento de datos personales en el marco de las actividades de publicidad, marketing y prospección comercial, a tenerse en cuenta en campañas de mercadeo de manera independiente de los canales de comunicación y de las nuevas tecnologías utilizadas para tal fin.

4.4.5. **Circular Única Protección Datos Personales SIC de 2022.** https://www.cerlatam.com/wp-content//uploads/2022/10/SuperIndustria-Circular-2022-N0007519-1_20220930-1.pdf

4.4.6. **Resolución 500 de 2021** Ministerio Tecnología de la Información y Comunicaciones: Establece lineamientos y estándares para la estrategia de seguridad digital y la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI).

4.5. Políticas y Estrategias Nacionales

4.5.1. **Política Nacional de Seguridad Digital:** (CONPES 3854 de 2016)**:** Establece lineamientos para fortalecer la seguridad digital en el país, promoviendo la protección de la información y los sistemas.

4.5.2. **Política de Seguridad de la Información marzo de 2020:** Documento que establece lineamientos, controles, roles y responsabilidades para la gestión de la información en entidades públicas.

5. POLITICA DE SEGURIDAD DE LA INFORMACION PARA BE CALL OUTSOURCING SAS

5.1. POLITICA GENERAL

Se define la Política de Seguridad de la información como la manifestación que hace la alta gerencia de BE CALL OUTSOURCING S.A.S., sobre la intención institucional de definir las bases para gestionar de manera adecuada y efectiva, la seguridad de la información; garantizando la confidencialidad, integridad y disponibilidad de sus activos de información.

BE CALL OUTSOURCING S.A.S. pretende mediante la adopción e implementación

de un Modelo de Seguridad y Privacidad de la información enmarcada en el Sistema de Gestión de Seguridad de la información, proteger, preservar y administrar la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información.

BE CALL OUTSOURCING S.A.S. asume el compromiso de implementar el sistema de Gestión de la Seguridad de la información para proteger los activos de información de los procesos misionales, comprometiéndose a:

- La gestión de los riesgos de los activos de información teniendo en cuenta el nivel de tolerancia al riesgo de la entidad.
- Una gestión integral de riesgos basada en la implementación de controles físicos y digitales orientados a la prevención de incidentes
- El fomento de la cultura y toma de conciencia entre el personal (funcionarios, contratistas, proveedores y terceros) sobre la importancia de la seguridad de la información.
- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.
- Proteger 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 terceros (ej.: proveedores o clientes), o como resultado de un servicio interne en Outsourcing.

- Se mitigarán los incidentes de Seguridad y Privacidad de la información, Seguridad digital de forma efectiva, eficaz y eficiente, y se protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia

5.2. DEBERES INDIVIDUALES DE LOS USUARIOS DE LA INFORMACION

- Usar la información de la organización. únicamente para propósitos del negocio autorizado y en cumplimiento de su labor.
- Respetar la confidencialidad de la información que maneja la organización
- No compartir perfiles de usuario, contraseñas, sesiones en estaciones de trabajo,

documentos o cualquier tipo de información confidencial.

- No anotar y/o almacenar en lugares visibles las contraseñas de acceso a los sistemas.
- Ajustarse a las directrices de clasificación de la información.
- Bloquear la sesión de la estación de trabajo al momento de ausentarse de la misma.
- Las impresiones deben ser recogidas al momento de generarlas, no se deben dejar por largos periodos de tiempo en la impresora.
- Devolver y no conservar ningún tipo de copia sus activos de información, en buen estado, una vez cese su relación laboral con la Entidad
- Este estrictamente prohibido la divulgación, cambio, retiro o pérdida no autorizada de información de la compañía almacenada en medios físicos removibles, como USB, cintas magnéticas, entre otros.
- Esta estrictamente prohibido utilizar software no licenciado en los recursos tecnológicos, copiar software licenciado de la empresa para utilizar en computadores personales, ya sea en su domicilio o en cualquier otra instalación y/o entregarlos a terceros.
- Abstenerse de usar computadoras personales dentro de las instalaciones de la compañía o para uso y/o divulgación de documentos que contengan información confidencial y/o sensible de la organización o sus clientes
- No está autorizado el uso de dispositivos móviles en plataforma. Esto incluye teléfonos, tabletas o cualquier otro dispositivo que permita la comunicación entre los usuarios y que pueda servir para divulgar o compartir información de laorganización o sus clientes

5.3. DEBERES DE LOS RESPONSABLES DE PERSONAL

- Conceder autorizaciones de acceso a la información acorde con las funciones a ser realizadas por las personas a quienes le coordinan el trabajo.
- Asegurar que los privilegios de acceso individuales reflejen una adecuada segregación de funciones. Un usuario no debe tener los permisos suficientes para originar, registrar y corregir/verificar una transacción sensitiva del negocio sin controles adecuados o una revisión independiente.
- Restringir el acceso del personal a aquellas áreas que hayan sido restringidas por razones de seguridad.
- Ser el responsable de conocer, solicitar y ratificar los privilegios de acceso a los

empleados que le reportan.

- Conservar los registros de los empleados con privilegios de acceso a la información. Adicionalmente, TI como encargada de la Seguridad de la información, debe mantener actualizadas las autorizaciones y perfiles de usuario basándose en los archivos de Recursos Humanos y/o contratación (gestión del Outsourcing), donde se encuentran todos los empleados y las áreas a las que pertenecen, al igual que como se establece en la Política de roles y Perfiles.
- Los contratos de Outsourcing o con terceras personas, deben identificar clara mente los acuerdos relacionados con la propiedad de la información y la no divulgación de información confidencial.
- Cuando un empleado se ausenta de su trabajo por un periodo de tiempo superior al mínimo establecido para cumplir con las regulaciones su superior inmediato debe:

a. Determinar si los accesos a los recursos físicos y a la información deben ser suspendidos.

b. Notificar la fecha en que el acceso debe ser suspendido, de ser necesario.

c. Recoger los equipos de seguridad como por ejemplo llaves, claves, computadoras, etc.

d. Cuando un empleado se encuentra por fuera de las funciones de la empresa., ya sea por licencia, suspensión, encargo. etc., el acceso a los recursos físicos y a la información debe ser inmediatamente suspendido por solicitud de su jefe inmediato, de ser necesario.

5.3.1. Cuando un empleado es retirado (voluntaria o involuntariamente), su jefe inmediato es responsable por:

a. Solicitar la revocación de las autorizaciones.

b. Revocar o restringir los privilegios de acceso antes de notificarle la terminación del contrato, si es apropiado.

c. Recoger los equipos, los dispositivos físicos y la revocación de las autorizaciones a los sistemas de información

5.4. DIRECTRICES RELACIONADAS CON EL MANEJO DE LA INFORMACION CONDIFIDENCIAL

- Los documentos con esta información no pueden ser dejados desatendidos o inseguros.
- Debe indicar el usuario dueños o fuente de información en la primera página o cubierta, o en algún repositorio central.
- Debe ser apropiadamente autorizado para la divulgación de acuerdo con los estándares de clasificación de la información por parte de los propietarios.
- La divulgación cualquiera que fuere su medio, verbal, escrita, telefónica o electrónica, debe ser efectuada sobre la base de la necesidad de conocerla de acuerdo con sus funciones.
- Reuniones relacionadas con el manejo de esta información deben llevarse a cabo en áreas de oficinas cerradas.
- No debe ser accedida o enviada a través de cualquier tecnología de fácil acceso, tales como teléfonos celulares o inalámbricos.
- Para propósitos de seguridad toda la información debe ser etiquetada con la clasificación respectiva.
- El etiquetado debe ser fácilmente leíble a simple vista.
- Antes de divulgarse verbalmente información clasificada como Restringida o Confidencial debe indicarse su clasificación.
- El acceso o distribución de información de Uso Interno debe estar limitado a empleados u otros con la necesidad de conocerla o usarla para cumplir con sus funciones y su divulgación debe realizarse a través de medios corporativos claramente definido
- Documentos que contengan información confidencial deben ser impresos en un área segura o con la supervisión adecuada.
- Distribución de información confidencial debe ser limitada a personas o grupos con la necesidad de conocerla o usarla para cumplir con sus funciones.
- Los mecanismos de entrega utilizados para información restringida deben contemplar confirmación de recibo.

- Estas políticas aplican tanto a los originales como a todas las copias de la información.
- Acceso a información confidencial que se encuentre almacenada debe ser adecuadamente controlado. Esto incluye información confidencial almacenada externamente o copias de respaldo.

5.5. USO ADEACUADO DE SOFTWARE

5.5.1. En las estaciones de trabajo de la empresa. solo se puede instalar software desarrollado o adquirido legalmente y cuya licencia de uso este a nombre de BECALL OUTSOURCING S.A.S.

5.5.2. La coordinación y ejecución de mantenimiento de programas o aplicaciones instaladas en las estaciones de trabajo es del equipo de T.I.

5.5.3. Las estaciones de trabajo de la empresa. deben ser utilizadas por los empleados, proveedores o contratistas solo para el desarrollo de las funciones normales de su trabajo.

5.5.4. Los usuarios deben cumplir con la legislación colombiana que regula los derechos de autor.

5.6. CONTROL DE VIRUS

- Los computadores personales deben mantener activo un software antivirus, Sistema Operativo, Microsoft Office, licenciados y actualizados y que su uso haya sido autorizado por el equipo de trabajo TI.
- Los servidores de archivos, groupware y correo electrónico deben mantener activo un software antivirus.
- Los computadores personales y servidores deben ser analizados contra virus periódica y automáticamente.
- Cualquier información que venga por medio electrónico o magnético como correo electrónico o información de INTERNET, debe ser revisada por un software antivirus antes de ser descargada y utilizada.

- El equipo de trabajo de TI es responsable por la actualización oportuna del software antivirus
- Es responsabilidad de los usuarios reportar todos los incidentes de infección de virus a las áreas encargadas.
- Es responsabilidad de los usuarios tomar copias de la información y verificar que el respaldo esté libre de cualquier infección de virus.
- El usuario debe asegurar que toda la información provenga de fuentes conocidas.
- Ningún usuario puede escribir, distribuir o introducir software que conozca o sospeche que tiene virus.

5.7. CONTROL DE CONTRASEÑAS

- Los perfiles de usuario y la contraseña tienen que ser asignados individualmente para soportar el principio de responsabilidad individual.
- Los usuarios no pueden prestar su contraseña, lo que se realice con su perfil queda bajo la responsabilidad del dueño.
- El usuario no debe compartir, escribir o revelar su contraseña.
- Las contraseñas individuales no deben ser mostradas en texto claro. Todos los sistemas de procesamiento deben eliminar la visualización de contraseñas ya sea en pantallas o en impresoras.
- Las contraseñas deben cambiarse con regularidad. La duración máxima de la contraseña debe ser un tiempo razonable (máximo 60 días).
- Si un sistema no obliga al cambio de contraseña, es responsabilidad del usuario realizar este cambio.
- No se deben repetir contraseña utilizadas anteriormente, en los últimos cinco cambios.
- Debe verificarse la identidad del usuario antes de que las contraseñas o perfiles de usuario sean habilitados nuevamente. Solo se puede cambiar una contraseña cuando el perfil de usuario pertenezca a quien solicita el cambio.

- La identificación del usuario y su contraseña no deben ser iguales.
- Las contraseñas deben ser cuidadosamente seleccionadas para que no sean adivinadas fácilmente, por lo tanto, se deben tener en cuenta las siguientes recomendaciones:
    - **a.** No utilizar el primer o segundo nombre, los apellidos, el nombre del esposo, el nombre de sus hijos, etc., en ninguna forma (reversado, diminutivos, etc.)
    - **b.** No utilizar otra información fácil de obtener acerca de Usted. Esto incluye: Placa o marca del carro, numero del teléfono, marca, nombre del edificio, etc.
    - **c.** No use contraseñas que solo contengan números o solo letras.
    - **d.** No utilice palabras contenidas en el diccionario u otras listas de palabras.
    - **e.** Use contraseñas fáciles de recordar para que no tenga que escribirlas.
    - **f.** No use el nombre del perfil de usuario en ninguna forma como,por ejemplo: reversado o duplicado.

- Siempre que el administrador de contraseñas asigne una contraseña, es responsabilidad del usuario cambiarla en su primer uso.

5.8. COPIAS DE RESPALDO DE INFORMACION (BACKUP)

- Se debe contar con un sistema automático para la recolección de copias de respaldo.
- Las copias de respaldo deben tener el mismo nivel de protección de la información que poseen en su fuente original.
- Los medios magnéticos que contienen información deben ser almacenados en lugares físicamente seguros.
- Los usuarios responsables por respaldar la información también son responsables de facilitar la oportuna restauración de la información.
- Los medios magnéticos deben tener rótulos visibles y legibles tanto internos como externos.
- Se debe mantener suficientes respaldos de la información para que en caso de contingencia se pueda recuperar la información oportunamente.
- Para responder adecuadamente a una contingencia, los respaldos de la información se deben almacenar en sitios externos.

- Cualquier medio magnético que contenga información clasificada como restringida o confidencial, debe estar claramente identificada.
- Al enviar información clasificada como restringida o confidencial a terceros se debe exigir un acuse de recibo.
- Todos los medios que contengan información clasificada como restringida o confidencial y que finalice su ciclo de vida, deben ser sobre escritos o destruidos físicamente para que la información no pueda ser recuperada.
- Es responsabilidad de los Administradores de las Plataformas, mantener respaldo de la configuración del sistema operativo y de los servicios que estas proveen.

5.9. POLITICA DE MANEJO DE DOCUMENTOS ELECTRONICOS

- Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información de propiedad de BE CALL OUTSOURCING S.A.S. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.
- Los usuarios podrán enviar información reservada y/o confidencial vía correo electrónico siempre y cuando vayan de manera comprimida y destinada exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones.
- Las comunicaciones electrónicas en lo posible deben ser concretas, precisas y completas
- Las comunicaciones electrónicas oficiales hacia el exterior deben ser revisadas por un jefe inmediato, puede ser un coordinador de área, Líder, sin este requisito no serán consideradas como documentos oficiales de la organización.
- Solamente se considera oficial un mensaje de correo electrónico que incluya el nombre y el cargo del funcionario de la organización
- Se deben conservar los niveles de seguridad en el manejo de la información electrónica conforme a los parámetros definidos institucionalmente para tal fin.
- Todas las direcciones de correo electrónico deben ser creadas usando el estándar establecido por el departamento de TI.
- Todos los funcionarios vinculados a la empresa tendrán correo electrónico personalizado
- El uso del correo electrónico para fines personales deberá ser racional.

- Se establecerá un tamaño de buzón de correo para cada usuario, es decir un espacio en disco en el servidor de correo, destinado al almacenamiento de mensajes electrónicos de cada usuario.

5.10. DIRECTRICES RELACIONADAS CON EL DESARROLLO DE SOFTWARE PARA BECALL – CLIENTE

- Los mecanismos de seguridad definidos para una aplicación específica no deben ser alterados, pasados por alto o comprometidos.
- Los controles de seguridad deben ser documentados y deben permitir probar su efectividad.
- El software desarrollado no debe presentar nuevas vulnerabilidades o reducir el nivel de seguridad existente.
- Cualquier software que use funciones privilegiadas del sistema operativo debe ser aprobado por el equipo de TI y el Cliente.
- El desarrollo y mantenimiento de software debe dejar las adecuadas pistas de auditoria (Registro de eventos).
- El equipo de trabajo del programa TI son responsables de efectuar pruebas para asegurar que se han cumplido los requerimientos de seguridad.
- Todas las aplicaciones deben contar con documentación funcional y técnica.

6. CONTROL DE CAMBIOS

Fecha	Revisión	Descripción / modificaciones
Feb 2020	00	Emisión inicial
Dic 2022	01	Actualización de información
09/30/2023	02	Actualización de la estructura del documento
26/10/2024	03	Se realizan ajustes sobre el marco conceptual legal
13/11/2024	04	Se realizan ajustes sobre la estructura del documento y se actualiza el rótulo
12/09/2025	05	Se actualizó rótulo y logo (OneSource Company)

Elaboró	Revisó	Aprobó
Pedro Jauregui	Camila Ríos/Carlos Ruiz/Jorge Jaramillo	Carolina Acevedo