Política de Seguridad de la Información wolkvox

1. Propósito

Este documento se plantea como lineamiento base para tener en cuenta en el manejo de la información durante la ejecución normal de las actividades de negocio. Por ello, se plasman, además de las directrices, la posición y compromiso de la alta dirección de la empresa en relación con mantener la confidencialidad, integridad y disponibilidad de los activos de información de la Empresa, de los proveedores y clientes que la han compartido con WOLKVOX, como actividad requerida para llevar a cabo el uso de las soluciones tecnológicas que ha contratado con éste o por el desarrollo de las relaciones de negocio.

2. Definiciones

Documento Referencia Definiciones SGSI wolkvox.

3. Alcance

Esta política aplica a toda la Empresa, sus empleados, contratistas, partners y terceros relacionados con wolkvox.

4. Nivel de Cumplimiento

Todas las personas incluidas en el alcance de esta política deberán cumplir al 100% con las directrices establecidas. El incumplimiento de la Política de Seguridad de la Información y Ciberseguridad conllevará consecuencias legales y disciplinarias conforme a la normativa de la compañía y a las regulaciones pertinentes del gobierno nacional y territorial en materia de seguridad de la información. Se contemplan excepciones a esta política, las cuales deberán ser aprobadas por el Comité de Seguridad de la Información y Continuidad.

5. Política General de Seguridad de la Información

La dirección de wolkvox , entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con terceros (clientes, empleados, socios, partners, proveedores u otros) que puedan estar interesados en el desarrollo de las actividades de negocio, todo enmarcado en el estricto cumplimiento de la ley que aplique en el país de uso, y en concordancia con la misión y visión de la Empresa resultado de los ejercicios de planeación y revisión de la estrategia organizacional que la Empresa lleve a cabo.

Para wolkvox, la protección de la información y la ciberseguridad de los servicios ofrecidos en nube busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición mínimo que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados. De acuerdo con lo anterior, esta política aplica a la Empresa según como se define en el alcance, sus empleados (incluyendo aprendices y practicantes), proveedores, partners, terceros y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor de un Sistema de Gestión de la Seguridad de la Información estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en el desarrollo de las funciones más importantes de la Empresa, incluyendo (más no delimitado) a la gestión de proyectos, la gestión de las tecnologías de la información, la gestión de los recursos físicos y financieros, y, la gestión del talento humano.
- Cumplir con los principios de seguridad de la información, según las mejores prácticas.
- Cumplir con los principios de la función administrativa.
- Cumplir con el marco legislativo nacional e internacional dónde la organización decida tener presencia.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos de información.
- Garantizar el cumplimiento de la normativa legal aplicable, tanto a nivel nacional como internacional, conforme a las obligaciones que Wolkvox haya adoptado voluntariamente o que le sean exigibles
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información, conforme las mejores prácticas.
- Fortalecer la cultura de seguridad de la información en los empleados, terceros, aprendices, practicantes y clientes de la Empresa.
- Mejorar continuamente la gestión de la seguridad de la información.
- Garantizar la continuidad del negocio frente a incidentes.
- Revisar y ajustar las políticas al menos una vez al año, o cada vez que sea requerido por un cambio.

6. Políticas específicas de la seguridad de la información

A continuación, se establecen las 13 políticas específicas de seguridad que soportan el Sistema de Gestión de Seguridad de la Información dewolkvox:

6.1. wolkvox ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, las mejores prácticas y a los

requerimientos regulatorios vigentes.

6.2. wolkvox se compromete con el cumplimiento de las leyes, normas y regulaciones relacionadas o de incumbencia con la Seguridad de la Información, en Colombia y en los países dónde se cuente con clientes que consuman las tecnologías ofrecidas. En caso de identificar brechas o condiciones no satisfechas, desde la gestión del Sistema de Gestión de Seguridad de la Información, buscará atender la necesidad de ajuste y cumplimiento.

6.3. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros, considerando los principios de segregación de tareas para evitar que dichos roles accedan a activos de información no relacionados con las tareas o funciones a cargo, reducir la posibilidad de modificación no autorizada, o no intencional, o el uso indebido de los activos de información.

6.4. wolkvox protege la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de estos.

6.5. wolkvox protege la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

6.6. wolkvox protege su información de las amenazas originadas por parte del personal interno, considerando los distintos momentos o etapas de los empleados durante la relación contractual con la Empresa, y una vez se dé por terminada dicha relación.

6.7. wolkvox protege las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

6.8. wolkvox controla la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos que soportan sus operaciones contratadas con el proveedor de servicios en la nube y sus sedes administrativas.

6.9. wolkvox implementa control de acceso a la información, sistemas y recursos de red, considerando principios de mínimos privilegios y de segregación de tareas de empleados, contratistas o terceros. Los deberes y áreas de responsabilidad en conflicto se deben identificar y dirimir para reducir las posibilidades de modificación no autorizada o no intencional de la información de la Empresa, o el uso indebido de los activos de la organización.

6.10. wolkvox garantiza que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

6.11. wolkvox garantiza una adecuada gestión de los incidentes y eventos de seguridad, así como de las debilidades asociadas con los sistemas de información en pro de una mejora efectiva de su modelo de seguridad.

6.12. wolkvox garantiza la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.

6.13. wolkvox garantiza el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas con terceros en el territorio colombiano, y respetará y buscará el cumplimiento de tales obligaciones con terceros que contraten sus servicios y se encuentren en países distintos al de Colombia.

El incumplimiento a la Política de Seguridad y Privacidad de la Información traerá consigo, las consecuencias legales que apliquen a la normativa de la Empresa, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial de Colombia, y la de los países dónde se cuente con clientes que consuman las tecnologías ofrecidas, en cuanto a Seguridad y Privacidad de la Información se refiere.

7. Política para la implementación de controles de seguridad de la información

A continuación, se listan las políticas puntuales para la implementación de los controles requeridos en la gestión del Sistema de Gestión de Seguridad de la Información de la Empresa.

7.1. Organización de la Seguridad de la Información.

Se define como entidad superior de gobierno en lo relacionado con el logro del propósito formulado, un Comité Directivo de Seguridad de la Información y Continuidad, integrado por: CEO (o su delegado), el IT Services Director, el Engineering Director, el Risk Leader in Information Security and Continuity, el Administrative and Financial Director, el Global Sales Director, Product Design and Marketing Director, y el Talent & Culture Director.

Este comité se encarga de la revisión y actualización de este documento de Políticas, de liderar las comunicaciones al interior de la Empresa para generar la cultura alrededor de la seguridad de la información, velar por el cumplimiento de normas y estándares que la empresa defina incorporar en su portafolio, supervisar los resultados del sistema de gestión de la seguridad de la información, solicitando ajustes o mejoras cuando sea requerido. Tendrá a cargo el direccionamiento de las comunicaciones a terceros, cuando se presenten incidentes en seguridad de la información y continuidad del negocio. Garantizará la correcta atención y manejo de los incidentes en seguridad de la información que se pudiesen presentar. Identificará y asegurará las conexiones necesarias entre el SGSI y el Sistema de Gestión de Seguridad y Salud en el Trabajo (SG SST) de la Empresa con el propósito de mantener una visión unificada en la gestión de los riesgos que puedan afectar la seguridad de la información y la seguridad en el trabajo.

El comité se reune con una periodicidad que por cuenta propia deberá definir, buscando garantizar se ejecutan oportunamente las funciones ya mencionadas.

7.2. Gestión de activos.

Se establecen las directrices mediante las cuales se le indica a los empleados los límites y procedimientos frente a la identificación, uso, administración y responsabilidad frente a los activos de información. Se plantean las siguientes:

Identificación de activos: Se debe hace un inventario de los activos de información de la Empresa, propios o de terceros, considerando la identificación del propietario o responsable de cada activo de información, y dejando clara las herramientas de apoyo que se usarán para realizar la tarea. Este inventario deberá ser revisado y actualizado en la medida que se ejecuten cambios (actualizaciones, adiciones, retiros) sobre los mismos.

Clasificación de los activos de información: La Empresa lleva a cabo la clasificación de los activos de información de acuerdo con la criticidad, sensibilidad y reserva de estos. Tales definiciones deben quedar estipuladas en un procedimiento de gestión. En esta revisión se convocará a los terceros que han provisto activos de información para ser almacenados y custodiados por la Empresa, de manera que se hagan igual partícipes de la responsabilidad de aseguramiento de estos.

Etiquetado de los activos de información: Todos los activos de información deberán ser etiquetados siguiendo criterios que permitan su rápida identificación, propósito y la clasificación dada. Estas definiciones deben quedar documentadas en un procedimiento.

Devolución/Transporte/Disposición Final de Activos: La Empresa delega en el Risk Leader in Information Security and Continuity la definición de los instrumentos y los mecanismos para llevar a cabo las actividades de devolución, transporte y/o disposición final de los Activos de Información, cuando los terceros lo hayan definido en el inicio de relaciones de negocios. Así mismo establecerá los mecanismos y controles para asegurar que los empleados realicen la entrega de activos físicos y de la información una vez finalizado el empleo, acuerdo o contrato que se tenga con la Empresa. Deberá considerarse como primera acción de control, la posibilidad de eliminar dejando constancia de la actividad ejecutada y el alcance posible. El despliegue y control de esta tarea estará a cargo del área IT Services.

Gestión de medios removibles: En La Empresa está prohibido el uso de medios removibles, entendiendo como medio removible a todos aquellos dispositivos electrónicos que almacenan información y pueden extraerse de los computadores, se harán campañas permanentes de información y toma de precaución para evitar que a través de estos dispositivos se activan riesgos que puedan afectar la disponibilidad, confidencialidad e integridad de los activos de información de la Empresa. Se podrán considerar excepciones que deberán ser identificadas, debidamente justificadas y aprobadas por el Risk Leader in Information Security and Continuity y/o el director del área.

Disposición de los activos/Respaldos a la Información: La Empresa establece los mecanismos para la adecuada custodia y disposición de los activos de información que han sido identificados y clasificados. Estos mecanismos se plasmarán en un procedimiento que describa las maneras en las cuales se ejecutará, de forma segura y correcta, la disposición final, retiro, traslado o reuso cuando ya no se requieren los activos.

Así mismo es deber de la Empresa, se ejecuta la obtención de los respaldos o backup de los activos de información ofrecidos como producto a los clientes. Se establece las directrices y procedimientos de almacenamiento de los activos de información, de manera que los respaldos se efectúen conforme la estrategia y las tecnologías en uso por la organización.

En relación con la información de los empleados en el uso de sus funciones, deben mantenerse habilitados los almacenamientos de la información directamente en los medios en la nube, conforme la herramienta colaborativa aprobada para el uso en la Empresa.

Software autorizado: La Empresa define y mantenien actualizado un listado de los productos de software de terceros autorizados para implementarse en su infraestructura tecnológica. Este control del software se ejercerá tras realizar un inventario de éste, consolidando el inventario como un activo de información de la empresa. Debe verificarse según los procedimientos de control definidos. Todo empleado que requiera de un software no listado en el inventario de software autorizado deberá hacer la petición correspondiente según procedimiento definido por las direcciones a cargo.

Redes, dispositivos móviles y de cómputo personales:

La Empresa dispone de una red inalámbrica destinada a visitantes, la cual podrá ser utilizada por empleados mediante dispositivos personales, como computadores portátiles o tabletas. En ningún caso se permite la conexión de dispositivos personales a la red corporativa. El acceso a redes inalámbricas desde teléfonos móviles se encuentra restringido. Todos los accesos serán monitoreados y auditados periódicamente para garantizar el cumplimiento de la política de seguridad de la información. El personal externo que visite las instalaciones podrá acceder a la red de visitante.

Los empleados de la Empresa tienen autorización en el ejercicio de sus funciones el uso del equipo de cómputo que se le ha asignado. El equipo de cómputo se asignará a cada empleado previa consideración de su rol y las aplicaciones y funcionalidades requeridas. Todo equipo trae instalado un sistema de seguridad informática, con base en la solución y mecanismos de protección antivirus que ha definido la Empresa. Ningún empleado puede deshabilitar en algún momento estas soluciones de seguridad y deberá monitorear y validar que el software permanezca actualizado y en servicio.

No está permitido, que ningún empleado, salvo cargos previamente autorizados por el Comité de Seguridad de la Información y Continuidad, puedan acceder a los componentes de la plataforma wolkvox desde locaciones externas a la oficina. Para ello, se deben matricular por estos roles las direcciones IP válidas desde las cuáles se permitirá el acceso a la plataforma. Sin embargo,

ante situaciones de emergencia, que imposibiliten la asistencia de los empleados a las sedes físicas de la Empresa, se levantará esta restricción de acceso de los empleados a la plataforma wolkvox, mientras dure la condición de emergencia.

Herramientas colaborativas: Entendiendo que en la Empresa se han establecido como herramienta de comunicación y de gestión de los activos de información a Google WorkSpace, es menester poder asegurar el uso de esta por los empleados conforme a los lineamientos de estas políticas, particularmente en lo referente al control de acceso. Se reitera la importancia de no compartir activos de información que no se han clasificado como Públicos por los canales colaborativos (propios o de la Empresa) que el empleado tenga habilitados en sus dispositivos personales y empresariales, entendiendo que el incumplimiento a esto se considerará como contravención a estas políticas de seguridad de la información. Se acepta el uso de las herramientas colaborativas autorizadas en la Empresa en dispositivos móviles del empleado.

Sobre el trabajo en casa y/o teletrabajo: Con base en los lineamientos que establece la normatividad colombiana diferenciando ambas modalidades de trabajo remoto para los empleados de la Empresa, se deberán identificar los riesgos generales asociados a esta modalidad de trabajo, y desarrollar los procedimientos y/o recomendaciones que posibiliten un trabajo remoto seguro para los empleados en beneficio de la Empresa y sus interesados..

Herramientas de Antivirus: La Empresa evalua, define e implementa la(s) herramienta(s) necesaria(s) para mitigar o darle tratamiento a los posibles riesgos que se desprendan del uso intensivo de sistemas informáticos conectados por redes, incluyendo la internet. Riesgos asociados a virus o malware que podrían colocar en riesgo la disponibilidad, confidencialidad e integridad de los activos de información de la Empresa. Deberán establecerselos procedimientos que aseguren la plena implementación de la solución definida en los equipos de cómputo de los empleados, su mantenimiento (incluyendo la actualización automática de manera periódica) y su uso activo y continuo. Además, deberá evaluarse la pertinencia y el nivel de riesgo y las acciones de tratamiento con este tipo de herramientas (antimalware) sobre los activos de información que soportan los productos y servicios de la Empresa provistos y ubicados en la nube.

Escritorio Limpio y Pantalla Limpia: Para lograr un adecuado aseguramiento de la información los empleados de la Empresa que tengan acceso a activos de información deberán adoptar buenas prácticas para el manejo y administración de información física y electrónica que se encuentra a su cargo en su puesto de trabajo, con el fin de evitar que personas no autorizadas accedan a dicha información. Durante los lapsos de tiempo en los que se deja desatendidos los equipos de cómputo se tendrá cuidado con bloquear la sesión del equipo, para evitar que terceros no autorizados accedan a la información.

Asimismo, establecen controles de bloqueo sobre las sesiones de los usuarios para que el equipo se bloquee en un lapso de tiempo determinado. Al imprimir información confidencial, restringida o de uso interno, los documentos deberán ser retirados de forma inmediata para evitar divulgación no autorizada de información. Los activos que contengan información confidencial, restringida o de uso interno, deberán ser almacenados en la herramienta de almacenamiento corporativo que destine la Empresa, en rutas que impidan el acceso por terceros, evitando su descarga en el equipo de cómputo. Guardar toda la documentación física y/o medio magnético en cajones, archivadores o sitios seguros, durante su ausencia del puesto de trabajo, manteniendo el mismo, libre de documentación física y medios electrónicos de almacenamiento.

7.3. Control de acceso

Se establecen a continuación las directrices con las que en la Empresa se determinan los mecanismos de protección, los límites y procedimientos frente a la administración y responsabilidad, relacionados con los accesos a la información, sin importar si estos accesos sean electrónicos o físicos. A continuación, tales políticas:

Control de acceso con usuario y contraseña: La definición de los procedimientos para la creación, modificación, suspensión o eliminación de usuarios y contraseñas en las plataformas corporativas será responsabilidad de los roles designados por la Organización en el ámbito de gestión de tecnología y seguridad de la información.

Dichos procedimientos deberán estar alineados con las políticas internas de seguridad, contemplar principios de control de acceso basado en roles (RBAC), y garantizar el cumplimiento de los requisitos establecidos por normas y estándares de la insdustria.

La ejecución de estos procedimientos podrá ser delegada a los equipos técnicos responsables, según lo determine la Organización, asegurando trazabilidad, registro y revisión periódica de las acciones realizadas.Todo usuario de los servicios tecnológicos sea este empleado, contratista u otro tercero, que tenga una cuenta y acceso a las plataformas de la Empresa, debe velar por el buen manejo del usuario y contraseña brindados, entendiendo que estos son personales e intransferibles y no deben prestarse, ni compartirse. Por ello, la Empresa debe crear y proveer para cada empleado y/o usuario, acorde con las limitaciones de acceso a los activos de información, un usuario y una contraseña para el acceso. Se definirá una línea base en la gestión de accesos a los sistemas de información de la Empresa. Es necesario además que todo usuario vigile que los accesos brindados a los activos de información correspondan a aquellos sobre los cuáles se ha otorgado acceso por motivo de sus funciones y tareas. Deben evitar acceder a activos de información que no hacen parte de la ejecución de sus funciones y tareas, reportando a su jefe inmediato los accesos no debidos que hayan identificado.

Suministro del control de acceso: Se definen procedimientos para la gestión de la asignación, modificación, revisión y revocación de derechos y privilegios de acceso para cada usuario, garantizando el cumplimiento de los controles establecidos en la gestión de identidades y accesos (IAM). Estas acciones se aplican tanto a los equipos de cómputo personal como a la plataforma Wolkvox y su infraestructura de red, conforme a los lineamientos aprobados por las áreas responsables. Se incluirán en el procedimiento, el manejo a los casos especiales como lo son usuarios con privilegios superiores utilizados para la administración de infraestructura, aplicaciones y sistemas de información de la Empresa, estipulando el alcance que se otorga sobre las plataformas a cargo, y que en ningún caso, está autorizado para, por decisión propia, eliminar, corregir o alterar registros de uso de su usuario en la plataforma, como tampoco, alterar, sin el aval del comité directivo de seguridad de la información y continuidad, la data que ha sido capturada durante la operación normal de los sistemas de información o plataformas que soportan las operaciones de la Empresa.

Gestión de Contraseñas: Siendo las contraseñas el mecanismo básico establecido para llevar a cabo la autenticación de los usuarios en los accesos a la red, aplicaciones y/o sistemas de información de la Empresa, se define que las mismas deben tener una longitud mínima de 10 caracteres, y deben incluir al menos un carácter especial, un número y mezcla de letras mayúsculas y minúsculas. Se establece como requisito general el que se configure una temporalidad a la vigencia de las contraseñas, de máximo tres meses. Así como que se exija el cambio de la contraseña una vez haya sido asignada por un administrador interno del sistema de información. Así como deshabilitar los accesos a los usuario o clientes una vez haya tenido la terminación de contrato. Es responsabilidad del Comité Directivo de Seguridad de la Información y la continuidad evaluar aquellos componentes de la plataforma en los que no es posible aplicar la política de definición de contraseñas. Con base en esta evaluación, se debe determinar el nivel de riesgo asociado y definir las acciones de tratamiento correspondientes. en .

Perímetros de Seguridad: Se establece como áreas con acceso restringido a empleados, contratistas o terceros las siguientes: el lugar dónde se encuentran ubicados los equipos de redes LAN y telecomunicaciones a internet en las sedes administrativas de la Empresa. Cualquier adición o modificación de la condición de estas áreas de seguridad física debe ser considerada por el comité directivo de seguridad de la información y continuidad, qué roles de empleados, contratistas o terceros, tendrán acceso a dichas áreas de seguridad. Así mismo, accesos a dichas áreas por parte de personas que no se encuentren dentro de los preautorizados, deben solicitar acceso a la persona que se haya delegado en cada caso, como responsable de autorizar acceso y en qué condiciones. Por ello, se debe documentar un procedimiento por el equipo de Infraestructura.

7.4. Desarrollo de software seguro.

La Empresa, consciente de la relevancia de ofrecer productos de software seguros al mercado, deberá establecer las maneras, los medios y las competencias para lograr artefactos de software seguros acorde con buenas prácticas para el desarrollo de software seguro. Para ello incorporará metodologías en la adecuada relación costo-beneficio que le permitan hacer estos desarrollos de software conforme lineamientos de la industria; así mismo, establecerá los controles para que, en la medida, que decida involucrar productos de software de terceros, estos, sean validados en su fortaleza en relación con las premisas de seguridad y/o puedan gestionarse con el proveedor para evolucionar el producto hacia la definición de software seguro que la Empresa considere.

7.5. Confidencialidad

Para la Empresa la gestión de la confidencialidad de los activos de información es tarea relevante, por ello ha establecido que todo documento que regule las relaciones de la Empresa con empleados, contratistas u otros deberá contener cláusulas de confidencialidad que habrán de establecer las condiciones para la entrega, custodia y manejo de los activos de información que podrían intercambiarse entre las partes fruto de la relación laboral o comercial. Se estipularán además las consecuencias que conlleva el manejo inadecuado de los activos de información por una de las partes.

7.6. Integridad

Para la Empresa toda información verbal, física o electrónica, debe ser adoptada, procesada y entregada o transmitida integralmente, coherentemente, exclusivamente a las personas correspondientes y a través de los medios estipulados, sin modificaciones ni alteraciones, salvo que así lo determinen las personas autorizadas y/o responsables de dicha información. En el caso de vinculación contractual, el compromiso de administración y manejo integro e integral de la información interna y externa hará parte de las cláusulas del respectivo contrato, bajo la denominación de Cláusula de integridad de la información.

7.7. Disponibilidad del servicio e información

La Empresa deberá contar con un plan de continuidad del negocio con el fin de asegurar, recuperar o restablecer la disponibilidad de los procesos que soportan el Sistema de Gestión de Seguridad de la Información y los procesos misionales de la Empresa ante el evento de un incidente de seguridad de la información.

La Empresa ha establecido unos objetivos de disponibilidad de los servicios asociados a la plataforma wolkvox, comprometiéndose con unos niveles de disponibilidad iguales o superiores al 99,9% del tiempo del mes.

Para lograr el cumplimiento de esta oferta de disponibilidad, la Empresa, debe diseñar e implementar los procedimientos de gestión, acorde con las mejores prácticas de la industria de manera que pueda gestionar los riesgos que puedan afectar el logro del objetivo de disponibilidad planteado.

Así mismo, la Empresa deberá definir los lineamientos para lograr una segregación de ambientes que permita minimizar los riesgos de puesta en funcionamiento de cambios y nuevos desarrollos con el fin de reducir el impacto de la indisponibilidad del servicio durante las fases de desarrollo, pruebas y producción. Así mismo, incorporar los lineamientos de Gestión de Cambios para que los pasos a producción afecten mínimamente la disponibilidad y se realicen bajo condiciones controladas.

7.8. Gestión de Incidentes de Seguridad de la Información

La Empresa, en cabeza de la alta dirección se compromete con el manejo idóneo de los eventos, incidentes y vulnerabilidades de seguridad de la información. Este manejo debe darse con base en las mejores prácticas y con alcance a todos los usuarios que tienen un acceso autorizado a cualquier sistema de información.

Se definira el procedimiento para el registro, atención y solución a los incidentes que tengan relación con la afectación de los activos de información propios o los de terceros que tiene bajo custodia. Se debe considerar las mejores prácticas para el manejo de la cadena de custodia de los elementos que puedan ser factor de análisis para identificar causas y responsables de los eventos presentados, y se debe documentar.

7.9. Capacitación y sensibilización en seguridad de la información

El logro de una cultura que comprenda y promueva los beneficios de la seguridad de la información es fundamental para la Empresa, pues ayudará en la disminución de las vulnerabilidades y amenazas relacionadas con las personas, por ello se ha establecido que:

- Hay un compromiso de la alta dirección en destinar los recursos suficientes para desarrollar los programas de formación a los empleados y terceros, así como al mantenimiento del sistema de gestión de la seguridad de la información.
- Deberá establecerse un programa de formación a empleados alrededor del sistema de gestión de la seguridad de la información
- Serán objeto de formación todos los empleados de la organización y serán informados los contratistas y terceros relacionados con la empresa en los lineamientos del sistema, así como en las responsabilidades que les incumbe como parte fundamental del compromiso por la seguridad de la información.
- A los empleados se les monitoreará en la asistencia a los eventos de formación alrededor del sistema de gestión de seguridad de la información que haga la Empresa, y se considerará esta actividad como elemento integrante del desempeño del empleado.
- Se deberá hacer revisión periódica de los resultados de capacitaciones en pro de lograr el mejoramiento de los procesos.

7.10. Uso de Controles Criptográficos y Gestión de Llaves

Controles Criptográficos: El comité de seguridad de la información y la continuidad será el encargado de definir los mecanismos de cifrado de información más apropiados frente a las necesidades de la Empresa, con base en el análisis de riesgos, considerando los criterios de autenticidad, confidencialidad e integridad y no repudio en las comunicaciones o en el tratamiento de la información.

Se establecen estándares de cifrado y metodologías recomendadas por la industria para los diversos activos y sistemas de información de Wolkvox, aplicando controles criptográficos donde sea pertinente. Asimismo, se consideran las disposiciones de las leyes, reglamentos y normas con las que Wolkvox ha demostrado cumplimiento, garantizando así un enfoque integral en la gestión de la seguridad de la información.

Gestión de Llaves: La Empresa debe proteger las llaves de cifrado contra la modificación y/o destrucción; las llaves secretas y las privadas, además requieren protección contra su distribución no autorizada. Con este fin deben usarse técnicas para

asegurar la integridad de la información. Se deben utilizar controles de protección física-lógica para proteger el equipo y/o sistema usado en la generación, almacenamiento y resguardo de llaves.

Los responsables de los sistemas de cifrado y de las llaves criptográficas serán los encargados de establecer los controles para asegurar el sistema y las llaves, con base en el análisis de riesgos, así como gestionar el acceso sólo a las personas autorizadas.

Estos sistemas o herramientas deberán estar incluidas en el inventario de software autorizado, y no se permitirá el uso de herramientas o sistemas de cifrado de información diferentes a los autorizados

7.11. Operación De Las Tecnologías Que Deben Seguir La Normatividad PCI-DSS

La empresa acorde con su definición estratégica de alinearse y ser cumplidora de las normas PCI-DSS deberá implementar y mantener todos los requisitos vigentes en dichas normas, garantizando su cabal cumplimiento. Dicha implementación y mantenimiento estará a cargo del equipo que brinda sostenibilidad al Sistema de Gestión de Seguridad de la información de la empresa Se establece como principio fundamental que la Empresa nunca almacenará datos de tarjetas de pago en sus componentes informáticos.

7.12. Relación con Proveedores

La Empresa debe establecer los mecanismos de control en sus relaciones con proveedores que suministren bienes o servicios que configuran o conforman las plataformas tecnológicas que son la base de la oferta de productos y servicios de la Empresa, así como los que participen en la recolección y custodia de datos personales de wolkvox y sus clientes, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por los mismos, cumplan con las políticas, normas y procedimientos de seguridad de la información y protección de datos personales. Deberán establecerse, los procedimientos que aseguren una correcta gestión de proveedores, en donde cada una de las partes interesadas expresen de manera explícita el seguimiento a los estándares de industria alrededor de la seguridad de la información o la conformidad con las buenas prácticas entorno a la seguridad de la información establecidas por Wolkvox.

Cualquier acceso por parte de un proveedor a los activos de información de la Empresa, debe de haber cumplido con una adecuada gestión de los riesgos y con las autorizaciones respectivas por parte de los propietarios de la información.

Al momento de terminar relaciones con un proveedor el cual maneje información de la Empresa, aquel debe destruir de una forma segura la información o en su defecto devolver la información, proceso que deberá estar incluido en el contrato con el proveedor.

7.13. Borrado Seguro de la Información

La Empresa establece lineamientos y procedimientos de borrado seguro de la información, considerando las operaciones de clientes y su data, bajo la premisa de mantener por un periodo de tiempo, según definiciones comerciales.

7.14. Contact Center as a Service

La gestión de la seguridad en el entorno **Contact Center as a Service (CCaaS)** se rige bajo un modelo de responsabilidad compartida entre Wolkvox, sus clientes y Google Cloud Platform (GCP), proveedor de la infraestructura en la nube.

En el marco del modelo de responsabilidad compartida, contar con Google Cloud Platform (GCP) como aliado estratégico permite a Wolkvox alojar sus servicios y aplicaciones, en la infraestructura en la nube confiable, segura y de alto rendimiento. Como parte de nuestro compromiso con la calidad del servicio, Wolkvox realiza un monitoreo constante a sus proveedores, implementando controles, mecanismos de seguimiento y procesos de validación que aseguran el cumplimiento de los estándares exigidos, con el mismo nivel de compromiso y rigurosidad que caracteriza a la compañía. Esta vigilancia activa es clave para

mantener la confianza de nuestros clientes y garantizar la continuidad, seguridad y excelencia en la prestación de nuestros servicios.Las certificaciones de cumplimiento y los informes detallados sobre sus centros de datos están disponibles públicamente en los portales oficiales de GCP:

- Modelo de responsabilidad compartida GCP
- Cumplimiento y certificaciones GCP

Wolkvox es responsable de la seguridad de los servicios que desarrolla y gestiona en la nube, tales como **Wolkvox Contact Center** y **Wolkvox CRM**. Esta responsabilidad incluye la protección de la información, la gestión de configuraciones y accesos, y la aplicación de controles de seguridad en el desarrollo e integración de sus soluciones.

Los clientes son responsables de la seguridad de los datos que gestionan dentro de la plataforma, así como de configurar correctamente los accesos y permisos de los usuarios finales.

Wolkvox ha definido un lineamiento para la selección de proveedores de servicios en la nube, que establece criterios y actividades orientadas a garantizar la **confidencialidad, integridad y disponibilidad** de los servicios contratados.

La compañía cumple con estándares internacionales de seguridad de la información, contando con certificaciones en **ISO/IEC 27001** y **PCI-DSS**, aplicables a su oferta CCaaS.

7.14.1. Controles de Seguridad Específicos:

7.14.1.1. **Detección de amenazas y vulnerabilidades:** Se utiliza la plataforma **Google Cloud Security Command Center**, que permite identificar, detectar y analizar amenazas y vulnerabilidades en tiempo real.

7.14.1.2. **Pruebas de penetración (Pentesting):** Se realizan dos pruebas externas anuales sobre la plataforma CCaaS, con el fin de identificar posibles brechas de seguridad y garantizar el cumplimiento del Sistema de Gestión de Seguridad de la Información (SGSI).

7.14.1.3. **Análisis de vulnerabilidades:** Se ejecutan análisis bimestrales para fortalecer la confiabilidad, integridad y disponibilidad de la plataforma, mitigando riesgos potenciales.

7.14.1.4. **Monitoreo:** Se emplean herramientas de monitoreo continuo que permiten supervisar el rendimiento y la disponibilidad de los servicios ofrecidos en la infraestructura CCaaS.

7.14.1.5. Seguridad en la nube : Wolkvox tiene un procedimiento de creación y hardening de servidores, donde se define Creación red VPC en GCP Wolkvox" el cual se describe los lineamientos de las reglas de IAP,VPC, IPTABLES para el fortalecimiento de los servidores.

7.14.1.6. Seguridad en Firewall. Wolkvox utiliza el servicio de firewall en sus sedes administrativas y los servicios de Google Cloud para la plataforma de Contact Center as a Service CCaaS que protege del tráfico no autorizado.

7.14.1.7. **Continuidad del negocio y recuperación ante desastres:** Los servicios están desplegados en múltiples regiones de GCP, asegurando alta disponibilidad (SLA del 99,9 %). Además, se cuenta con un plan de recuperación ante desastres que se prueba semestralmente para validar su eficacia en escenarios de interrupción operativa.

8. Seguimiento

Este documento de políticas deberá ser revisado al menos una vez al año por el comité directivo de seguridad de la información, o antes cuando se haga evidente que las políticas definidas deben revisarse y/o ajustarse para asegurar la confidencialidad, integridad y disponibilidad de los activos de información de la empresa.

9. Derechos de Autor y/o Cibergrafía

Este documento se ha construido por Wolkvox S.A.S. considerando las directrices establecidas por el Ministerio de las TIC en Colombia en su Guía No. 2 – Elaboración de la Política General de la Información. El documento referenciado está basado en buenas prácticas y estándares internacionales de la industria (ISO/IEC 27001, ISO/IEC 27017) y por ello, tiene plena cobertura

para atender la necesidad de nuestros clientes en torno a los lineamientos que sigue la Empresa en relación con la Seguridad de la Información.

Versión	Fecha	Comentarios
Versión actual (v. 5)	**jul 04, 2025 10:10**	**Gestion Documental** : Se ajusta el numeral 7.2 Redes, dispositivos móviles y de cómputo personales, se ajusta a la gestión actual de wolkvox. Se aplica anotación en el caso: PET-25627144836721.
v. 4	jul 03, 2025 14:16	Gestion Documental 1. Se elimina: - Proteger la información personal según el reglamento general de protección de datos (GDPR) y las leyes aplicables en los países miembros de la comunidad europea - Proteger los datos de tarjetas de pago según lo establecido en la norma PCI-DSS. - Resguardar la información de salud protegida según lo establecido en la ley HIPAA del gobierno de los Estados Unidos. 2. Se adiciona : - Garantizar el cumplimiento de la normativa legal aplicable, tanto a nivel nacional como internacional, conforme a las obligaciones que Wolkvox haya adoptado voluntariamente o que le sean exigibles. - Se redacta la política en tiempo presente. Aprobado por Juan Acevedo el 02/07/2025. Igualmente, se compartió a los miembros del comité de seguridad de la información y continuidad sin obtener respuesta con observaciones y/o comentarios, por lo cual, se da por aprobado el documento. Caso: PET-25627144836721.
v. 3	jul 01, 2025 16:03	Juan Guillermo Ramire Se elimina Proteger la información personal según el reglamento general de protección de datos (GDPR) y las leyes aplicables en los países miembros de la comunidad europea ▪ Proteger los datos de tarjetas de pago según lo establecido en la norma PCI-DSS. ▪ Resguardar la información de salud protegida según lo establecido en la ley HIPAA del gobierno de los Estados Unidos. Cumplir con los controles de seguridad basados en 27017 para los servicios en nube. Se adiciona Garantizar el cumplimiento de la normativa legal aplicable, tanto a nivel nacional como internacional, conforme a las obligaciones que Wolkvox haya adoptado voluntariamente o que le sean exigibles Se redacta la política en presente.
v. 2	jun 20, 2025 08:43	Gestion Documental 1.Se migra a Confluence. 2. Se ajusta el logo, colores y diseño según lo definido por la gerencia general. 3. Se ajusta la presencia de cargos en la política con el fin de no particularizar la responsabilidad, ya que esta se define en los procedimientos y lineamientos definidos internamente. 4. Además, se realizan los siguientes ajustes y/o inclusiones: - Política General de Seguridad de la Información: se adicionan las normativas HIPAA y GDPR. - Redes, dispositivos móviles y de cómputo personales: ajustes en lineamientos y controles. - Control de acceso: se actualiza el apartado de usuario y contraseña, así como el proceso de suministro del acceso. - Cambio de nomenclatura en perfiles: se actualizan nombres de roles/perfiles para mayor claridad. - Uso de controles criptográficos y gestión de llaves: incorporación de nuevos controles. - Seguridad en la nube para servicios CCAAS: inclusión de controles específicos conforme a la norma ISO/IEC 27017. Aprobado por el comité directivo, se envía correo por parte de Juan Ramírez, Risk in Information security and Continuity. Caso: PET-2493162425393.
v. 1	jun 20, 2025 08:40	Gestion Documental Se migra el documento a Confluence.