1. Objetivo

La presente “Política de Seguridad de la Información Corporativa”, tiene por objetivo establecer el lineamento de la empresa respecto de la responsabilidad, resguardo y gestión de riesgos de la información, así como entregar directrices generales sobre el acceso, manipulación, procesamiento, transmisión, protección, almacenamiento o cualquier otro tratamiento que se realice sobre los activos de información de la empresa.

En consecuencia, a través de la “Política de Seguridad de la Información Corporativa”, se buscar dar cumplimiento a lo siguiente:

a) Establecer un programa de seguridad de la información y los lineamientos generales de seguridad de la información para la infraestructura tecnológica y operación de la compañía.
b) Dar cumplimiento de los requisitos legales y contractuales vigentes y aplicables a la compañía en materia de seguridad de la información.
c) Velar por que todos(as) los(as) colaboradores(as) de la compañía cumplan con la “Política de Seguridad de la Información Corporativa”.
d) Hacer de conocimiento de todos(as) los(as) colaboradores(as) de la compañía el impacto relacionado al incumplimiento de la “Política de Seguridad de la información Corporativa”.

2. Alcance

El Sistema de Gestión de Seguridad de la Información (SGSI) de Tecnologías de la Información en Salud (en adelante TISAL), abarca los siguientes procesos y servicios proporcionados para el Grupo EBM:

a) Servicios de desarrollo
b) Control de calidad (QA)
c) Continuidad operacional de sistemas
d) Seguridad de la información
e) Redes
f) Plataforma de mesa de ayuda regional
g) Soporte técnico en campo
h) Gestión y administración de activos

Límites y Aplicabilidad del SGSI

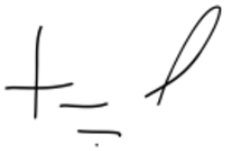
El SGSI se aplica a todas las operaciones, procesos, personal e infraestructura tecnológica involucrados en la prestación de los servicios mencionados anteriormente. Esto incluye:

- Todas las instalaciones físicas donde se llevan a cabo estos procesos.
- Los sistemas de información, bases de datos y redes utilizados para soportar estos servicios.
- Todo el personal involucrado en la entrega y gestión de estos servicios, incluyendo empleados(as), contratistas y terceros relevantes.

Hágase referencia al documento "Alcance del SGSI"[1].

[1] Disponible en el Gestor Documental de TISAL.

3. Aspectos de Control

No. DE VERSIÓN	REVISADO POR	APROBADO POR
3.0	**Nombre**: Hernán Lagunas **Cargo**: Responsable del SGSI **Fecha**: 07-11-2024 **Firma**: 	**Nombre:** Felipe Alfaro **Cargo:** Gerente General **Fecha:** **Firma:** Powered by ecert Firma electrónica avanzada FELIPE ENRIQUE ALFARO JARAMILLO 2024.11.07 14:51:11 -0300 **Nombre:** Sergio Mella **Cargo:** CISO Empresas Banmédica Prestadores **Fecha:** 07-11-2024 **Firma:** 

MODIFICACIONES			
No. DE VERSIÓN	**FECHA**	**DESCRIPCIÓN**	**AUTOR**
1.0	30-11-2020	Versión inicial.	Área de Seguridad de la Información Corporativa
2.0	31-12-2021	Actualización de la política.	Área de Seguridad de la Información Corporativa
3.0	26-08-2024	Se incorpora alcance y publicación del alcance. Actualización de formato.	Área de Seguridad de la Información Corporativa

Contenido

1. Objetivo 1
2. Alcance 2
3. Aspectos de Control 3
4. Evaluación y Revisión 5
5. Mecanismos de Difusión 5
6. Roles y Responsabilidades 6
7. Términos y Definiciones 7
8. Referencias 8
9. Generalidades 9
9.1. Introducción 9
9.2. Cumplimiento de la Política 9
9.3. Restricciones Particulares o Especiales 10
9.4. Disposiciones de la Política 10
9.4.1. Gestión del Programa de Seguridad 10
9.4.2. Evaluación y Gestión de Riesgos 11
9.4.3. Seguridad del Personal 11
9.4.4. Seguridad Física 11
9.4.5. Seguridad de Operaciones 12
9.4.6. Registro, Monitoreo y Gestión de Incidentes 12
9.4.7. Seguridad de la Comunicación 12
9.4.8. Control de Acceso, Administración de Acceso e Identificación y Autenticación 12
9.4.9. Seguridad de la Red 13
9.4.10. Seguridad de Partes Externas o Terceros 13
9.4.11. Seguridad en el Desarrollo de Aplicaciones 13
9.4.12. Continuidad del Negocio y Recuperación Ante Desastres 13
9.4.13. Clasificación y Protección de Datos 14
9.4.14. Seguridad en la Nube 14
9.5. Aspectos de Control 14
9.6. Publicación del Alcance del SGSI 15
10. Excepciones 16

4. Evaluación y Revisión

La "Política de Seguridad de la Información Corporativa" será revisada con una frecuencia anual desde su aprobación, sin embargo, ante cambios significativos que modifiquen el nivel de riesgo del presente documento, la presente política podrá ser analizada, evaluada y actualizada.

Entre los cambios que hacen necesaria la revisión de la política, se destacan los siguientes:

- Cambios en las leyes y/o reglamentos que afecten a la organización.
- Incorporación o modificaciones importantes de procesos críticos del negocio.
- Cambios significativos en el soporte tecnológico.
- Cambios significativos en las amenazas a que se expone la información de la compañía.
- Esta norma debe ser revisada y presentada para su aprobación, por el Comité de Seguridad de la Información (CSI).

5. Mecanismos de Difusión

La presente "Política de Seguridad de la Información Corporativa" debe ser distribuida y difundida a todos los(as) Gerentes(as), Jefaturas y Colaboradores(as) de la organización a través de correo electrónico y/o a través de su publicación en el gestor documental que TISAL defina.

Además, el alcance del Sistema de Gestión de Seguridad de la Información (SGSI) de TISAL se publicará y mantendrá accesible para todas las partes interesadas relevantes a través de los siguientes medios:

- **Intranet Corporativa:** Se creará una sección dedicada al SGSI en la intranet de la empresa, donde se publicará el alcance completo del sistema.
- **Portal de Clientes:** Se incluirá una versión resumida del alcance en el portal de clientes del Grupo EBM, enfocada en los aspectos relevantes para los usuarios externos.
- **Manual del SGSI:** El alcance formará parte integral del Manual del SGSI, que estará disponible para consulta interna. Hágase referencia al documento "Manual del SGSI"[2].

[2] Disponible en el Gestor Documental de Tisal.

6. Roles y Responsabilidades

Para efectos de cumplir con la presente "Política de Seguridad de la Información Corporativa", los(as) directores(as), Gerencias, funcionarios(as) y los(as) colaboradores(as) en general de TISAL tendrán las siguientes responsabilidades y roles:

- **Área de Comunicaciones Internas:** Colaborará en la redacción y diseño de las versiones resumidas y visuales del alcance de la política.
- **CISO:** Es responsable de supervisar el proceso de publicación y actualización del alcance del SGSI.
- **Colaboradores(as) de TISAL:** Son responsables de utilizar la versión más reciente del alcance publicado relacionadas con el SGSI.
- **Directorio:** Debe realizar las acciones necesarias a fin de que se adopten las medidas para asegurar el cumplimiento de la "Política de Seguridad de la Información Corporativa" y se asegure el monitoreo periódico del cumplimiento de los controles y procedimientos que implementen para tal fin.
- **Gerencia de Operaciones y Seguridad:** Es responsable de mantener la infraestructura técnica necesaria para la publicación en medios digitales.
- **Gerencias de TISAL:** Deben alinear sus procedimientos a la política y adoptar las medidas necesarias para asegurar que el personal a su cargo las conozca y aplique, por lo que deberá ejecutar y/o coordinar las correspondientes acciones de difusión y fiscalización.
- **Responsable de Seguridad de la Información de TISAL:** Deberá:
  a) Informar al Directorio sobre cualquier tema de interés relacionado al cumplimiento de la política.
  b) Identificar y asegurar la correcta aplicación de:
    - Los marcos regulatorios legales vigentes y aplicables en materia de seguridad de la información.
    - Los lineamientos de seguridad para las aplicaciones que realizan tratamiento de datos fuera de las instalaciones de TISAL.
    - Los lineamientos de seguridad de la información para el envío de datos por medios de soporte informático.
    - Los lineamientos para mantenimiento de registros de auditoría.
    - Los lineamientos para transferencias por correo electrónico.
    - Los lineamientos para que las App No IT y documentos digitales cumplan con la seguridad de la información.
  c) Brindar soporte de entendimiento para la aplicación de la "Política de Seguridad de la Información Corporativa".
  d) Desarrollar y mantener los roles y responsabilidades del programa de seguridad de la información corporativo.
- **Responsable de Seguridad de la Información y los(as) encargados(as) pertinentes:** deberán:
  a) Asegurar el cumplimiento de la Política.

b) Incorporar en la cultura de la empresa las obligaciones asociadas con la Seguridad de la Información, sustentadas en la Política.
c) Asegurar el monitoreo e investigación para el cumplimiento de la Política.
d) Coordinar y aplicar las sanciones por el incumplimiento de la Política.
e) Asegurar el desarrollo e implementación de procedimientos que permitan el cumplimiento de la Política de Seguridad de la Información.
f) Adoptar la Seguridad de la Información como un elemento integral del ciclo de vida de proyectos.
g) Asegurar la madurez de la Seguridad de la Información con alineación a la Política.
h) Definir las líneas base de seguridad para la infraestructura donde residen las aplicaciones.
i) Ejecutar capacitaciones para que los(as) colaboradores(as) conozcan las normas internas de Seguridad de la Información.

7. Términos y Definiciones

Para efectos de la presente política se considerarán las siguientes definiciones:

- **Activo de Información:** Todo documento físico (DF), documento digital (DD) y aplicativos informáticos (APP) que tengan un valor para la empresa y/o soporten o sean parte de la actividad, proceso o giro de negocio de la organización.
- **Aplicativo informático fuera de la custodia de la Unidad de Sistemas (APPnoIT):** Todo activo de información orientado al procesamiento y administración de datos que se encuentre administrado por una unidad, y además se encuentre alojado en la misma unidad o en la unidad de sistemas. Se incluye a esta definición los archivos digitales con lógica de programación en su contenido, como, por ejemplo: macros en Excel, bases de datos en Access, flujos de trabajo en SharePoint, entre otros.
- **Áreas Seguras:** Áreas donde se requiere un segundo nivel de autorización para obtener acceso físico. Áreas de servidores, centro de datos, closets de cableado, son ejemplos específicos de áreas seguras.
- **Autenticación:** La autenticación se refiere a la verificación de la autenticidad, sea de la persona o de la información, por ejemplo, un mensaje puede ser autentificado que efectivamente ha sido generado por el origen declarado. Las técnicas de autenticación usualmente conforman las bases para todas las formas de control de acceso a los sistemas de información y/o datos y serán determinadas y comunicadas de tiempo en tiempo al interior de la compañía por parte del Área de Seguridad de la Información de TISAL.
- **Control de Acceso:** El control de acceso se refiere a las reglas y mecanismos determinados por el Área de Seguridad de la Información de TISAL, desplegados al interior de la empresa y que controlan el acceso a los sistemas de información y activos de información, así como el acceso físico a las instalaciones y dispositivos donde aquellos se encuentran. La seguridad de la información está sustentada en el control de acceso, sin el cual, la seguridad de la información, por definición, no podría existir.

- **Confidencialidad:** Obligación de guardar reserva y secreto respecto de los activos de información, de los sistemas de tecnología de la información (TI) y, en general, de la información de la compañía que se identifique como confidencial o que por su naturaleza requiera trato confidencial; y de asegurar que dicha información es únicamente compartida entre las personas autorizadas en conformidad a esta política.
- **Disponibilidad:** Asegurar que los sistemas de tecnología de la información (TI) y los activos de información necesarios, están disponibles para ser utilizados en el momento que son requeridos únicamente para las personas autorizadas.
- **Integridad:** Asegurar que la información es auténtica y completa. Proveer el suficiente nivel de confianza de que la información es lo suficientemente precisa para el propósito requerido.
- **Documento digital (DD):** Toda representación de hecho, imagen o idea, incluyendo activos de información, que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior. Se excluye de esta definición a todo archivo digital que contenga lógica de programación en su contenido, como por ejemplo macros en Excel.
- **Documento físico (DF):** Todo activo de información que contenga datos registrados por escrito y en soporte de papel, tales como comprobantes de caja, documentos de control operativo, documentos activos, documentos pasivos, documentos para archivo físico, entre otros.
- **Segundo nivel de autorización:** Autorización adicional obligatoria requerida para poder ganar acceso a áreas restringidas.
- **Usuarios:** Personas naturales que pueden hacer uso de ciertos servicios que ofrece TISAL, sea en su condición de clientes, pacientes, afiliados(as) o por cualquier otra razón.

8. Referencias

- Alcance del SGSI
- Manual del SGSI
- Reglamento Interno de Orden, Higiene y Seguridad

9. Generalidades

9.1. Introducción

TISAL[3] requiere que se creen, apliquen y mantengan los controles de seguridad adecuados para proteger la confidencialidad, integridad y disponibilidad de la información de la empresa, incluyendo, pero no limitado a información y datos relativos a:

- Nuestros(as) colaboradores(as), personas a las que prestamos servicios y nuestra compañía (en adelante la nombraremos como "Información de la Compañía").
- Sistemas de TI, sitios web, aplicaciones, infraestructura, equipos como teléfono, correo de voz, hardware, software, así como el uso de sistemas de tecnología de la información de la organización y comunicaciones electrónicas como correo electrónico, intranet, internet y redes, como topología, protocolo y arquitectura (en lo sucesivo denominados conjuntamente "Sistemas de tecnología de la información de la empresa").

Esta "Política de Seguridad de la Información Corporativa", en conjunto con las Normas de Seguridad de la Información, definen los controles de seguridad requeridos colectivamente para dar cumplimiento al marco normativo vigente en lo que respecta al gobierno de seguridad de la información basado en ISO 27001:2022.

9.2. Cumplimiento de la Política

Considerando la importancia que reviste para la empresa el cumplimiento del marco normativo y lineamientos institucionales en materia de seguridad de la información, si la organización determina que un(a) colaborador(a) ha violado esta política, este(a) puede estar sujeto a sanciones laborales según lo establecido en el "Reglamento Interno de Orden Higiene y Seguridad", las que, según la gravedad de la infracción cometida, pueden incluir la terminación del contrato individual de trabajo respectivo. Lo anterior, sin perjuicio de las acciones judiciales que puedan dirigirse contra el(la) transgresor(a) para hacer efectiva su responsabilidad tanto civil como penal.

Los factores para tener en cuenta al evaluar las posibles sanciones incluyen, pero no se limitan, a los siguientes:

- El alcance de la violación.
- La naturaleza de la violación (conducta accidental, inadvertida o intencional).
- El daño o riesgo potencial creado por la divulgación para las personas cuya información fue liberada, la entidad o personas afectadas (considerándose particularmente graves las infracciones que conciernan a información de afiliados(as) o pacientes o que de alguna forma comprometa información comercialmente sensible de la organización).

[3] En adelante e indistintamente mencionada como, la "Compañía", "Organización" y/o "Empresa".

- El hecho de que el(la) colaborador(a) haya informado de la situación a los(as) encargados(as) correspondientes tan pronto tuvo conocimiento de los hechos y si colabora en las auditorías o investigaciones internas que puedan iniciarse en relación a los hechos informados.
- Eventual reiteración, en caso de haberse registrado por parte del(la) colaborador(a) una conducta errónea repetida o intencional o violaciones de las políticas y procedimientos de la organización.

Los(as) colaboradores(as) son responsables de plantear con prontitud cualquier preocupación sobre posibles violaciones de esta política. Si un(a) empleado(a) es consciente de una situación que él o ella cree que puede estar violando esta política o que de alguna otra manera puede resultar contraria a la ley o la normativa aplicable, debe ponerse inmediatamente en contacto con cualquiera de los siguientes recursos:

- Responsable de la Seguridad de la Información (CISO).
- Responsable de Cumplimiento (Compliance).
- Área de Seguridad de la Información Corporativa.
- También puede notificar mediante un correo electrónico a la casilla CSIRT@empresasbanmédica.com.

Los casos reales o sospechosos de posibles incidentes de seguridad se deben notificar al(la) Responsable de Seguridad de la información para la respuesta a incidentes de seguridad en conformidad al programa de gestión de riesgos del Área de Seguridad de la Información Corporativo y los planes de continuidad del negocio y recuperación ante desastres, para su investigación y seguimiento.

9.3. Restricciones Particulares o Especiales

Al haber distintas funciones y roles que manejan información confidencial, las Gerencias podrán disponer, en caso de que lo estimen necesario, mayores restricciones en su unidad o área que las disposiciones de esta política, en cuyo caso prevalecerá la más exigente.

9.4. Disposiciones de la Política

9.4.1. Gestión del Programa de Seguridad

- El Área de Seguridad de la Información tiene la responsabilidad de desarrollar, documentar, mantener y comunicar un programa integral de seguridad de la información corporativo. La autoridad y la responsabilidad de administrar el programa de seguridad de la información corporativo se delegan en el(la) Director(a) de Seguridad de la Información (CISO).
- La misión del Área de Seguridad de la Información Corporativa es proteger la confidencialidad, integridad y disponibilidad de la información de la organización. Esto incluye crear, administrar, comunicar y supervisar la Política.

9.4.2. Evaluación y Gestión de Riesgos

- El programa de gestión de riesgos del Área de Seguridad de la Información Corporativo proporciona información de análisis de riesgos precisa y relevante que facilita la toma de decisiones consistentes de gestión de riesgos. Las decisiones de gestión de riesgos se tomarán en colaboración con el liderazgo legal, empresarial, de tecnologías de la información y del Área de Seguridad de la Información Corporativa para optimizar el equilibrio entre las necesidades operativas del negocio y los requisitos legales, reglamentarios, de cliente(a) y de seguridad.
- Las evaluaciones de riesgos se realizan para determinar los controles de seguridad requeridos en función del uso y el riesgo, así como la normativa legal, reglamentaria, de seguridad del(la) cliente(la) y de seguridad de la información aplicable.

9.4.3. Seguridad del Personal

- Las responsabilidades de seguridad y de los(as) colaboradores(as) se deben definir, comunicar, evaluar y supervisar adecuadamente para mitigar el riesgo de error, robo, fraude, pérdida o uso indebido de la información de la empresa y de los sistemas de tecnología de la información de la empresa.
- Los(as) colaboradores(as) deben cumplir con la “Política de Seguridad de la Información Corporativa”, incluidos los requisitos de las normas de seguridad para un uso aceptable de los sistemas de tecnología de la información de la empresa.
- De forma regular, los(as) colaboradores(as) deben reconocer sus responsabilidades de seguridad, tal como se define en la “Política de Seguridad de la Información Corporativa”.
- Supervisamos, de acuerdo con las leyes vigentes y aplicables, todas las actividades en los sistemas de tecnología de la información de la Empresa.

9.4.4. Seguridad Física

- La información de la empresa, los sistemas de tecnología de la información de la empresa y las áreas seguras deben estar protegidas contra el acceso físico no autorizado.
- El Área de Seguridad de la Información en conjunto con las áreas pertinentes definirán los controles para proteger la infraestructura tecnológica ubicada en instalaciones bajo el control de la compañía contra riesgos ambientales razonables, para preservar la salud y la seguridad de los(as) trabajadores(as) y terceros de la compañía.
- El Área de Seguridad de la Información en conjunto con las áreas pertinentes implementarán controles ambientales adecuados para el correcto funcionamiento y disponibilidad de la información de la empresa, de los activos de información y de los sistemas de tecnología de la información (TI) de la Empresa.

9.4.5. Seguridad de Operaciones

- Los sistemas de tecnología de la información (TI) de la empresa se deben configurar, operar y administrar de manera controlada para proteger la confidencialidad, integridad y disponibilidad de la información de la empresa.
- Los hardware y software que deben ser aprobados antes de su uso dentro de la organización por parte del Área de Seguridad de la Información.
- El hardware y el software deben ser soportados formalmente a través del Área de Infraestructura Corporativa, incluyendo el mantenimiento regular y las actualizaciones periódicas.

9.4.6. Registro, Monitoreo y Gestión de Incidentes

- Los sistemas de tecnología de la información (TI) de la empresa se deben supervisar para detectar eventos operativos, de seguridad y de sistema que puedan afectar la confidencialidad, integridad y disponibilidad de la información de la Empresa.
- Los incidentes de seguridad se deben administrar mediante una capacidad de respuesta documentada, que incluye procedimientos para notificar, analizar, escalar, investigar y resolver incidentes de seguridad de manera oportuna, todo en conformidad al programa de gestión de riesgos del Área de Seguridad de la Información Corporativo y los planes de continuidad del negocio y recuperación ante desastres de la compañía.

9.4.7. Seguridad de la Comunicación

- La confidencialidad, integridad y disponibilidad de la información de la empresa y activos de información se debe proteger, cuando se comunique, a través de las técnicas y mecanismos determinados e informados de tiempo en tiempo al interior de la compañía por parte del Área de Seguridad de la Información.
- La transmisión de la información de la empresa se debe realizar de acuerdo con los requisitos normativos y contractuales que se encuentran vigentes y son aplicables, además la “Política de Seguridad de la Información Corporativa”.

9.4.8. Control de Acceso, Administración de Acceso e Identificación y Autenticación

- El acceso a la información de la empresa y a los sistemas de tecnología de la información (TI) y a los activos de información de la empresa deben ser sujeto a control de acceso y autenticación.
- El acceso se debe limitar a la cantidad mínima necesaria para realizar las tareas asignadas.

9.4.9. Seguridad de la Red

- Las redes de la organización, y la capacidad de conectarse a los sistemas de tecnología de la información de la empresa, deben ser administradas y controladas.
- Todas las conexiones a sistemas de tecnología de la información que no sean de la empresa deben estar aprobadas por el Área de Seguridad de la Información y cumplir con los requisitos de seguridad que éste determine y comunique como aplicables al interior de la Compañía.

9.4.10. Seguridad de Partes Externas o Terceros

- Las redes de la organización, y la capacidad de conectarse a los sistemas de tecnología de la información de la empresa, deben ser administradas y controladas.
- La organización debe gestionar los riesgos presentados al permitir que entidades externas que no sean afiliadas de la organización (“Partes Externas” o “Terceros”) accedan a la información de la empresa o a los sistemas de tecnología de la información de la empresa.
- Las partes externas o terceros podrán acceder a la información de la empresa, a los activos de información o a los sistemas de tecnología de la información de la empresa en el contexto de un acuerdo contractual formal que establezca los requisitos y responsabilidades de seguridad apropiados de la parte externa o tercero, los cuales no podrán ser inferiores a los establecidos en esta política.
- Los dispositivos en uso por las partes externas o terceros deben ser revisados y aprobados por el Área de Seguridad de la Información antes de estar conectados a los sistemas de tecnología de la información de la empresa.

9.4.11. Seguridad en el Desarrollo de Aplicaciones

- Las aplicaciones de la empresa se deben diseñar, implementar y administrar para proteger la confidencialidad, integridad y disponibilidad de los sistemas de tecnología de la información de la empresa, los activos de información y la información de la empresa.
- El software y el código de la aplicación deben estar protegidos contra modificaciones no autorizadas.

9.4.12. Continuidad del Negocio y Recuperación Ante Desastres

- La organización debe desarrollar, probar y mantener planes de continuidad del negocio y recuperación ante desastres con el fin de mitigar el impacto causado por interrupciones en las operaciones críticas del negocio, y para permitir una recuperación eficiente y efectiva. Los planes de continuidad del negocio y recuperación ante desastres incluirán procesos y controles para proteger el negocio de la organización, la vida y la seguridad de los(as) colaboradores(as), así como para proteger la imagen, la reputación, los activos y los recursos de la organización.

- Los requisitos de continuidad del negocio y recuperación ante desastres están determinados por los riesgos empresariales, las obligaciones legales, reglamentarias y contractuales, y los posibles impactos comerciales de las interrupciones del servicio, entre otros que determine el Directorio.

9.4.13. Clasificación y Protección de Datos

- La información utilizada o mantenida por la organización debe ser recopilada, utilizada, mantenida y divulgada solo por las personas autorizadas y sólo en las oportunidades y medida permitidas, siempre de acuerdo con todas las leyes y regulaciones vigentes y aplicables, las políticas de la organización y, si también es aplicable, autorizaciones individuales más estrictas o contratos con clientes.
- La información utilizada o mantenida por la organización se debe clasificar de acuerdo con las definiciones de nivel de clasificación de datos de la organización. Estas definiciones proporcionan orientación sobre las formas apropiadas de manejar y proteger la información de la empresa con el fin de proteger su confidencialidad, integridad y disponibilidad.

9.4.14. Seguridad en la Nube

- La organización debe asegurar que cuando se adquiera un servicio en la nube, este cumpla con los requisitos comerciales, con las leyes y regulaciones vigentes y aplicables, además de la “Política de Seguridad de la Información Corporativa”. Se debe establecer dónde implementar los controles de seguridad, además de los requisitos adicionales para poder respaldar y gestionar los riesgos presentes en los entornos en la nube.

9.5. Aspectos de Control

De acuerdo con la definición estratégica de TISAL, la presente política se adopta como apoyo al cumplimiento del marco normativo de Seguridad de la Información, la evaluación anual de los controles de seguridad definidos en la Política y Normas de Seguridad de la Información, con la finalidad de fortalecer de manera continua el Sistema de Gestión de Seguridad de la Información SGSI.

9.6. Publicación del Alcance del SGSI

PROCESO DE ACTUALIZACIÓN

Para garantizar que la publicación del alcance del SGSI se mantenga actualizada se efectuaran las siguientes gestiones:

- **Revisión Periódica de la Política:** El(la) Responsable de Seguridad de la Información (CISO) revisará el contenido publicado al menos una vez al año.
- **Actualización por Cambios:** Cualquier modificación en el alcance del SGSI desencadenará una actualización inmediata en todos los medios de publicación.
- **Proceso de Aprobación:** Todas las actualizaciones del alcance publicado deberán ser aprobadas por la alta dirección antes de su difusión.
- **Notificación de Cambios:** Se implementará un sistema de notificación para informar a las partes interesadas sobre cualquier actualización significativa en el alcance del SGSI.
- **Registro de Versiones:** Se mantendrá un registro las versiones anteriores del alcance publicado, incluyendo las fechas de vigencia y los cambios realizados.
- **Feedback:** Se establecerá un mecanismo para que las partes interesadas puedan proporcionar comentarios o solicitar aclaraciones sobre el alcance publicado.

TOMA DE CONCIENCIA DEL SGSI

El programa de toma de conciencia del Sistema de Gestión de Seguridad de la Información (SGSI) de TISAL tiene como objetivos:

- Asegurar que todos(as) los(as) empleados(as) y partes interesadas relevantes comprendan la importancia del SGSI.
- Promover la comprensión de la contribución individual a la eficacia del SGSI.
- Fomentar una cultura de seguridad de la información en toda la organización.
- Reducir los incidentes de seguridad causados por falta de conocimiento o negligencia.

MEDIOS DE CONCIENTIZACIÓN

Se implementarán los siguientes métodos para fomentar la toma de conciencia sobre el SGSI:

a) Capacitaciones:
   - Inducción para nuevos(as) empleados(as) sobre el SGSI.
   - Cursos normativos e-learning anuales de actualización para todos(as) los(as) colaboradores(as).

b) Comunicaciones Internas:
   - Correos electrónicos mensuales con consejos y recordatorios sobre prácticas seguras.
   - Publicación de infografías y posters en áreas comunes.

c) Simulacros y Ejercicios Prácticos:
   - Simulaciones de phishing para evaluar la conciencia de seguridad.
   - Ejercicios de respuesta a incidentes.

10. Excepciones

Para la "Política de Seguridad de la Información Corporativa" no se presentan excepciones para su cumplimiento.