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.C., 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 esta.

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 2, numeral 6:** Establece el derecho de toda persona a que los servicios informáticos, públicos o privados, no suministren información que afecte su intimidad personal y familiar

4.2. Leyes

4.2.1. **Ley 29733**: Establece los derechos de los titulares de datos, como la consulta y la rectificación, y definen las obligaciones de los responsables y encargados del

tratamiento, incluyendo la necesidad de una autorización previa para el tratamiento de datos personales

4.2.2. **Ley 28493** Ley que regula el uso del Correo Electrónico comercial no solicitado (SPAM). La ley regula el envío de comunicaciones comerciales publicitarias o promocionales no solicitadas, realizadas por correo electrónico, sin perjuicio de la aplicación de las disposiciones vigentes en materia comercial sobre publicidad y protección al consumidor.

4.2.3. **Ley 30096**: Tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia.

4.2.4. **Ley 30171:** Modifica la Ley N° 30096 de Delitos Informáticos. Su objetivo es perfeccionar la lucha contra la ciberdelincuencia, incluyendo la tipificación de conductas ilícitas relacionadas con las tecnologías de la información y comunicación, como el acceso ilícito, la alteración de datos, el fraude informático y, específicamente, las proposiciones sexuales a menores de edad a través de medios tecnológicos.

4.2.5. **Ley 31814**: Ley que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país para promover el uso de la inteligencia artificial en el marco del proceso nacional de transformación digital.

4.3. Decretos

4.3.1. **Decreto Supremo N° 016-2024-JUS.** Se deroga el Decreto Supremo N.º 003-2013JUS que aprueba el Reglamento de la Ley N.º 29733, Ley de Protección de Datos Personales.

4.3.2. **Decreto de Urgencia N° 007-2020**. Establecer las medidas que resultan necesarias para garantizar la confianza de las personas en su interacción con los servicios digitales prestados por entidades públicas y organizaciones del sector privado en el territorio nacional

4.4. Circulares y Resoluciones

4.4.1. **Resolución Directoral Nº 019-2013-JUS/DGPDP.** Esta resolución es parte del marco normativo peruano para la protección de datos personales, que establece los requisitos y procedimientos para garantizar la seguridad de la información en los bancos de datos

4.4.2. DIRECTIVA N° 01-2020-JUS/DGTAIPD. Tiene por objeto establecer las directrices para el tratamiento de los datos personales que se captan a través de los sistemas de videovigilancia con fines de seguridad y control laboral.

4.4.3. Resolución No. 0326-2020-JUS. Aprobación de la Metodología para el Cálculo de las Multas en materia de Protección de Datos Personales

4.4.4. Resolución Ministerial N.° 004-2016-PCM. Aprueban el uso obligatorio de la Norma Técnica Peruana "ISO NTP/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática

4.4.5. Resolución ministerial N.° 166-2017-PCM. Resolución ministerial que modifica el artículo 5 de la R.M. N° 004-2016-PCM referente al Comité de Gestión de Seguridad de la Información

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.C., 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.C. 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.C. 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

✓ Lo referente a **DEBERES INDIVIDUALES DE LOS USUARIOS DE LA INFORMACION** se determinará en el documento *ITC-08-02 Control de acceso al sistema*

✓ Lo referente a **DEBERES DE LOS RESPONSABLES DE PERSONAL** se determinará en el documento *ITC-08-02 Control de acceso al sistema*

✓ Lo relacionado a **DIRECTRICES RELACIONADAS CON EL MANEJO DE LA INFORMACION CONDIFIDENCIAL** se determinará en el documento *ITC-08-22 Procedimiento Control Fuga de Información*

✓ Lo relacionado a USO ADEACUADO DE SOFTWARE se determinará en los documentos *ITC-08-23 Hardening Informático y ITC-08-26 Política de uso e instalación de software*

✓ Lo referente a CONTROL DE VIRUS se determinará en los documentos *ITC-08-03 Instalación de software Antivirus Kaspersky y ITC-08-23 Hardening Informático*

✓ Lo referente a **CONTROL DE CONTRASEÑAS** Se determinará en los documentos *ITC08-15 Altas bajas o modificación de usuarios Be Call y ITC-08-02 Control de acceso al sistema*

✓ Lo referente a **COPIAS DE RESPALDO DE INFORMACION (BACKUP)** Se determinará en el documento *ITC-08-01 Metodología Backup Be Call*

✓ Lo referente a **POLITICA DE MANEJO DE DOCUMENTOS ELECTRONICOS** se determinará en el documento

6. CONTROL DE CAMBIOS

Fecha	Revisión	Descripción / modificaciones
01/04/2025	00	Emisión inicial