M-SGI-002

Manual de Políticas del SGI

Responsables

Elaboró:	Líder del Sistema de Gestión Integral
Revisó:	Control de Documentos
Aprobó:	Gerente de Cumplimiento y Mejora continua

Control de versiones

Versión	Fecha	Descripción del cambio
1	04/02/2019	Emisión inicial
2	28/05/2019	Modificación en el alcance, política 9.1 Política de Control de Acceso Lógico, 12.3 Política de respaldo
3	07/06/2019	Modificación a la política 15 Relación con proveedores
4	09/06/2020	Actualización del manual de políticas del SGI con base en las mejoras identificadas (uso de medios removibles, canales seguros, especificación de roles para la solicitud de accesos y perfiles).
5	11/08/2021	Actualización de políticas de respaldo, revisión por proceso de FIRST (CSIRT), acceso VPN, se modifica el área de “Ciberseguridad” por “Ciberinteligencia”, se elimina el puesto “analista de alianzas” se modifica por “área de alianzas”, se realiza revisión general del área de operaciones. RAC94
6	22/11/2021	Inclusión de periodicidad para la ejecución de pruebas de vulnerabilidad
7	12/05/2022	Revisión y actualización derivada de auditoría interna RAC 106, 107
8	13/05/2022	Inclusión de políticas en el apartado 14, derivado de la revaluación de riesgo.
9	12/08/2022	Actualización de Formato, e implementación del SGCN ISO 22301

Clave del formato de procedimiento: F-SGI-004 v3
Comentarios o dudas: sgi@silent4business.com

Contenido

1. Introducción

Este Manual define las políticas y lineamientos específicos de Seguridad de la Información y de Continuidad del Negocio, los cuales son de observancia general para Silent4Bussiness. Constituye la base normativa para proteger la Confidencialidad, Integridad y Disponibilidad de la información.
Cabe mencionar que el presente documento está alineado a estándares internacionales de Seguridad de Información, como lo son ISO/IEC 27001:2013 "Seguridad de Información – Requerimientos, Requisitos del sistema de Gestión del Servicio ISO/IEC 20000-1:2018."

2. Alcance

El Manual de Políticas de Seguridad de la Información y de Continuidad aplica a todo el personal que participa en el desarrollo de las actividades definidas en el alcance del SGI; y que tenga acceso a información de la organización para su consulta, procesamiento, almacenamiento y/o transmisión.

3. Definiciones

Activo: Cualquier elemento que tenga valor tangible o intangible para la organización.

Administración de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos que afrontan. La administración de riesgos incluye la evaluación de riesgos, su tratamiento, aceptación y comunicación.

Alta Dirección: Rol cubierto por la Dirección General de Silent4Business

Amenaza: Causa potencial de un incidente no deseado que puede provocar daños a uno o más activos, procesos, servicios de la organización.

Análisis de riegos: Método analítico de la administración de riesgos que permite la identificación de vulnerabilidades y amenazas de seguridad y de los servicios, así como la evaluación de la magnitud o impacto de los daños a efecto de determinar dónde sería necesaria la implementación de controles y la cantidad máxima razonable de recursos que sería necesario invertir.

Confidencialidad: Principio de Seguridad de la Información que consiste en asegurar que el acceso al activo únicamente se realiza por los autorizados y a través de los procedimientos establecidos para ello.
Control Recurso aplicado para mitigar el riesgo.

Disponibilidad: Principio de Seguridad de la Información que estipula que el activo puede ser utilizado por los autorizados cuando éstos lo requieran.

Integridad: Principio de Seguridad de la Información que consiste en que el activo sólo puede ser modificado por los autorizados.

Organización: Para propósitos del Sistema de Gestión Integral se entiende por la organización a Silent4Business, S.A. de C.V.

Procedimiento Forma específica de desarrollar una actividad paso a paso. Los procedimientos están documentados.

Proceso: Es un conjunto de actividades que suceden de forma ordenada a partir de la combinación de materiales, equipo, gente, métodos y medio ambiente, para convertir insumos en productos o servicios con valor agregado.

Registro: Documento que presenta resultados obtenidos o proporciona evidencia de actividades desempeñadas.

Responsable del SGI: Rol cubierto por el responsable de mantener y mejorar el SGI.

Riesgo: Resultado de multiplicar la probabilidad de un evento por su impacto o consecuencia.

Riesgo Residual: Es el riesgo que permanece después de que la organización realiza el tratamiento de los riesgos identificados como parte de la Administración de Riesgos, es decir, es el riesgo que permanece después de implementar los controles seleccionados.

Seguridad de la Información: Preservación de la Confidencialidad, Integridad y Disponibilidad de la información.

SGI: Sistema de Gestión Integral.

Sistema de Gestión Integral: Es el conjunto de directrices generales y de operación para Silent4Business, el marco metodológico de referencia utilizado para garantizar la efectividad del SGI, es el siguiente:
•ISO 9001:2015 Sistemas de Gestión de la Calidad – Requisitos.
•ISO/IEC 20000-1:2018 Sistemas de Gestión de Servicios TI – Requisitos.
•ISO/IEC 27001:2013 Sistemas de Gestión de Seguridad de la Información – Requisitos.

SoA: Declaración de Aplicabilidad (Statement of Applicability, SoA por sus siglas en inglés).
Tratamiento del Riesgo Proceso de selección e implementación de controles para modificar el riesgo.

Vulnerabilidad: Debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas comprometiendo en consecuencia la confidencialidad, integridad y disponibilidad de la información o de los activos.

4. Descripción del manual

5. Políticas de Seguridad

5.1 Política de Seguridad de la Información

"En Silent for Business proveemos Soluciones Integrales de Ciberinteligencia, manteniendo los estándares de Calidad, Seguridad de la Información propia y de terceros; cumpliendo con los Niveles de Servicio acordados para su entrega, así como los requisitos legales aplicables, con la finalidad de lograr la satisfacción de nuestros Clientes y promover una cultura de mejora continua en el Sistema de Gestión Integral alineada a los objetivos de negocio".

La política del SGI es revisada de forma anual en las sesiones de planeación estratégica o en caso de algún cambio significativo en la organización que impacte al SGI.

Para facilitar la comunicación se apoya de diferentes medios, tales como cuadros, pantallas, mesa digital, comunicados, cursos e inducciones y campañas especiales.

Lineamientos específicos:

1. Las políticas de Seguridad de la Información deben revisarse al menos una vez al año a fin de garantizar que se mantienen actualizadas y son adecuadas y efectivas para los propósitos de la Organización.
2. El manual de políticas de Seguridad de la Información debe permanecer disponible para consulta a través de los medios disponibles para tal efecto a todo el personal que labora en la Organización y que forma parte del Sistema de Gestión Integral.

Controles de ISO 27001:2013 cubiertos

Esta política cubre los siguientes controles específicos de seguridad de información del Anexo A de ISO 27001:2013:

Política de Seguridad de la Información	
Control	**Nombre del Control**
A.5.1.1	Documento de política de seguridad de información.
A.5.1.2	Revisión de la política de seguridad de información.

6. Organización de la Seguridad de la Información

6.1 Política para la Organización Interna

Lineamientos específicos:

1. Todas las áreas dentro del alcance del SGI conocen sus responsabilidades dentro de las funciones de su puesto, para cumplir con los objetivos de seguridad y los requerimientos de la organización.
2. La Alta Dirección en coordinación con los Directores y Gerentes, deben formular, revisar, aprobar, e implementar políticas de Seguridad de la Información, así como proporcionar los recursos necesarios e iniciar planes y programas para mantener los conocimientos de Seguridad de la Información.
3. Las actividades de Seguridad de la Información deben ser coordinadas mediante reuniones por los representantes de diferentes áreas de la organización con funciones y roles relevantes para asegurar el cumplimiento con las políticas de Seguridad de la Información e identificar cambios o amenazas a las que se encuentre expuesta la información.
4. Todo el personal de la Organización incluido en el alcance del SGI debe cumplir con las Políticas de Seguridad de la Información.
5. Todo el personal debe conocer sus responsabilidades con respecto al uso que le den a los sistemas de información, a los equipos de cómputo y la información que manejan.
6. Todo el personal debe estar plenamente consciente de sus obligaciones laborales y legales, además de sus responsabilidades relacionadas con la Seguridad de la Información y continuidad de las operaciones con compartir y divulgar inapropiadamente información, tanto al interior de la organización como con externos.
7. Cualquier adquisición de mecanismos de procesamiento de información (hardware y software) debe ser aprobado por el personal autorizado a fin de garantizar que es compatible con la infraestructura actual de la Organización y que no represente un riesgo para la Seguridad de la Información.
8. Los colaboradores deben utilizar únicamente los equipos y mecanismos de procesamiento de información que la misma le proporcione para el desempeño de sus funciones, quedando prohibido el uso de equipo personal. Evaluando aquellos escenarios específicos para su autorización.
9. Todo el personal que labora en la organización debe contar con un acuerdo de confidencialidad de información firmado.
10. Se debe mantener un listado actualizado de contactos con autoridades relevantes u otras organizaciones (p.ej. protección civil, policía, bomberos, etc.) que puedan proporcionar apoyo, en caso de requerirse.
11. Se debe mantener contacto con grupos de especialistas en aspectos de seguridad de información (foros, asociaciones, comités, membresías, etc.), a fin de mejorar el conocimiento, permanecer actualizados en temas relevantes de seguridad de información, recibir información pronta y oportuna sobre nuevas vulnerabilidades e intercambiar información y experiencia.
12. Las responsabilidades referentes a la seguridad de información, así como la implementación del SGI (controles, políticas, procesos y/o procedimientos de seguridad de información) deben ser

revisados al menos una vez al año de manera independiente por personal que no esté involucrado en el alcance del Sistema, o siempre que ocurran cambios significativos a la implementación del SGI, como parte de la auditoría interna al SGI.

Controles de ISO 27001:2013 cubiertos

Esta política cubre los siguientes controles específicos de seguridad de información del Anexo A de ISO 27001:2013:

Política para la Organización Interna	
Control	**Nombre del Control**
A.6.1.1	Funciones y responsabilidades de Seguridad de la Información.
A.6.1.2	Segregación de funciones.
A.6.1.3	Contacto con las autoridades.
A.6.1.4	Contacto con los grupos de interés especial.
A.6.1.5	Seguridad de la Información en la gestión de proyectos.

6.2.1 Política de Dispositivos Móviles

Se deben establecer medidas de seguridad apropiadas para proteger la información de los riesgos de utilizar cómputo móvil fuera de las instalaciones.

Lineamientos específicos

1. Todos los equipos de cómputo móvil de la organización que sean utilizados fuera de las instalaciones deben tener fondo de pantalla y bloqueo a los 5 minutos después de un periodo de inactividad, así como, tener instalado, actualizado y activado el software antivirus de la organización.

2. Cuando el usuario deba dejar desatendido su equipo de cómputo móvil, debe bloquearlo o finalizar sesión con el fin de evitar accesos no autorizados al mismo y a la información a la que por su perfil pudiera tener acceso.

3. Toda la información contenida en los equipos de cómputo móvil debe respaldarse periódicamente de acuerdo con el procedimiento de respaldos.

4. Se deben utilizar técnicas de cifrado de información para los equipos de cómputo de directores, Gerentes de área y Administradores de proyectos de la organización que sean utilizados fuera de las instalaciones con el fin evitar robo y/o acceso no autorizado a la información contenida en los equipos.

5. Deben considerarse los accesorios necesarios para conservar la integridad física de los equipos portátiles; así como su robo o extravío, a través de candados o anclajes al mobiliario en medida de lo posible.

6. Los usuarios que se les asigne equipos portátiles deben ser responsables del uso de los mismos considerado los siguientes puntos:
   - Cuidado físico del equipo.
   - Información contenida.
   - Software instalado.
   - Configuración del equipo.
   - Hardware.

7. Siempre que sea posible, deben evitarse medios de transporte públicos para la transportación de los equipos portátiles.

8. No está permitido el préstamo o intercambio de equipos portátiles por parte de los usuarios.

9. Cuando se viaje con equipos móviles se deben llevar como equipaje de mano (no documentar).

10. No se debe dejar el equipo móvil desatendido en lugares públicos.

11. Evitar dejar el equipo móvil en un lugar visible dentro del automóvil con el fin de evitar el robo del equipo y compromiso de la información ahí contenida.

12. La conexión que se realice en redes públicas queda bajo responsabilidad del usuario, en caso de poner en riesgo el equipo y su información será sujeto de sanciones.

13. Ningún usuario debe intentar reparar el equipo, en caso de presentarse cualquier tipo de falla debe reportarlo de inmediato a Soporte Interno.

14. No está autorizado que los usuarios configuren el software y ni el hardware ya instalado en los equipos o dispositivos móviles.

15. No está autorizado que los usuarios bajen software ni contenido de Internet que ostente derechos de autor (fotografías, vídeos, libros, etc.) para instalarlo o mantenerlo en los equipos portátiles.

16. Soporte interno correspondiente debe revisar al menos una vez al año los equipos portátiles para eliminar cualquier aplicación, programa o archivo sospechoso.

17. La comunicación para los usuarios remotos debe ser a través de VPN’s.

18. La organización se reserva el derecho de monitorear y revisar los equipos o dispositivos de cómputo móvil en cualquier momento que lo considere pertinente.

19. El personal que tenga asignado celulares deberá apegarse a las políticas establecidas en la responsiva (F-GET-027).

20. El personal que configure su correo electrónico en su equipo celular personal será responsable de establecer medidas de protección para el desbloqueo del mismo, así mismo, queda prohibido el envío de información personal a través de la cuenta laboral, o enviar información laboral a cuentas personales.

Controles de ISO 27001:2013 cubiertos

Esta política cubre los siguientes controles específicos de seguridad de información del Anexo A de ISO 27001:2013:

Política de Dispositivos Móviles	
Control	**Nombre del Control**
A.6.2.1	Política sobre dispositivos móviles.

6.2.2 Política de Teletrabajo

Se deben establecer medidas de seguridad apropiadas para proteger la información de los riesgos de utilizar cómputo móvil fuera de las instalaciones.

Lineamientos específicos

1. El Gerente de Operaciones debe garantizar la seguridad del teletrabajo y el uso de dispositivos móviles de Silent4Business.
2. Se debe documentar e implementar medidas de seguridad de soporte, tales como respaldos para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.
3. El home office se aplica en caso de contingencias para los colaboradores que de acuerdo con su rol así lo determine el negocio/Área, previo visto bueno de Dirección General, quiénes deberán apegarse a las políticas de home office establecidas M-GET-009.

Esta política cubre los siguientes controles específicos de seguridad de información del Anexo A de ISO 27001:2013:

Política de Teletrabajo	
Control	**Nombre del Control**
A.6.2.2	Teletrabajo (Políticas Home Office).

7. Seguridad en Gestión de Talento

7.1 Política de Seguridad en Gestión de Talento (Antes de la contratación)

Todo el personal que labora en la organización debe pasar por un proceso de seguridad de información en Gestión de Talento previo a su contratación.

Lineamientos específicos

4. Los roles y responsabilidades con respecto a la Seguridad de Información deben estar definidas en las descripciones de puesto.
5. Los colaboradores deben cumplir, como parte de sus obligaciones contractuales, con la normatividad interna que se establezca (manuales, políticas, procedimientos, etc.).
6. El área de Gestión de Talento debe contar con la siguiente información del personal que contrata y que labora o presta sus servicios para la organización:
    - Verificar la identidad del candidato al puesto.
    - Verificar que la información contenida en el Curriculum Vitae sea verdadera.
    - Verificar referencias (personales, de trabajo, académicas).
    - Cartas de recomendación de al menos 2 últimos empleos.
    - Antecedentes no penales.
    - Estudio socioeconómico.
    - Estado de cuenta.
    - Número de seguro social.
7. Se debe proteger la privacidad de la información recabada del personal de la organización.
8. Como parte de contrato se deben especificar los términos y condiciones de empleo para el personal de la organización.

Controles de ISO 27001:2013 cubiertos

Esta política cubre los siguientes controles específicos de seguridad de información del Anexo A de ISO 27001:2013:

Política de Seguridad en Gestión de Talento (Antes de la contratación)	
Control	**Nombre del Control**
A.7.1.1	Detección.
A.7.1.2	Términos y condiciones de contratación.

7.2 Política durante el empleo

Todo el personal que labora en la organización debe pasar por un proceso de seguridad de información en Gestión de Talento durante el tiempo que preste sus servicios a la organización.

Lineamientos específicos

1. El jefe inmediato superior debe asegurarse que el personal a su cargo cumpla con sus funciones y responsabilidades para las cuales fue contratado.
2. Es responsabilidad de los colaboradores entender y apegarse a las políticas establecidas dentro del presente manual.
3. En caso de incumplimiento a la normatividad interna establecida por la organización (manuales, políticas, procedimientos, etc.), se deben aplicar las acciones disciplinarias correspondientes, apegándose a la Ley Federal del Trabajo.

Controles de ISO 27001:2013 cubiertos

Esta política cubre los siguientes controles específicos de seguridad de información del Anexo A de ISO 27001:2013:

Política Durante el Empleo	
Control	**Nombre del Control**
A.7.2.1	Administración de responsabilidades.
A.7.2.3	Proceso disciplinario.

7.2.2 Política de concienciación, educación y capacitación en Seguridad de la Información

Todo el personal que labora en la Organización, y cuando sea relevante, los proveedores y terceras partes deben recibir apropiada concientización y capacitación de manera regular para mantenerse actualizados en las políticas y procedimientos de Seguridad de la Información de la organización.

Lineamientos específicos

1. Se deberá apegarse al plan de capacitación interna de la organización asegurándose que se integren temas de concientización, educación y capacitación en Seguridad de la Información.

2. Todo el personal de la organización debe recibir difusión, concientización y capacitación constante en temas referentes a la Seguridad de la Información, así como material de referencia para permitirles la correcta protección de la información.

3. Cumplimiento y Mejora Continua debe proveer los cursos y material necesarios para actualizar regularmente a los colaboradores, con la finalidad de informarlos sobre sus obligaciones con respecto a la Seguridad de la Información.

4. Cada colaborador debe leer, comprender, respetar y cumplir las políticas, lineamientos y procedimientos de seguridad de información.

5. Todo colaborador debe atender los entrenamientos de concientización en la Seguridad de la Información posterior a su ingreso. Para contar con la evidencia de que se asistió a dicho entrenamiento. Se deberá realizar una plática de reforzamiento a todo el personal al menos una vez por año.

Controles de ISO 27001:2013 cubiertos

Esta política cubre los siguientes controles específicos de seguridad de información del Anexo A de ISO 27001:2013:

Política de Capacitación en Seguridad de la Información	
Control	**Nombre del Control**
A.7.2.2	Concientización, capacitación y educación de seguridad de información.

7.3 Política después del empleo

Todo el personal que labora en la Organización debe pasar por un proceso de seguridad de información en Gestión de Talento una vez que se dé por terminada la relación laboral.

Lineamientos específicos

1. Gestión de talento debe comunicar al personal las responsabilidades de terminación del empleo los cuales deben incluir los requerimientos de seguridad establecidos y las responsabilidades legales, de acuerdo con el contrato firmado.

2. El responsable de área debe de comunicar los motivos por el cual el personal será desvinculado de la organización determinando el período durante el cual debe cumplir con las responsabilidades.

3. El personal interno que deje de laborar para la organización debe hacer entrega formal de los equipos, dispositivos, documentos corporativos, información y/o software que se le haya proporcionado como parte de sus funciones ejemplo: Activos de la organización, dispositivos de cómputo móvil, tarjetas de acceso, manuales e información almacenada en medios electrónicos también deben ser devueltos conforme al procedimiento de desvinculación del personal PR-GET-005.

4. Se debe llenar un formato de baja de resguardo una vez que se regresen los activos descritos en las mismas.

5. Los responsables de las áreas deben notificar a Gestión de talento cualquier cambio en la plantilla laboral (altas, bajas y cambios), a fin de reflejar dichos cambios en las cuentas de acceso, correo electrónico y telefonía, así como a vigilancia para evitar riesgos de accesos físicos no autorizados a las instalaciones de la organización, quien notificará a Soporte Interno para actualizar los accesos a los sistemas y aplicaciones correspondientes, de acuerdo con el procedimiento de movimientos de personal PR-GET-006.

6. Cuando ocurra la terminación del empleo, los derechos de acceso de esta persona hacia los activos asociados con sistemas de información y servicios deben ser bloqueados de manera temporal hasta tres meses. Cuando ocurran cambios de puesto, estos deben reflejarse en la cancelación de todos los derechos de acceso que no sean aprobados para el nuevo puesto. La cancelación o adaptación de los derechos de acceso incluye acceso físico y lógico, llaves, tarjeta de identificación, suscripciones y el retiro de cualquier documentación que identifique a la persona como miembro activo de la organización.

7. Se debe restringir el acceso tanto físico, como lógico al personal que fue desvinculado de la organización.

Controles de ISO 27001:2013 cubiertos

Esta política cubre los siguientes controles específicos de seguridad de información del Anexo A de ISO 27001:2013:

Política Después del Empleo	
Control	**Nombre del Control**
A.7.3.1	Cese o cambio de puesto de trabajo.

8. Manejo de Activos

8.1 Política de Responsabilidad sobre Activos

Todos los activos de información deben estar identificados y tener un propietario designado, quien será responsable de proteger la Seguridad de Información del activo. Así mismo se deben definir de una manera clara y precisa los lineamientos para el uso aceptable de los activos y la información de la Organización.

Lineamientos específicos:

1. Todos los activos de información críticos de la organización deben estar claramente identificados en un inventario de activos, el cual debe ser actualizado al menos una vez al año o cuando ocurran cambios de activos.

2. Todo activo de información debe tener asignado un propietario o dueño del mismo, quien debe responsabilizarse de su protección.

3. El área de Soporte Interno de la organización debe administrar y proporcionar los recursos necesarios (refacciones, equipo de cómputo, infraestructura TI y Software) al personal, con el fin de apoyar al óptimo desempeño de sus funciones.

8.1.1 Política sobre el uso aceptable de Activos

Se deben tener identificados, documentados e implementados lineamientos sobre el uso aceptable de los activos de información.

Lineamientos específicos:

1. Todo el personal al que se le asigna un equipo de cómputo o comunicaciones (laptop, Smartphone, etc.), debe firmar una carta responsiva, mediante el cual se hace responsable de su resguardo y buen uso.

2. Todo el personal, contratistas y terceros que tengan alguna relación laboral con la organización utilizarán los activos cumpliendo estrictamente con las medidas de seguridad especificadas y los controles establecidos por ésta.

3. Los activos y la información de la organización a la cual tienen acceso y uso el personal es únicamente para desempeñar las funciones para las cuales fueron contratados.

4. Todo el personal que labora en la organización debe estar consciente de la importancia de proteger los activos y mecanismos de procesamiento de información y de no hacer un mal uso de estos.

5. Los usuarios son responsables del buen uso de los activos proporcionados por la organización.

6. Se debe contar con espacio físico apropiado para almacenar documentos en papel (p. ej. Gavetas, archiveros, etc.) con el propósito de evitar accesos no autorizado y/o robo a dicha información.

7. Se debe respetar en todo momento la privacidad y los derechos de autor relacionados a los activos de información utilizados, generados u obtenidos por la organización.

8. El usuario de un equipo de cómputo deberá asegurarse que su equipo tiene activados los siguientes mecanismos de protección de acceso:
    - Contraseña de inicio de sesión.
    - Protector de pantalla con contraseña.

9. Está prohibido utilizar las hojas impresas con información confidencial para reciclaje.

10. Toda la información confidencial que se encuentre impresa debe destruirse físicamente mediante trituradora de papel.

11. Toda aquella conducta, comportamiento o acción que no esté expresamente permitida conforme a esta política se debe considerar como una prohibición.

Controles de ISO 27001:2013 cubiertos

Esta política cubre los siguientes controles específicos de seguridad de información del Anexo A de ISO 27001:2013:

Política Sobre la Responsabilidad sobre los activos	
Control	**Nombre del Control**
A.8.1.1	Inventario de activos
A.8.1.2	Propiedad de los Activos
A.8.1.3	Uso aceptable de los activos
A.8.1.4	Devolución de activos

8.2 Política de Clasificación de la Información

Toda la información debe estar clasificada para definir un apropiado nivel de protección e identificar las necesidades, prioridades y grado esperado de protección cuando se maneja dicha información.

Lineamientos específicos

1. De acuerdo con lo establecido el propietario de la información es el responsable de la clasificación de esta de acuerdo con las siguientes categorías:

    - ***Confidencial.*** Se clasifica así para la información cuya difusión pueda:

        - Comprometer la estabilidad y permanencia de la organización en el mercado. Ejemplos: Estrategias de negocio, nuevos proyectos, planes de crecimiento, estrategias de inversión, secretos comerciales e industriales, nómina, expedientes de clientes, contratos, etc.

        - Poner en riesgo la estrategia comercial de la Organización.

        - Poner en riesgo la vida, la seguridad o la salud de cualquier persona,

        - La que por disposición expresa de una Ley sea considerada confidencial, reservada, comercial reservada o gubernamental confidencial;

        - Los secretos comercial, industrial, fiscal, bancario, fiduciario u otro considerado como tal por una disposición legal;

    - ***Privada.*** Se considera como tal a:

        - La información que se genera de manera interna como parte de las actividades diarias, por lo tanto, puede tener acceso a ella el personal de la organización, pero no puede distribuirse libremente al exterior de esta. Ejemplos: Manuales, procesos, procedimientos, instructivos, políticas, comunicación interna, etc.

        - La información entregada con tal carácter por terceras partes a la organización;

    - ***Pública.*** Se considera como tal a aquella información que se puede divulgar sin restricciones al público en general siempre y cuando no exista ningún impedimento legal o normativo para ello. Ejemplos: trípticos, publicaciones en revistas, posters, publicidad, etc.

Estos niveles de clasificación aplican para el uso de información del equipo CSIRT, así como su interacción con otras comunidades.

2. Los criterios de valoración, clasificación y conservación de documentos o registros deben responder a las necesidades de la operación de la organización.

3. La clasificación de la información comercial para proyectos del sector público, es considerada de carácter público, a excepción de los costos que se determinen antes de dar por iniciado el proceso de licitación y/o estudio de mercado. La información técnica que derive de los proyectos adjudicados, será decisión del cliente determinar el grado de sensibilidad y protección de su información.

8.2.2 Política de etiquetado y manejo de Información

Se debe contar con lineamientos apropiados para el etiquetado y manejo de información de acuerdo con el esquema de clasificación definido por la organización.

Lineamientos específicos

1. Los medios de almacenamiento de cómputo (cintas magnéticas, CD-ROM's, DVD, USB, etc.) y documentos impresos que contengan información clasificada como confidencial debe estar identificados.
2. Se debe tener especial cuidado en el manejo y almacenamiento de información clasificada como confidencial o privada, a fin de evitar la pérdida, modificación y/o mal uso de ella.
3. La información clasificada como pública y privada no requiere estar etiquetada.
4. El almacenamiento de la información en cualquiera de los niveles de clasificación, deberá realizar a través de los repositorios oficiales de la organización. Tal como sharepoint y fileserver, los cuales deberán tener carpetas divididas para cada una de las áreas, los dueños de la información validarán que el acceso a su información sólo se encuentre disponible para las personas que ellos autoricen.
5. Toda la información que se transmita por medios electrónicos será asegurada de acuerdo con el nivel de clasificación. El dueño de la información será responsable de implementar las medidas de seguridad que considere pertinentes para la información confidencial, tales como: contraseña, cifrado, leyenda de confidencialidad, entre otros.
6. La información que se trasmita de manera impresa no estará necesariamente protegida cuando se trate de información pública o privada, en el caso de la información confidencial, la persona responsable de su uso o envío deberá considerar el uso de leyendas, cuando sea posible, deberá tener el cuidado necesario para evitar que sea vulnerada.
7. El acceso a la información interna en formato electrónico ya sea de nivel confidencial o privada, deberá estar protegida de un acceso no autorizado, mediante usuario y contraseña para los repositorios oficiales; será responsabilidad del área o persona dueña de la información asegurar que no se otorguen accesos no autorizados.

8. Para la información impresa clasificada como confidencial, será responsabilidad del dueño de la misma vigilar que no sea accedida por personas no autorizadas.
9. La eliminación de la información confidencial impresa deberá realizarse mediante la trituradora, para la información electrónica será mediante el procedimiento de soporte interno a fin de asegurar que se elimine de manera segura. En el caso de información pública o privada se realizará a consideración del dueño de la misma, siempre que evite un mal uso o acceso no autorizado.
10. El tiempo de retención de la información se deberá establecer en el control de documentos.
11. Los controles para la divulgación de información serán de acuerdo con el nivel de clasificación de esta, será responsabilidad del dueño de la información definir las personas autorizadas para acceder a la misma.

8.2.3 Política de Manejo de activos

Todos los medios deben controlarse y protegerse físicamente para prevenir exposición, modificación, eliminación o destrucción de la información e interrupción de las actividades del negocio

Controles de ISO 27001:2013 cubiertos

Esta política cubre los siguientes controles específicos de seguridad de información del Anexo A de ISO 27001:2013:

Política de Clasificación de la información	
Control	**Nombre del Control**
A.8.2.1	Clasificación de la información
A.8.2.2	Etiquetado de la información
A.8.2.3	Manejo de activos

8.3 Política de Manejo de Medios

Lineamientos específicos

1. Una vez que ya no sean requeridos los medios removibles propiedad de Silent (memorias USB, CD, etc.), deben ser revisados por cada usuario que lo utiliza para los fines requeridos, antes de ser eliminados o reasignados para garantizar que no contienen información confidencial o reservada.

2. El uso de USB's o memorias, para el personal de la organización está permitido únicamente como un medio de facilitar el manejo de la información.

3. La trasferencia de información debe utilizar mediante canales seguros de comunicación.

4. Se deberán establecer las medidas de seguridad en caso de requerir la copia de documentos con información confidencial por cualquier medio.

5. Los registros de Seguridad de la Información deben estar identificados, almacenados, protegidos y fácilmente recuperables.

6. La documentación de los sistemas debe estar protegida contra accesos no autorizados y resguardarse de manera segura.

Controles de ISO 27001:2013 cubiertos

Esta política cubre los siguientes controles específicos de seguridad de información del Anexo A de ISO 27001:2013:

Política de Manejo de medios	
Control	**Nombre del Control**
A.8.3.1	Gestión de medios Extraíbles
A.8.3.2	Retirada de soportes
A.8.3.3	Transferencia de medios físicos

9. Control de Accesos

9.1 Política de Control de Acceso Lógico

El acceso a la información y a los sistemas de información debe estar controlado con base a las necesidades del negocio y a los requerimientos de seguridad.

Se debe controlar el acceso a los servicios de red interna y externa. El acceso de los usuarios a la red no debe comprometer la seguridad de los servicios de red.

Lineamientos específicos

1. Se deben identificar a los usuarios que tienen que acceder a los sistemas, aplicaciones y servicios de red.

2. Las cuentas de acceso a los sistemas y aplicaciones son otorgadas de forma personal e intransferible y son los titulares de estas, los responsables directos del uso que se les dé y las actividades que con ellas se realicen.

3. Las cuentas de acceso deben ser personalizadas, es decir, que identifiquen de manera única al usuario.

4. Cuando el usuario detecte un mal uso de su cuenta de acceso debe notificarlo de manera inmediata a su jefe inmediato y a la gerencia correspondiente para que se cambie la contraseña de inmediato.

5. El acceso a los sistemas, aplicaciones y servicios de red deben otorgarse con base en el ID de usuario, los privilegios asignados y la contraseña de acceso, tomando como base el principio del mínimo privilegio (lo estrictamente necesario), de acuerdo con la necesidad de conocer información para el cumplimiento adecuado de sus funciones.

6. Todos los sistemas, aplicaciones y servicios de red de la organización deben ser accedidos mediante el uso de una cuenta de acceso (ID de usuario) y contraseña.

7. El responsable del área o dueño de proceso, es el único facultado para solicitar la generación de cuentas de usuario (incluyendo los privilegios asociados a la cuenta) para el personal a su cargo.

8. Se debe llevar un registro de todas las cuentas de acceso y privilegios asignados a los usuarios.

9. Los equipos de cómputo que por necesidades del servicio deban ser utilizados por más de un usuario, deben contar con perfiles personalizados por cada uno.

10. Se deben implementar los métodos de autenticación apropiados para controlar el acceso de usuarios remotos.

11. Se debe controlar el acceso físico y lógico a los puertos de configuración y diagnóstico remoto a fin de evitar mantener activa la conexión remota en todo momento y que se pudieran obtener accesos no autorizados.

12. La red interna de la Organización debe estar segmentada por medio de componentes de red; ya sea por usuarios, grupos, servicios o sistemas.

13. Los equipos externos deberán conectarse a la red de invitados, misma que se encuentra separa del segmento de red que resguarda la infraestructura corporativa.

14. Se deben de contar con segmentos seguros para los equipos críticos de la organización.

15. Las actividades relacionadas con la operación de la red interna en donde se encuentran ubicados los equipos de administración y monitoreo deben ser independientes de la red de datos de usuarios.

16. Los componentes de la red deben de contar con las configuraciones adecuadas de seguridad, con la actualización de parches y versiones indicadas por el proveedor.

17. Se deben tomar las medidas necesarias cuando se lleve a cabo cualquier expansión de la red para asegurar la protección de esta y de la información almacenada procesada y transmitida vía red.

18. Se debe garantizar que los componentes de la red interna de la organización tengan asignada una única y autorizada dirección de red.

19. El direccionamiento de red debe ser asignado con base en las actividades establecidas para la instalación y configuración de los componentes de red.

20. Siempre que se usen equipos móviles proporcionados por la organización se debe tener especial cuidado para asegurar que la información no se comprometa, teniendo en cuenta aspectos de seguridad física, control de acceso lógico, respaldos de la información contenida en el equipo, protección contra virus y código malicioso, entre otros.

Controles de ISO 27001:2013 cubiertos

Esta política cubre los siguientes controles específicos de seguridad de información del Anexo A de ISO 27001:2013:

Política de Control de Acceso Lógico	
Control	**Nombre del Control**
9.1.1	Política de control de acceso.
9.1.2	Acceso a redes y servicios de red.

9.2 Política de Gestión de Acceso de Usuario

La asignación de contraseñas debe estar controlada a través de un proceso formal de administración de contraseñas, así como también se debe controlar la asignación de los privilegios de acceso a los sistemas de información y servicios de la organización, cubriendo todo el ciclo desde el registro inicial de nuevos usuarios hasta el final hasta eliminar el registro de un usuario que ya no requiere el acceso a los sistemas de información y servicios.

Lineamientos específicos

1. Los derechos o privilegios de acceso para cada usuario o grupo de usuarios deben ser definidos y asignados de manera clara.

2. Las cuentas de acceso de los usuarios deben ser revisadas, a fin de que no existan cuentas activas de personal que ya no presta sus servicios en la Organización o que tenga privilegios que no sean acordes con el desempeño de sus funciones.

3. Se deben bloquear las cuentas después de 3 intentos fallidos dentro de 15 minutos consecutivos de acceso.

4. Si la cuenta de usuario ha sido bloqueada deberá solicitar a soporte interno el desbloquear.

5. Se deben bloquear las cuentas que hallan excedido la vigencia de 60 días y no hayan cambiado su contraseña.

6. El desbloqueo manual de cuentas sólo debe realizarse a petición expresa del usuario.

7. Se debe contar con un sistema de administración de passwords que garantice la calidad de estos, es decir, que sean passwords fuertes, seleccionados de acuerdo con lo establecido por Soporte Interno (longitud mínima de 10 caracteres, que contenga caracteres alfanuméricos, tiempo de vida de 42 días).

8. Soporte Interno debe revocar las cuentas de los usuarios cuando, el usuario ponga en riesgo la operación de la red, cuando el responsable del área lo considere necesario, o cuando la relación laboral entre el usuario y la organización se dé por terminada.

9. No se permite repetir las contraseñas por al menos 24 iteraciones.

10. Las contraseñas no deben ser enviadas en mensajes de correo electrónico o cualquier otra forma de comunicación electrónica o escrita.

11. Las contraseñas asociadas a una cuenta de administración por omisión (default) con privilegios especiales en los sistemas operativos tales como root, administrador, entre otros; deben ser cambiadas antes de que el sistema entre a producción, o en caso de que se hayan utilizado con fines de mantenimiento por un tercero al finalizar dicha actividad. Las contraseñas no deben ser compartidas con persona alguna por ninguna razón o circunstancia.

12. Para la creación de una contraseña se deben seguir las siguientes recomendaciones:

    - Las contraseñas no deben ser una palabra de uso común o contar con cualquiera de las siguientes características:
        - Nombres de la familia, mascotas, de amigos, de compañeros de trabajo, de animaciones, etc.

- Cumpleaños e información personal tal como direcciones y números telefónicos.
- Patrones de números o palabras como aaabbb, TQM, 12345, etc.
- No usar palabras de cualquier idioma, modismos, dialectos, etc.

- Se deben crear contraseñas que son fáciles de recordar y difíciles de adivinar. Una forma de hacer esto es crear una contraseña basada en un título de una canción, afirmación, o cualquier otra frase. Por ejemplo, la frase puede ser: “Esto puede ser una forma de recordarlo” y la contraseña podría ser: “EpS1Fdr!” o “Eps1f@+r” o alguna otra variación.

13. Las contraseñas deben estar formadas con al menos un elemento de los grupos mostrados a continuación:
    - Grupo de caracteres alfabéticos: letras mayúsculas y minúsculas (a-z, A-Z).
    - Grupo de caracteres numéricos: números (0-9)
    - Grupo de caracteres especiales: signos de puntuación: !@#$%^&*()+|~- =\`{}[]:";'<>?,./
14. Los usuarios no deben utilizar herramientas que intenten adivinar las contraseñas, a excepción de las áreas que por su naturaleza de operación lo requieran.
15. No utilizar la opción “recordar contraseña” en ninguna aplicación.
16. Siempre que un administrador establezca una contraseña por primera vez, debe forzarse al usuario a que la cambie la siguiente vez que la utilice.
17. Las actividades que están prohibidas en el uso de las contraseñas incluyen, más no limitan, las siguientes:
    - Compartir las contraseñas
    - Escribir y dejar las contraseñas en lugares de fácil acceso físico y/o visual debajo de su teclado, en post its, en su agenda o cuaderno, etc.)
    - Revelar una contraseña por teléfono a ninguna persona.
    - Revelar una contraseña en un correo electrónico.

Controles de ISO 27001:2013 cubiertos

Esta política cubre los siguientes controles específicos de seguridad de información del Anexo A de ISO 27001:2013:

Política de Gestión de acceso de usuario	
Control	**Nombre del Control**
A.9.2.1	Registro de altas y bajas de usuario.

Política de Gestión de acceso de usuario	
Control	**Nombre del Control**
A.9.2.2	Provisión de acceso a usuario.
A.9.2.3	Gestión de derechos de acceso privilegiado.
A.9.2.4	Gestión de información secreta de autentificación de los usuarios.
A.9.2.5	Revisión de los derechos de acceso a usuario.
A.9.2.6	Eliminación o ajuste del derecho de acceso.

9.3 Política de Responsabilidad de los Usuarios

Todos los usuarios de sistemas, aplicaciones, equipos de cómputo y servicios de red, deben estar conscientes de la importancia de mantener la seguridad de información y de la responsabilidad que tienen con respecto a mantener controles de acceso efectivos.

Lineamientos específicos

1. Cuando el usuario deba dejar desatendido su equipo de cómputo, debe bloquearlo o finalizar sesión con el fin de evitar accesos no autorizados al mismo y a la información a la que por su perfil pudiera tener acceso.
2. Se debe mantener el escritorio limpio de documentos en papel, medios de almacenamiento, dispositivos móviles, etc. siempre que el usuario no se encuentre en su lugar de trabajo, resguardando bajo llave dicha información y dispositivos.
3. Sólo se debe mantener sobre el escritorio o lugar de trabajo la información mínima indispensable que se requiera para realizar las actividades del empleado.
4. Se debe recoger de inmediato la información que se mande a imprimir.
5. Se debe mantener el escritorio del equipo de cómputo libre de acceso directo a documentos

Controles de ISO 27001:2013 cubiertos

Esta política cubre los siguientes controles específicos de seguridad de información del Anexo A de ISO 27001:2013:

Política de Responsabilidades de los Usuarios	
Control	**Nombre del Control**
A.9.3.1	Autentificación secreta.

9.4 Política de Control de Acceso a Sistemas Operativos

Los mecanismos de procesamiento de información, aplicaciones y sistemas de información deben usarse restringiendo el acceso a los sistemas operativos únicamente a los usuarios autorizados.

Lineamientos específicos

1. El acceso al sistema operativo de los equipos debe ser controlado a través de un procedimiento de registro (log-on) seguro, a fin de minimizar la oportunidad de obtener un acceso no autorizado al sistema, por lo tanto, se debe proporcionar la mínima información necesaria durante este proceso, como pudieran ser algunos identificadores de usuario y mensajes de error o ayuda.

2. No está autorizado que los usuarios instalen o configuren software y/o hardware. Todo el software que sea necesario instalar en los equipos debe ser autorizado por el Líder del SGI.

3. Si el equipo de cómputo no mantiene actividad durante un lapso de 5 minutos, el sistema debe bloquearse automáticamente y se debe reestablecer cuando el usuario introduzca la contraseña adecuada (se debe tener habilitado el protector de pantalla al pasar los 5 minutos antes mencionados).

4. Si no ha habido actividad en la aplicación o sistema durante un lapso (10 minutos), el sistema o aplicación, siempre que lo permita, debe sacar de sesión al usuario automáticamente, obligando al usuario a volver a introducir su ID y contraseña (loguearse) para poder tener acceso nuevamente a la aplicación o sistema en cuestión.

5. El acceso a la información, sistemas y aplicaciones debe estar restringido al personal de acuerdo con los privilegios de acceso y al control de acceso establecido.

6. Los sistemas privados deben tener un ambiente dedicado (aislado).

7. Los sistemas privados sólo pueden compartir recursos con otros sistemas o aplicaciones que sean confiables.

Controles de ISO 27001:2013 cubiertos

Esta política cubre los siguientes controles específicos de seguridad de información del Anexo A de ISO 27001:2013:

Política Control de Acceso a sistemas operativos	
Control	**Nombre del Control**
9.4.1	Restricción de acceso a la información.

Política Control de Acceso a sistemas operativos	
Control	**Nombre del Control**
9.4.2	Procedimientos de inicio de sesión seguro.
9.4.3	Sistema de gestión de contraseñas.
9.4.4	Uso de programas y utilidades privilegiadas.
9.4.5	Control de acceso al código fuente del programa.

10. Cifrado

10.1 Política de controles criptográficos

Se debe contar con mecanismos de cifrado para proteger los datos mientras se encuentran en tránsito o residen en sistemas de información que son propiedad o están administrados por SIlent4business

Lineamientos específicos

1. El Gerente de Operaciones junto con el Gerente de Ciberinteligencia deben definir los métodos de cifrado de la información confidencial de Silent4business de acuerdo con el nivel de clasificación de los activos.

2. El Gerente de Operaciones junto con el Gerente de Ciberinteligencia deben verificar que todo sistema de información o aplicativo que requiera realizar transmisión de información confidencial, cuente con mecanismos de cifrado de datos.

3. El Gerente de Operaciones junto con el Gerente de Ciberinteligencia establecen y desempeñan las actividades para el manejo y la administración de llaves de cifrado.

Controles de ISO 27001:2013 cubiertos

Esta política cubre los siguientes controles específicos de seguridad de información del Anexo A de ISO 27001:2013:

Política de Controles Criptográficos	
Control	**Nombre del Control**
A.10.1.1	Política de uso de controles criptográfico.
A.10.1.2	Gestión de claves.

11. Seguridad física y ambiental

11.1 Política de Áreas Seguras

Se debe contar con protección física adecuada a la clasificación de la información a proteger, para lo cual se debe contar con perímetros de seguridad física y controles de acceso a las áreas, a fin de evitar accesos físicos no autorizados, daño e interferencia.

Lineamientos específicos

1. Se deben tener claramente delimitadas las áreas consideradas como seguras, dentro de las instalaciones de la organización, a las cuales sólo tendrá acceso el personal que como parte del desempeño de sus funciones así lo requiera.

2. El acceso físico a las instalaciones de la organización por parte del personal interno debe ser por medio de una tarjeta de proximidad.

3. En el caso de los visitantes, deberán registrarse en la recepción.

4. Los visitantes pasarán a recepción de la organización donde esperarán a que el personal que visitan los reciba, mismo que los debe acompañar en todo momento dentro de las instalaciones, evitando dejarlo sólo sobre todo en áreas consideradas como seguras.

5. Dentro de las instalaciones de la organización, se debe portar la tarjeta de identificación de manera visible, no obstruyendo o distorsionando la información de este con micas, cintas adhesivas o cualquier otro elemento que no permita identificar claramente al portador de este.

6. Al personal interno que por algún motivo haya olvidado su tarjeta de identificación, se les proporcionará una tarjeta de visitante temporal, siguiendo los mismos lineamientos que un visitante.

7. En caso de pérdida o robo de una tarjeta de identificación y acceso, debe ser reportado en un lapso no mayor de 24 horas a su jefe inmediato y al área de Gestión de Talento, con el objeto de bloquear los privilegios de acceso asociados a dicha tarjeta.

8. La tarjeta de acceso es personal e intransferible por lo cual ninguna persona no autorizada podrá acceder a las instalaciones de la organización utilizando el mismo acceso de una persona autorizada.

9. Todo el personal que no realiza actividades permanentes en el centro de datos y visitantes que requieran tener acceso al mismo deben registrarse en la bitácora de acceso.

10. Con el objeto de no permitir que información clasificada como confidencial o privada sea extraída de los dispositivos o equipos de la Organización, todo componente del centro de

datos o electrónico, únicamente podrá ser retirado bajo autorización de su jefe inmediato superior.

11. En el caso de oficinas con puerta y áreas consideradas como seguras, éstas deben permanecer cerradas bajo llave siempre que el responsable de esta no se encuentre físicamente en su lugar de trabajo.

12. Las instalaciones de la organización deben contar con el equipo apropiado de Seguridad Física contra amenazas externas (extintores, detectores de humo, aire acondicionado, energía regulada, entre otros), para evitar daños tanto a la información como a los equipos; y se debe instruir al personal sobre el uso y funcionamiento de los equipos.

13. Los equipos donde se manejan aplicaciones críticas del negocio se deben ubicar en zonas de poco tránsito.

14. Con objeto de proteger a los activos de la organización, de accesos no autorizados, la recepción funge también como área de entrega de material, equipos y documentación en general.

Controles de ISO 27001:2013 cubiertos

Esta política cubre los siguientes controles específicos de seguridad de información del Anexo A de ISO 27001:2013:

Política de Áreas seguras	
Control	**Nombre del Control**
11.1.1	Perímetro de seguridad físico.
11.1.2	Controles físicos de entrada.
11.1.3	Seguridad de oficinas, habitaciones y facilidades.
11.1.4	Protección contra amenazas externas y del ambiente.
11.1.5	Trabajo en áreas seguras.
11.1.6	Áreas de entrega y carga.

11.2 Política de seguridad del equipo

Todo el equipo de la Organización y mecanismos de soporte a la infraestructura tecnológica (energía eléctrica, cableado, aire acondicionado, etc.) debe estar protegido contra amenazas físicas y ambientales, a fin de proteger la información contra daños o pérdidas.

Lineamientos específicos

1. Los equipos de cómputo y los servidores críticos deben estar protegidos contra el robo de partes, de tal manera que no puedan ser abiertos. Las llaves deben ser controladas por las Gerencias correspondientes.

2. Los equipos portátiles deben ser guardados, para evitar robo de estos, cuando se encuentren fuera de las instalaciones de la Organización en medida de lo posible.

3. Los servidores deben ubicarse en un rack y sólo personal autorizado tendrá acceso al mismo.

4. Se debe contar con planta de energía y fuente de energía ininterrumpida (UPS), con el fin de garantizar suministro de energía eléctrica de manera continua.

5. Los cables de telecomunicaciones (voz y datos), y energía eléctrica que transporten datos o soporten los servicios de infraestructura de TI deben estar protegidos contra intercepción y daño físico.

6. Está prohibido comer, fumar y tomar líquidos dentro del Centro de Datos.

7. Todos los equipos deben permanecer bloqueados cuando no sean usados por un administrador.

8. Los cables eléctricos, switches y toma de energía se deben localizar fuera del alcance de posibles derrames de líquidos.

9. Todos los equipos deben estar conectados a una tierra física.

10. Se deben mantener y monitorear las condiciones de temperatura y humedad en el Centro de datos.

11. Al reasignarse el equipo de cómputo a otro usuario o al darse por terminada la vida útil del mismo se debe seguir un procedimiento formal de reasignación o baja de equipo que considere al menos la eliminación segura de la información contenida en el equipo de cómputo a fin de evitar su recuperación y comprometer la confidencialidad de esta y se debe actualizar el inventario de activos de información.

12. El mantenimiento de los equipos de cómputo y comunicaciones se realiza conforme el calendario de mantenimiento definido por la organización.

13. El equipo de soporte (aire acondicionado, UPS, sistema contra incendios, etc.) debe recibir mantenimiento preventivo al menos una vez al año.

14. El personal externo que acuda a dar soporte o mantenimiento al Centro de Datos debe estar acompañado en todo momento por algún miembro del equipo del Centro de Datos.

15. Los servidores, equipos de escritorio, equipos portátiles y equipos de telecomunicación que se retiren de su sitio original para efectos de mantenimiento o manipulación por terceros, deben ser revisado con el fin de restringir el acceso a información confidencial y/o privada propiedad de la organización contenida en ellos.

16. Se debe llevar un registro de los servidores que se retiran de las instalaciones de la Organización, anotando al menos:

    a. Descripción del activo a ser retirado.

    b. Persona responsable del activo mientras se encuentre fuera de las instalaciones de la organización.

    c. Motivo para el retiro del activo.

    d. Fecha y hora de retiro del activo.

    e. Fecha y hora programada para el reingreso del activo.

    f. Nombre y firma de quien autoriza el retiro.

Controles de ISO 27001:2013 cubiertos

Esta política cubre los siguientes controles específicos de seguridad de información del Anexo A de ISO 27001:2013:

Política de Seguridad del Equipo	
Control	**Nombre del Control**
11.2.1	Instalación y protección de equipo.
11.2.2	Servicios de soporte.
11.2.3	Seguridad en el cableado.
11.2.4	Mantenimiento de equipos.
11.2.5	Retiro de activos.
11.2.6	Seguridad del equipo y activos fuera de las instalaciones.
11.2.7	Eliminación segura o reúso del equipo.
11.2.8	Equipo de usuario desatendido.
11.2.9	Política de escritorio limpio y pantalla limpia.

12. Seguridad en las operaciones

12.1 Política de responsabilidad y procedimientos de operación.

Se debe garantizar la correcta y segura operación de los mecanismos de procesamiento de información de la organización.

Lineamientos específicos

1. Se deben documentar, actualizar y mantener disponibles los procedimientos operativos, manuales de configuración e información necesaria para el correcto funcionamiento de los equipos e infraestructura de la organización.

2. Se debe llevar un control de cambios apegados al proceso de Gestión de Cambios P-SGI-022 para los sistemas operativos, aplicaciones y migraciones de la infraestructura actual, para garantizar la efectividad y correcta implementación considerando el análisis de riesgos de dicho cambio incluyendo el roll back.

3. Todos los cambios a los sistemas se tienen que llevar a cabo bajo un proceso que incluya un análisis de riesgos o impactos que dicho cambio pudiera ocasionar, así como una especificación de los controles de seguridad que serían necesarios implementar.

4. Siempre que el sistema operativo donde residen y corren los sistemas sea cambiado o actualizado, se deben revisar y probar dichos sistemas para garantizar que la actualización o cambio efectuado no tenga un impacto adverso en las operaciones y en la seguridad de información.

5. Se deben mantener registros de todos los cambios realizados.

6. Se debe mantener una segregación de funciones/ tareas evitando que una sola persona tenga el control total sobre un proceso de principio a fin, para reducir las oportunidades de modificación o mal uso de los activos e información de la organización.

7. Se debe contar con una división de roles y responsabilidades claramente definida a fin de evitar que una sólo persona pueda afectar un proceso crítico.

8. Se debe evitar el conflicto de intereses entre la operación, administración y verificación del cumplimiento.

9. Se debe garantizar, por medio de las revisiones y auditorías internas, que el personal realice sólo las tareas autorizadas de acuerdo con lo establecido en las descripciones de puesto, relevantes a sus puestos y posiciones respectivas.

10. Los ambientes de desarrollo, prueba y producción (operación) deben estar separados a fin de reducir el riesgo de accesos lógicos no autorizados o cambios al sistema que está actualmente funcionando (proveedor).

11. Se deben realizar una planeación y preparación de las capacidades futuras de los sistemas e infraestructura de cómputo y telecomunicaciones a fin de garantizar la disponibilidad de los recursos para entregar el desempeño requerido de los sistemas de acuerdo con proceso de Gestión de la Capacidad P-SGI-010.

    a) Se deben realizar proyecciones de los requerimientos de capacidades futuras a fin de evitar una sobre carga de los sistemas.

    b) El uso de los recursos debe ser monitoreado de manera constante y se deben realizar proyecciones con respecto a los requerimientos de capacidades futuras para garantizar el nivel de desempeño requerido por el sistema.

    c) Los requerimientos operacionales de los nuevos sistemas deben establecerse, documentarse y probarse antes de su aceptación y uso.

    d) Se debe establecer un criterio de aceptación para los nuevos sistemas de información, actualizaciones y nuevas versiones.

    e) Se debe contar con el número suficiente de licencias para el desempeño adecuado de las actividades

Controles de ISO 27001:2013 cubiertos

Esta política cubre los siguientes controles específicos de seguridad de información del Anexo A de ISO 27001:2013:

Política de Responsabilidades y procedimientos de operación	
Control	**Nombre del Control**
12.1.1	Documentación de procedimientos operacionales.
12.1.2	Gestión de cambios.
12.1.3	Gestión de la capacidad.
12.1.4	Separación de los ambientes de desarrollo, pruebas y operación.

12.2 Política de protección contra código malicioso

A fin de proteger la integridad de las aplicaciones, bases de datos e información de la organización se deben tomar las precauciones necesarias para prevenir y detectar la introducción de código malicioso (virus, gusanos, bombas lógicas, caballos de Troya, etc.) y código malicioso no autorizado.

Lineamientos específicos

1. Todos los equipos de cómputo de la organización deben tener instalado, actualizado y activado el software antivirus autorizado, incluyendo servidores cuyo sistema operativo así lo permita.
2. La configuración de los equipos debe garantizar que la operación se realice de acuerdo con las políticas de seguridad definidas.
3. Las actividades que se prohíben en el uso de equipos de cómputo incluyen, más no limitan, las siguientes:
   a) Desinstalar, desactivar o no actualizar el software de antivirus de la organización.
   b) Descargar software no autorizado o que viole las leyes de propiedad intelectual.

Controles de ISO 27001:2013 cubiertos

Esta política cubre los siguientes controles específicos de seguridad de información del Anexo A de ISO 27001:2013:

Política de Protección contra Código Malicioso	
Control	**Nombre del Control**
A.12.2.1	Controles contra código malicioso.

12.3 Política de respaldo

Se deben establecer e implementar procedimientos rutinarios de respaldo de información y realizar restauraciones periódicas de la información respaldada.

Lineamientos específicos

1. Toda la información de la organización en formato electrónico que se considere crítica, debe respaldarse periódicamente de acuerdo con las necesidades del área.
2. Las actividades relativas a la ejecución de respaldos se realizan bajo el procedimiento de Gestión de respaldos (PR-SGI-011).
3. Se deben realizar pruebas de restauración de información a fin de verificar la integridad y funcionalidad de los respaldos de información de manera aleatoria.

4. Los respaldos de información confidencial deben almacenarse en un sitio protegido contra amenazas.

5. Antes de cualquier cambio físico o lógico que afecte la infraestructura tecnológica y/o la configuración de los equipos, se debe realizar los respaldos necesarios.

6. Los respaldos de información del equipo de respuesta a incidentes se realizarán en los medios oficiales de resguardo de información de la organización, de acuerdo con el procedimiento Gestión de respaldos (PR-SGI-011).

Controles de ISO 27001:2013 cubiertos

Esta política cubre los siguientes controles específicos de seguridad de información del Anexo A de ISO 27001:2013:

Política de Respaldos	
Control	**Nombre del Control**
12.3.1	Respaldo de información.

12.4 Política de bitácoras y monitoreo

Todos los sistemas o aplicaciones de la organización deben ser monitoreados y los eventos de seguridad de información registrados en bitácoras o logs, a fin de detectar actividades no autorizadas y garantizar que los problemas de los sistemas o aplicaciones son identificados.

Lineamientos específicos

1. Todos los sistemas o aplicaciones, así como las plataformas sobre las que operan, deben tener activadas las bitácoras de operación, error, transacción, registro de usuarios y de actividades.

2. Se debe monitorear de manera periódica, tomando en cuenta la normatividad aplicable a la Organización, el uso de las instalaciones, mecanismos de procesamiento de información, sistemas, aplicaciones y servicios que ésta proporciona.

3. Se deben mantener las bitácoras de la herramienta de gestión de tickets.

4. Se deben mantener los registros de logs de los sistemas y aplicaciones de la organización

5. Las bitácoras podrán ser depuradas con el propósito de liberar recursos en la plataforma sobre la que operen los sistemas o aplicaciones de la Organización, siempre y cuando se garantice que, como resultado de los procedimientos de respaldo y recuperación de la información, se podrá contar con bitácoras continuas o sin pérdida de registro alguno.

6. Las bitácoras de los sistemas o aplicaciones deben ser revisadas periódicamente a fin de poder detectar cualquier registro o falta de él, que sea indicio de alguna actividad anormal o maliciosa.

7. Las actividades que se prohíben en el manejo de las bitácoras incluyen, más no limitan, las siguientes:

   - No desactivar las bitácoras de los sistemas o aplicaciones y de la plataforma sobre la que operen.

   - Borrar o alterar, accidental o intencionalmente, las bitácoras o los registros de las (os) mismas (os).

8. Todos los equipos de la organización deben tener sincronizado su reloj tomando como base una fuente de tiempo confiable, para garantizar exactitud y controlar los eventos, alarmas e incidentes que se generen, lo cual permitirá tener trazabilidad, rastreabilidad y poder seguir una línea de tiempo en caso de requerirse una investigación.

Controles de ISO 27001:2013 cubiertos

Esta política cubre los siguientes controles específicos de seguridad de información del Anexo A de ISO 27001:2013:

Política de Bitácora y monitoreo	
Control	**Nombre del Control**
12.4.1	Bitácoras de eventos.
12.4.2	Protección de información en bitácoras.
12.4.3	Bitácoras de administrador y operador.
12.4.4	Sincronización de relojes.

12.5 Política de control de Software

Se deben implementar controles para reducir el riesgo derivado de instalación insegura de Software.

Lineamientos específicos

1. No está autorizado que los usuarios instalen o configuren software y/o hardware. Todo el software que sea necesario instalar en los equipos debe ser autorizado por el Gerente de Operaciones.

2. Está expresamente prohibido bajar software de Internet para instalarlo en los equipos de cómputo. No está autorizado bajar contenido de Internet que no haya sido autorizado por el Gerente de Operaciones

3. No está autorizado el uso de aplicaciones de Internet que sean peer-to-peer (eMule, Ares Galaxy, chats, Messenger, etc.) que no hayan sido autorizadas por el Gerente de operaciones.

Controles de ISO 27001:2013 cubiertos

4. Esta política cubre los siguientes controles específicos de seguridad de información del Anexo A de ISO 27001:2013:

Política de control de Software	
Control	**Nombre del Control**
12.5.1	Instalación de software en sistemas operacionales.

12.6 Políticas de Gestión de Vulnerabilidades Técnicas

Se deben administrar las vulnerabilidades técnicas para reducir el riesgo derivado de su explotación.

Lineamientos específicos

1. Se debe obtener información acerca de las vulnerabilidades técnicas de los sistemas o aplicaciones que están siendo usados en la organización, evaluar la exposición a tales vulnerabilidades y tomar las medidas apropiadas para manejar los riesgos asociados, al menos una vez al año.
2. Una vez que se ha identificado una nueva vulnerabilidad técnica potencial, se deben identificar los riesgos asociados y las acciones a ser tomadas; tales acciones pueden involucrar bajar e instalar parches al sistema y/o aplicar otros controles.
3. Las actualizaciones al sistema operativo y aplicación de parches a las aplicaciones por parte de la organización deben ser probadas en un ambiente controlado antes de liberarlas al ambiente de producción a fin de evitar problemas operacionales con las aplicaciones que se tienen instaladas. Después de cualquier cambio en aplicaciones en producción se debe correr un protocolo de pruebas para asegurar su correcto funcionamiento.

4. Dependiendo de qué tan grave sea la vulnerabilidad técnica, las acciones a tomar deben llevarse a cabo de acuerdo con el control de cambios establecido o siguiendo el procedimiento de manejo de incidentes de seguridad de información.
5. Se deben establecer controles para restringir la instalación de software no permitido esto para mitigar el riesgo de la explotación de posibles vulnerabilidades.

Controles de ISO 27001:2013 cubiertos

Esta política cubre los siguientes controles específicos de seguridad de información del Anexo A de ISO 27001:2013:

Política de Gestión de Vulnerabilidades Técnicas	
Control	**Nombre del Control**
A.12.6.1	Control de vulnerabilidades técnicas.
A.12.6.2	Restricciones en la instalación de Software.

12.7 Política de auditoría de sistemas de Información

1. En medida de lo posible se debe garantizar que todos los sistemas o aplicaciones, así como las plataformas sobre las que operan, tengan activadas las bitácoras de operación, error, transacción, registro de usuarios y de actividades.

2. Se debe monitorear de manera periódica, tomando en cuenta la normatividad aplicable a la Organización, el uso de las instalaciones, mecanismos de procesamiento de información, sistemas, aplicaciones y servicios que ésta proporciona.

3. Todos los sistemas de información podrán ser auditados lo cual permitirá revisar la trazabilidad de la información.

Controles de ISO 27001:2013 cubiertos

Esta política cubre los siguientes controles específicos de seguridad de información del Anexo A de ISO 27001:2013:

Política de Gestión de Vulnerabilidades Técnicas	
Control	**Nombre del Control**
12.7.1	Controles de auditoría de sistemas de información.

13. Seguridad en la Telecomunicaciones

13.1 Política de Gestión de seguridad en redes

Se debe proteger toda la información clasificada como confidencial o privada que pase sobre redes que estén fuera de los límites de la Organización. Así mismo, se debe controlar el uso de Internet tomando en cuenta el flujo de datos, el monitoreo de la información transmitida por este medio y las implicaciones legales aplicables.

Lineamientos específicos

1. Se debe administrar y controlar la red de la organización, a fin de protegerla contra amenazas y mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluyendo la información en tránsito.

2. El servicio de Internet se provee con fines estrictamente laborales.

3. Dado que el servicio de Internet hace uso de los recursos de la organización, la actividad de los usuarios puede ser monitoreada, sin generar alguna obligación, por lo que los usuarios no pueden esperar que se mantenga privacidad sobre el servicio.

4. Se podrá hacer uso de filtros y otras técnicas para restringir el acceso a sitios de Internet que no tengan fines estrictamente laborales. Los reportes de intentos de acceso serán examinados de manera regular y enviados a los Gerentes para su valoración.

5. El servicio de Internet es otorgado de forma personal y son los usuarios, los responsables directos de evitar accesos no autorizados a sitios de Internet que no tengan fines estrictamente laborales, así como de las actividades que bajo su cuenta se realicen.

6. Las actividades que se prohíben cuando se hace uso del servicio de Internet incluyen, más no limitan, las siguientes:

   Acceso a las siguientes categorías de sitios:

   - Material pornográfico.
   - Drogas.
   - Apuestas, juegos.
   - Asuntos ilegales o cuestionables.
   - Grupos extremistas.

- Racismo.
- Alcohol y tabaco.
- Citas y anuncios personales.
- Violencia y armas.
- Y, en general, todo aquello que no contribuya a la productividad laboral.
- Descarga de todo tipo de software o aplicación que pueda representar una vulnerabilidad a la Información de la organización.

7. Derivado de las funciones o actividades del equipo CSIRT, podrán realizar la navegación a sitios incluidos quedarán exceptuados de la política anterior, siempre que estas se lleven a cabo en un ambiente controlado con fines laborales.

8. El diseño y contenido de la página web de la organización, debe apegarse a las políticas establecidas por la Alta Dirección.

9. El contenido de las páginas debe tener información de interés para los usuarios, de ningún modo esta información debe atentar contra los intereses y políticas de la organización

10. Toda la información que se genera para el portal de Internet será propiedad de la organización

11. Se debe segmentar la red para evitar accesos no autorizados a información confidencial o privada.

12. El acceso a la red de manera remota se deberá realizar mediante VPN, la cual deberá ser autorizada por el jefe inmediato y el área de normatividad al correo sgi@silent4business.com, una vez aprobada por ambas partes, el personal solicitante deberá reenviar el correo al área de soporte interno con al menos la siguiente información: nombre de solicitante, nombre de jefe inmediato, puerto, protocolo, IP/hostname, privilegios, justificación de uso y vigencia.

Controles de ISO 27001:2013 cubiertos

Esta política cubre los siguientes controles específicos de seguridad de información del Anexo A de ISO 27001:2013:

Política de Gestión de Seguridad en la Red	
Control	**Nombre del Control**
13.1.1	Controles de red.
13.1.2	Seguridad en los servicios en red.
13.1.3	Segregación en redes.

13.2 Política de Intercambio de información con partes externas

Se debe proteger apropiadamente la información clasificada como confidencial o privada de la organización contra accesos no autorizados, mal uso y/o corrupción durante su proceso de intercambio mediante el uso de mecanismos y acuerdos adecuados para los mismos.

Lineamientos específicos

1. Para el intercambio de información mediante el uso de mecanismos de comunicación electrónica se debe considerar: proteger el intercambio de información de cualquier intercepción, copia, modificación, mal enrutamiento o destrucción, de acuerdo con la clasificación de información de la misma

2. Los acuerdos de intercambio de información deben considerar las siguientes condiciones de seguridad:
    a. Responsabilidades para controlar y notificar la transmisión, el envío y recepción de la información intercambiada.
    b. El posible uso de un sistema de etiquetado para la información confidencial que sea intercambiada, asegurándose de que el significado de las etiquetas sea entendido y de que la información este protegida apropiadamente, siempre que sea acordado entre el emisor y receptor de esta
3. La información confidencial que se utilice como parte de la interacción con otras comunidades de equipos CSIRT deberá mantenerse en el repositorio del área de Ciberinteligencia, aplicando las medidas de seguridad que eviten un acceso no autorizado.

Controles de ISO 27001:2013 cubiertos

Esta política cubre los siguientes controles específicos de seguridad de información del Anexo A de ISO 27001:2013:

Política de Intercambio de Información con partes externas	
Control	**Nombre del Control**
A.13.2.1	Políticas y procedimientos de transferencia de la información.
A.13.2.2	A cuerdos de transferencia de información.

13.2.3 Política de correo electrónico

El uso del correo electrónico organizacional está permitido únicamente para fines estrictamente laborales, por lo cual toda la información transmitida por este medio debe controlarse a fin de evitar exposición no autorizada de información confidencial y/o privada.

Lineamientos específicos

1. Las cuentas de correo electrónico son otorgadas de forma personal y son los titulares de estas, los responsables directos del uso del servicio y del contenido de los mensajes, evitando el uso de lenguaje inapropiado en los mismos.

2. El envío y recepción de archivos adjuntos está permitido únicamente después de haber confirmado la clasificación de la información y de haber verificado los archivos por posible infección de virus u otra forma de código malicioso.

3. Los archivos recibidos de remitentes desconocidos deben ser borrados inmediatamente sin ser abiertos.

4. Las actividades que se prohíben cuando se hace uso del servicio de correo electrónico incluyen, más no limitan, las siguientes:
    - El envío de música, video, imágenes y cualquier otro tipo de información que no tenga ninguna relación con fines laborales.
    - El abrir, reenviar y responder correos de procedencia dudosa o no solicitados (spam, cadenas), mismos que deberán ser eliminados permanentemente.
    - Utilizar el correo electrónico para chatear, ya sea con personal interno o externo.

5. El usuario es responsable de la depuración de su cuenta de correo electrónico, por lo cual debe archivar y respaldar de manera regular y adecuada dicha información, de acuerdo con sus necesidades, puede solicitar apoyo del personal de la gerencia correspondiente para realizarlo.

6. El Gerente de Operaciones tiene la facultad de monitorear o revisar los correos electrónicos de los usuarios cuando se ponga en riesgo la operación de los servicios y/o la Seguridad de la Información de la Organización.

7. Está prohibido el envío de información propiedad de la organización desde cuentas personales (Hotmail, Gmail, Yahoo, etc.).

8. Se debe garantizar la no repudiación en él envió de mensajería electrónica.

Controles de ISO 27001:2013 cubiertos

Esta política cubre los siguientes controles específicos de seguridad de información del Anexo A de ISO 27001:2013:

Política de Correo Electrónico	
Control	**Nombre del Control**
A.13.2.3	Mensajería electrónica.

14. Adquisición y mantenimiento de la información

14.1 Política de requerimientos de seguridad de los sistemas de información

Se deben identificar, definir, justificar y acordar los requerimientos de seguridad de información durante la fase de diseño de los sistemas o aplicaciones que soportan los procesos de la organización, previo a la implementación y/o mantenimiento de dichos sistemas. Se deben tomar en cuenta controles de validación de datos de entrada y de salida, así como garantizar un correcto procesamiento interno.

Lineamientos específicos

1. El área que solicita el desarrollo de un nuevo sistema de información debe establecer en conjunto con el proveedor o el área que se encargará del desarrollo, el entendimiento común de los requerimientos del sistema, permitiendo así confirmar el acuerdo de lo que será la solución y la estimación del tiempo y costo.

2. Debe quedar documentada la definición del requerimiento inicial del desarrollo del sistema, el cual debe incluir los requerimientos de seguridad.

Controles de ISO 27001:2013 cubiertos

Esta política cubre los siguientes controles específicos de seguridad de información del Anexo A de ISO 27001:2013:

Política de Requerimientos de Seguridad de los Sistemas de Información	
Control	**Nombre del Control**
14.1.1	Análisis y especificación de requerimientos de seguridad.

15. Relación con proveedores

15.1 Política de seguridad con relación a los proveedores

En Silent4business se establecerá mecanismos de control en sus relaciones con terceras partes, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por las mismas, cumplan con las políticas, normas y procedimientos de Seguridad de la Información.

Los responsables de la realización y/o firma de contratos o convenios con terceras partes se asegurarán de la divulgación de las políticas, normas y procedimientos de Seguridad de la Información a dichas partes.

Lineamientos específicos

1. Los responsables de áreas solicitantes junto con el área alianzas estratégicas deben generar un modelo base para los Acuerdos de Niveles de Servicio y requisitos de Seguridad de la Información, con los que deben cumplir terceras partes o proveedores de servicios; dicho modelo, debe ser divulgado a todas las áreas que adquieran o supervisen recursos y/o servicios tecnológicos.

2. El área de alianzas estratégicas, cumplimiento y normatividad en conjunto con apoyo jurídico debe elaborar modelos de Acuerdos de Confidencialidad y Acuerdos de Intercambio de Información con terceras partes. De dichos acuerdos deberá derivarse una responsabilidad tanto civil como penal para la tercera parte contratada.

3. El Gerente de Operaciones debe establecer las condiciones de conexión adecuada para los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de la organización.

4. El Gerente de Operaciones debe implementar las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros proveedores de servicios.

Controles de ISO 27001:2013 cubiertos

Esta política cubre los siguientes controles específicos de seguridad de información del Anexo A de ISO 27001:2013:

Política de Seguridad de la Información con relación a los proveedores	
Control	**Nombre del Control**
A.15.1.1	Política de Seguridad de la Información para las relaciones con los proveedores.
A.15.1.2	Seguridad dentro del acuerdo con los proveedores.
A.15.1.3	Información y comunicación de la cadena de suministro de tecnología.

15.2 Política de gestión de la presentación del servicio

1. El dueño de la información debe mantener los niveles acordados de Seguridad de la Información y de prestación de los servicios de los proveedores, en concordancia con los acuerdos establecidos con estos. Así mismo, velará por la adecuada gestión de cambios en la prestación de servicios de dichos proveedores.

2. El Gerente de Operaciones debe verificar las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros proveedores de servicios.

3. Cada Líder responsable de proveedores debe monitorear periódicamente, el cumplimiento de los Acuerdos de Niveles de Servicio, Acuerdos de Confidencialidad y los requisitos de Seguridad de la Información (en caso de que aplique) de acuerdo con el procedimiento de Evaluación de Proveedores PR-ALI-003.

4. El área de Alianzas Estratégicas revisa periódicamente, el cumplimiento de los Acuerdos de Niveles de Servicio, Acuerdos de Confidencialidad y los requisitos de seguridad (en caso de que aplique).

Controles de ISO 27001:2013 cubiertos

Esta política cubre los siguientes controles específicos de seguridad de información del Anexo A de ISO 27001:2013:

Política de Administración de Vulnerabilidades Técnicas	
Control	**Nombre del Control**
15.2.1	Monitoreo y revisión de servicios del proveedor.
15.2.2	Gestión de cambios a los servicios del proveedor.

16. Administración de incidentes de seguridad de información

16.1 Política de administración de incidentes de Seguridad de la Información

Todos los colaboradores, contratistas y terceros que laboren o presten algún servicio para la organización deben reportar cualquier evento, debilidad o incidente de seguridad de información que detecten tan pronto como sea posible por medio de los canales establecidos para tal efecto, a fin de que éstos puedan ser atendidos en tiempo y forma con lo cual se pueda mitigar el posible impacto de estos. Siempre que el incidente amerite una investigación más profunda se debe recabar toda la evidencia posible, dentro del marco legal y normativo aplicable.

Lineamientos específicos

1. Todos los colaboradores deben reportar de inmediato los eventos e incidentes de Seguridad de la Información que identifiquen, al Líder del SGI. A continuación, se listan algunos ejemplos de incidentes de seguridad de información, los cuales son enunciativos, más no limitativos:

   - Incapacidad para tener acceso o malfuncionamiento de los sistemas críticos necesarios para la operación.
   - Robo o perdida de información confidencial.
   - Incumplimiento con políticas y/o procedimientos de Seguridad de la Información.
   - Accesos físicos no autorizados a las instalaciones y/o áreas consideradas como restringidas.
   - Identificar a personal ajeno a la organización sin acompañante dentro de las instalaciones.
   - Cambios a los sistemas no controlados.
   - Pérdida de integridad de las Bases de Datos.
   - Eliminación no autorizada de archivos electrónicos.
   - Daño intencional físico a equipos de cómputo y telecomunicaciones.
   - Violaciones al control de acceso lógico (compartir passwords, hackeo, etc.)
   - Ejecución intencionada de código malicioso (virus, gusanos, etc.) que ponga en riesgo la información.
   - Ejecución intencionada de herramientas y escáneres detectores y atacantes de vulnerabilidades de seguridad en los sistemas informáticos.

2. Se debe seguir un proceso formal para reportar los Incidentes de Seguridad de la Información P-SGI-018, que contemple la respuesta a incidentes y su escalamiento.

3. Se debe mantener un registro auditable detallado de todos los incidentes y eventos de Seguridad de la Información reportados incluyendo la investigación y cierre de los mismos, el cual se debe almacenar por al menos un año.

4. Toda la documentación de los incidentes de seguridad de información registrados debe estar clasificados como confidenciales y ser custodiados por el Líder del SGI.

5. Se deben llevar a cabo sesiones de lecciones aprendidas con el personal involucrado en el manejo de incidentes, con base a los incidentes de seguridad de información presentados.

6. Ningún usuario no autorizado debe intentar probar o corregir la debilidad que dio origen al incidente de Seguridad de la Información detectado.

7. Se debe evitar el uso de activos de información o mecanismos comprometidos por el incidente de seguridad de información.

8. Se debe preservar la escena (asegurar el área afectada por el incidente) y proteger la evidencia con el objetivo de preservar su admisibilidad y valor en caso de que sea necesario entablar una acción legal, para lo cual se deben tener en consideración las siguientes acciones:

    - Tomar fotografías, asegurar las bitácoras, tomar notas el estado del sistema, etc.
    - Identificar cada parte de la evidencia por medio de etiquetas, fechas, firmas, etc.
    - Usar acuses de recibo cuando la evidencia sea transferida a otra persona para su manejo.
    - Controlar el acceso a la evidencia.
    - Definir quien tiene acceso a la evidencia.
    - Recolecta toda la información posible a cerca del incidente.

9. Cuando se tenga evidencia de que el incidente de Seguridad de la Información fue provocado por los colaboradores de la organización, se deben tomar las acciones correspondientes de acuerdo con lo establecido en el procedimiento disciplinario PR-SGI-007.

Controles de ISO 27001:2013 cubiertos

Esta política cubre los siguientes controles específicos de seguridad de información del Anexo A de ISO 27001:2013:

Política de Administración de Incidentes de Seguridad de la Información	
Control	**Nombre del Control**
A16.1.1	Responsabilidades y procedimientos.
A16.1.2	Notificación de los eventos de Seguridad de la Información.
A16.1.3	Notificación de puntos débiles de la seguridad.
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información.
A16.1.5	Respuesta a incidentes de Seguridad de la Información.
A16.1.6	Aprendizaje de los incidentes de Seguridad de la Información.
A16.1.7	Recopilación de evidencias.

17. Administración de continuidad de negocio

17.1 Política de Continuidad del Negocio

Se debe implementar un proceso de administración de la continuidad de la organización para minimizar el impacto en caso de presentarse un desastre y poder recuperarse de una pérdida de activos e información (resultado de desastres naturales, accidentes, falla de equipos o acciones deliberadas), a un nivel aceptable a través de una serie de controles preventivos y de recuperación, para lo cual se deben identificar los procesos críticos de la organización tomando en cuenta los requerimientos de seguridad de información, a fin de garantizar que ésta se preserva aun en un caso de desastre.

Lineamientos específicos

1. Se debe dar cumplimiento a la estrategia de recuperación para las diferentes plataformas que conforman la infraestructura tecnológica de la Organización, así como desarrollar, documentar, probar y mantener un Plan de Continuidad del Negocio (BCP) de la organización que conduzca a la restauración de los sistemas críticos de información, a fin de garantizar su continuidad.

2. Al estar operando desde el sitio alterno durante la ejecución del Plan de Continuidad del Negocio, se debe considerar y mantener el mismo nivel de seguridad de información que el utilizado para la infraestructura en el sitio primario, aun cuando los niveles de servicio no sean los mismos que los ofrecidos durante la operación normal.

3. Establecer y usar un marco de trabajo que permita identificar y evaluar el grado de criticidad de los procesos que se realizan en la organización, a fin de definir niveles de prioridad de recuperación en caso de que se presente un desastre.

4. Garantizar en la medida de lo posible que todo el personal esté disponible y pueda ser localizado en caso de requerirse ejecutar el Plan de Continuidad del Negocio.

5. El Plan de Continuidad del Negocio debe especificar la manera en que se trasladará la infraestructura crítica de la organización al sitio alterno, así como también el aprovisionamiento de recursos (mobiliario, equipo, materiales, etc.), cuando aplique.

6. El Plan de Continuidad del Negocio debe ser ampliamente difundido y conocido por todo el personal de la Organización a fin de garantizar una recuperación exitosa en caso de presentarse algún desastre.

7. Se debe especificar claramente las condiciones y los pasos a seguir para activar el Plan de Continuidad del Negocio.

8. Se debe probar el Plan de Recuperación ante Desastres al menos una vez al año para garantizar que éstos se mantienen actualizados, son relevantes y efectivos.

9. Se deben generar registros de cada prueba que se realice al Plan de Continuidad del Negocio, a fin de dejar evidencia de las acciones tomadas, los tiempos de recuperación y los puntos de mejora.

10. Se deben establecer las medidas de protección civil correspondientes a fin de garantizar la seguridad del personal en caso de contingencia.

Controles de ISO 27001:2013 cubiertos

Esta política cubre los siguientes controles específicos de seguridad de información del Anexo A de ISO 27001:2013:

Control	Política de Continuidad del Negocio Nombre del Control
A.17.1.1	Planificación de la continuidad de la Seguridad de la Información.
A.17.1.2	Implementar la continuidad de la Seguridad de la Información.

A.17.1.3	Verificación, revisión y evaluación de la continuidad de la Seguridad de la Información.

17.2 Política de redundancia

El Gerente de Operaciones/ Líder SGI realizara el análisis de impacto al negocio para identificar los activos críticos y definir una plataforma tecnológica redundante que satisfaga los requerimientos de disponibilidad aceptables para Silent4business.

Lineamientos específicos

1. El Gerente de Operaciones/ Líder SGI deben analizar y establecer los requerimientos de redundancia para los sistemas de información críticos para la organización y la plataforma tecnológica que los apoya.

2. El Gerente de Operaciones/ Líder SGI debe evaluar y probar soluciones de redundancia tecnológica y seleccionar la solución que mejor cumple los requerimientos del Silent4business.

3. El Gerente de Operaciones/ Líder SGI a través de los involucrados, debe administrar las soluciones de redundancia tecnológica y realizar pruebas periódicas sobre dichas soluciones, para asegurar el cumplimiento de los requerimientos de disponibilidad de Silent4business.

Esta política cubre los siguientes controles específicos de seguridad de información del Anexo A de ISO 27001:2013:

Control	Política de Redundancia Nombre del Control
A.17.2.1	Disponibilidad de los recursos de tratamiento de la información.

18. Cumplimiento

18.1 Política de cumplimiento con requerimientos legales

La planeación, operación, uso y administración de los sistemas de información deben estar sujetos a los requerimientos legales y contractuales de la organización.

Lineamientos específicos

1. Todas las leyes, regulaciones y requerimientos contractuales aplicables a la organización deben estar explícitamente identificados, definidos, documentados y actualizados.

1. Todo el software instalado en los equipos de cómputo de la organización debe cumplir con la Ley Federal de Derechos de Autor. Así mismo, se encuentra prohibido la inclusión de logos que cuenten con derechos de propiedad intelectual para su uso.

2. Los registros importantes de la organización deben ser protegidos contra pérdida, destrucción, modificación y acceso no autorizado.

3. Se deben implementar los controles necesarios para poder identificar, almacenar, proteger, recuperar disponer y cumplir con los tiempos de retención de todos los registros de la organización.

4. Se deben proteger los datos de carácter personal contra accesos y divulgaciones no autorizadas, conforme lo marca Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

5. El uso de mecanismos de cifrado se debe hacer dentro del marco legal aplicable, por lo cual no se enviará información encriptada cuando esto sea un impedimento legal, normativo o contractual.

Controles de ISO 27001:2013 cubiertos

Esta política cubre los siguientes controles específicos de seguridad de información del Anexo A de ISO 27001:2013:

Política de Cumplimiento con Requerimientos Legales	
Control	**Nombre del Control**
A.18.1.1	Identificación de legislación aplicable.
A.18.1.2	Derechos de propiedad intelectual.
A.18.1.3	Protección de registros de la organización.
A.18.1.4	Protección y privacidad de datos de información personal.
A.18.1.5	Regulación de controles criptográficos.

18.2 Política de revisiones de la Seguridad de la Información

Los sistemas de información deben ser revisados regularmente para garantizar el cumplimiento técnico con los estándares, políticas y lineamientos de Seguridad de la Información implementados.

Lineamientos específicos

2. Cada responsable de área debe asegurar que todos los procedimientos y políticas de Seguridad de Información aplicables a su área son implementados correctamente para lograr el cumplimiento de los objetivos establecidos.

3. Se deben realizar auditorías internas al menos una vez al año a todo el SGI de la organización.

4. Se deben establecer revisiones técnicas periódicas, al menos una vez al año, (análisis de vulnerabilidades y pruebas de penetración), para evaluar el grado de adecuación y cumplimiento con los controles de seguridad de información implementados. Dichas revisiones pueden ser realizadas por personal interno y/o externo, en cuyo caso deben ser involucrados los responsables de las áreas correspondientes.

5. Se deben buscar ventanas de mantenimiento apropiadas para ejecutar las revisiones de cumplimiento técnico (análisis de vulnerabilidades y pruebas de penetración), a fin de no comprometer la Seguridad de la Información.

6. En caso de utilizar herramientas automatizadas para realizar las revisiones de cumplimiento técnico se deben aplicar controles de Seguridad de la Información apropiados (control de acceso, administración de privilegios, entre otros).

7. Se deben aplicar acciones correctivas de acuerdo con los resultados obtenidos de la verificación de cumplimiento técnico.

Controles de ISO 27001:2013 cubiertos

Esta política cubre los siguientes controles específicos de seguridad de información del Anexo A de ISO 27001:2013:

Política de Revisiones de la Seguridad de la Información	
Control	**Nombre del Control**
A.18.2.1	Revisión independiente de la Seguridad de la Información.

A.18.2.2	Cumplimiento de las políticas y normas de seguridad.
A.18.2.3	Revisión del cumplimiento de normas técnicas.

5. Anexos

No aplica