CONTENIDO

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

Activo de Información: corresponde a toda unidad completa de datos o información que se ha identificado como existente en la empresa, bien sea porque ha sido creada en la misma, o ha sido recibida de terceros y es parte de los procesos de gestión que debe ejecutar la Empresa en su cotidianidad. Los activos son los recursos del Sistema de Seguridad de la Información necesarios para que la Empresa funcione y logre los objetivos que ha propuesto la alta dirección.
Cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de la Empresa y, en consecuencia, debe protegerse.

Amenaza: Factor externo que aprovecha una debilidad en los activos de información y puede impactar en forma negativa en la organización. No existe una única clasificación de las amenazas, lo importante es considerarlas todas a la hora de su identificación.

Antivirus: Es un tipo de software que se utiliza para evitar, buscar, detectar y eliminar malware de una computadora. Una vez instalados, la mayoría de los software antivirus se ejecutan automáticamente en segundo plano para brindar protección en tiempo real contra ataques maliciosos. Adicionalmente, ayudan a resguardar los archivos y el hardware de la ejecución de malware, como gusanos, troyanos y programas espía.

Autenticación: Es el procedimiento de comprobación de la ID de un usuario o recurso/sistema tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

Autenticidad: Propiedad que garantiza que la identidad de un sujeto o recurso es la que declara.

Cadena de Custodia: Registro detallado del tratamiento de la evidencia en el proceso de atención a un incidente en seguridad, incluyendo quienes, cómo y cuándo la transportaron, almacenaron y analizaron, a fin de evitar alteraciones o modificaciones que comprometan la misma.

Características de la Información: Las principales características son la confidencialidad, la disponibilidad y la integridad.

CCTV: Es una sigla en inglés "*closed circuit television*" que traducido al español es "circuito cerrado de televisión", consiste en una o más cámaras de vigilancia conectadas a uno o más monitores de vídeo o televisores que reproducen las imágenes transmitidas por las cámaras.

Centro de cómputo: Es un área específica que destinan las compañías para el almacenamiento de múltiples equipos de cómputo para la operación de sus procesos informáticos. Estos equipos se encuentran conectados entre sí a través de una red de datos. El centro de cómputo deberá cumplir ciertos estándares de industria con el fin de garantizar básicas condiciones de seguridad, disponibilidad y continuidad, entre ellas, el tener los controles de acceso físico, materiales de paredes, pisos y techos retardantes en relación con la inflamabilidad. Suministro de alimentación eléctrica principal y alterna, condiciones medioambientales adecuadas, entre otros.

Centros de cableado: Son cuartos de la empresa donde se podrán instalar los dispositivos de comunicación y tienen llegada los cables eléctricos y/o de datos que cubren los espacios de la sede de la empresa. Al igual que los centros de cómputo, los centros de cableado deben cumplir requisitos de control de acceso físico, condiciones de materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.

Ciberseguridad: Conjunto de elementos, medidas y equipos destinados a controlar la seguridad informática de una entidad o espacio virtual.

Cifrado: Es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.

Compromiso de la Dirección: Es la actitud y la obligación que se adquiere por parte del primer nivel de dirección de la compañía respecto al establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI.

Confiabilidad: Se define como la probabilidad en que un producto realizará su función prevista sin incidentes por un período de tiempo especificado y bajo condiciones indicadas.

Confidencialidad: Es el nivel de acceso otorgado a la información para que sea accedida solo por quienes estén autorizados.

Contención: Acción que se formula o implementa para evitar que el incidente siga ocasionando daños.

Control de Acceso: Es la habilidad de permitir o denegar el uso de un recurso particular a una entidad en particular.

Control: Es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

Criptografía: Es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.

Custodio del activo de información: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado.

Disponibilidad: Es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

Equipo de cómputo: Dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

Erradicación: Eliminar la causa del incidente y todo rastro de los daños.

Estándar: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.

Evento de seguridad: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad. [ISO/IEC 27000:2009]

Gestión de Incidentes: Es el conjunto de todas las acciones, medidas, mecanismos, recomendaciones, tanto proactivos, como reactivos, tendientes a evitar y eventualmente responder de manera eficaz y eficiente a incidentes de seguridad que afecten activos de una empresa, minimizando su impacto en el negocio y la probabilidad que se repita.

Fuga de información: Incidente que pone en poder de una persona o entidad ajena a la organización, información confidencial y que sólo debería estar disponible para integrantes de esta (tanto de todos como de un grupo reducido). Este tipo de incidente puede ser tanto interno como externo, y a la vez generado de forma intencional o no.

Firewall: Un firewall es un dispositivo de seguridad de la red que monitorea el tráfico de red entrante y saliente y decide si permite o bloquea tráfico específico en función de un conjunto definido de objetivos de seguridad.

Guía: Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares, buenas prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, se seguirán a menos que existan argumentos documentados y aprobados para no hacerlo.

Hash: Función computable mediante un algoritmo, que tiene como entrada un conjunto de elementos, que suelen ser cadenas, y los convierte (mapea) en un rango de salida finito, normalmente cadenas de longitud fija.

Ingeniería Social: En el campo de la seguridad informática, es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos ganando su

confianza muchas veces, con el fin de obtener información, acceso o privilegios en sistemas de información que les permiten realizar algún acto que perjudique o exponga a la persona o a la organización a riesgos y/o abusos.

IDS**:** Sistema de detección de intrusos.

IPS: Sistema de prevención de intrusos.

Impacto: Consecuencias que produce un incidente de seguridad sobre la organización.

Incidente de seguridad de la información: Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad: Es la protección de la exactitud y estado completo de los activos.

Log's: Registro de los sistemas de información que permite verificar las tareas o actividades realizadas por determinado usuario o sistema.

Malware: Es un término general para referirse a cualquier tipo de "*malicious software*" (software malicioso) diseñado para infiltrarse en un dispositivo sin conocimiento previo del usuario. Hay muchos tipos de malware y cada uno busca sus objetivos de un modo diferente. Sin embargo, todas las variantes comparten dos rasgos definitorios: funcionan de forma oculta y trabajan activamente en contra de los intereses de la persona, entidad o dispositivo atacado.

Medio removible: Es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información. Los medios removibles incluyen cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.

Mejor Práctica: Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.

Partner: Persona jurídica o natural con la que Wolkvox ha establecido un acuerdo para que pueda ofrecer, vender y mantener el portafolio de las soluciones wolkvox.

Phishing: Es un tipo de delito encuadrado dentro del ámbito de las estafas. Se vale de técnicas como la ingeniería social, haciéndose pasar por una persona o empresa de confianza en una aparente comunicación electrónica, con el objetivo de adquirir información confidencial de forma fraudulenta.

Plan de continuidad del negocio (*Business Continuity Plan*): Plan orientado a permitir la continuidad de las funciones operativas de la organización, en caso de un evento imprevisto que las ponga en peligro.

Procedimiento de Gestión de Riesgos en Seguridad de la Información y Continuidad: Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Política: Declaración de alto nivel que describe la posición de la Empresa sobre un tema específico.

Política de seguridad: Documento que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información.

Política de escritorio limpio: Es aquella que indica a los empleados, clientes, proveedores y demás colaboradores, que deben dejar su escritorio libre de cualquier tipo de informaciones susceptibles de mal uso al finalizar su jornada laboral.

Procedimiento: Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la Empresa, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro del a dependencia donde ellos se aplican.

Propietario de la información: Es la unidad organizacional o proceso donde se crean los activos de información y se mantiene la propiedad de estos, para modificarlos, eliminarlos o compartirlos.

Recuperación: Volver el entorno afectado a su estado natural.

Responsable por el activo de información: Es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Riesgo Residual: Según [ISO/IIEC Guía 73:2002] Es el riesgo que permanece tras el tratamiento del riesgo.

Segregación de tareas: Separar tareas sensibles entre distintos empleados, clientes, proveedores u otros con alguna relación contractual con la Empresa para reducir el riesgo de un mal uso, deliberado o por negligencia, de los sistemas e informaciones.

Sistema de información: Es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por la empresa o de origen externo ya sea adquirido por la empresa como un producto estándar de mercado o desarrollado para las necesidades de ésta.

Spamming: Se llama spam, correo basura o sms basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming. La vía más usada es el correo electrónico.

Sniffer: Software que captura los paquetes que viajan por la red para obtener información de la red o del usuario.

Spoofing: Falsificación de la identidad origen en una sesión. La identidad es por una dirección IP o Mac *Address*.

SGSI: Sistema de gestión de la seguridad de la información

Tratamiento de riesgos: Según [ISO/IEC Guía 73:2002]: Proceso de selección e implementación de medidas para modificar el riesgo.

Validación: Garantizar que la evidencia recolectada es la misma que la presentada ante las autoridades.

Virus: En adelante nos referiremos a “malware”. Ver dicha definición en este glosario.

Vulnerabilidad: Condición que podría permitir que una amenaza se materialice con mayor frecuencia, con mayor impacto o ambas. Una vulnerabilidad puede ser la ausencia o debilidad en los controles administrativos, técnicos y/o físicos.

PCI-DSS: El Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (Payment Card Industry Data Security Standard) o PCI DSS fue desarrollado por un comité conformado por las compañías de tarjetas (débito y crédito) más importantes, comité denominado PCI SSC (Payment Card Industry Security Standards Council) como una guía que ayude a las organizaciones que procesan, almacenan y/o transmiten datos de tarjetahabientes (o titulares de tarjeta), a asegurar dichos datos, con el fin de evitar los fraudes que involucran tarjetas de pago débito y crédito.

CHD: Siglas del inglés. "Cardholder Data" (' Datos de la tarjeta/Datos de la tarjeta del cliente)'). Como requisito mínimo, los datos de la tarjeta incluyen el número de cuenta principal (PAN) y además pueden incluir la fecha de vencimiento y el nombre del titular de tarjeta. El PAN se encuentra en el anverso de la tarjeta y codificado en la banda magnética de la tarjeta o en el chip inserto en su interior. También conocido como datos del titular de la tarjeta. Además, consulte los Datos confidenciales de autenticación para ver cuáles son otros elementos de datos que pueden ser parte de una transacción de pago, pero que no deben almacenarse después de que se autoriza la transacción.

PAN**:** Acrónimo de "Primary Account Number" (Número de cuenta principal)'). Número único para tarjetas de débito y crédito que identifica la cuenta del titular de tarjeta.

SAD**:** Acrónimo de "Sensitive Authentication Data" ('datos de autenticación confidenciales'), incluye la información de la cinta magnética, el PIN (NIP) o el bloque PIN (NIP), así como el valor de autorización de Tarjeta-no-presente al cual nos referiremos como CVV2 pero puede tomar cualquiera de los siguientes acrónimos: CAV2/CVC2/CVV2/CID.

SPT**:** Siglas del Inglés. "Store, Process, or Transmit" ('almacenar, procesar o transmitir'), lo que significa que un sistema o proceso entra en contacto con CHD y / o SAD y, por lo tanto, está automáticamente dentro del alcance (Procesos, Personas, Tecnología).

CDE**:** Siglas del inglés. "Cardholder Data Environment" ('entorno de datos del titular de la tarjeta'), básicamente lo que estamos tratando de proteger, que comienza con los sistemas que: SPT CHD o SAD, pero no se limita a estos.

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 cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

El incumplimiento a la política de Seguridad de la Información traerá consigo, las consecuencias legales y disciplinarias que apliquen a la normativa de la compañía, incluyendo lo establecido en las normas que competen al gobierno nacional y territorial en cuanto a Seguridad de la Información se refiere.

Para el presente documento existirán excepciones, las cuales contarán con la aprobación de la Gerencia General o del Comité Directivo de Seguridad 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 las leyes en Colombia, 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 busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición 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 defina 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 (SGSI) 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.
- Proteger los datos de tarjetas de pago según lo establecido en la norma PCI-DSS.
- 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 SGSI de WOLKVOX:

6.1. WOLKVOX ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información (SGSI), 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 SGSI, 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 protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de estos.

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

6.6. WOLKVOX protegerá 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 protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

6.8. WOLKVOX controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos que soportan sus operaciones.

6.9. WOLKVOX implementará control de acceso a la información, sistemas y recursos de red, considerando principios 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 garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
6.11. WOLKVOX garantizará 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 garantizará 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 garantizará 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 SGSI 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 Operations Director, el Software Engineering and Infrastructure Director, el Risk Leader in Information Security and Continuity, el Administration Director, el Global Sales and marketing Director, y el Human Resources Director.

Este comité se encargará 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 la norma PCI-DSS sobre los entornos que determine la Empresa, 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 deberá reunir 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 hacer 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 será levantado por el Risk Leader in Information Security and Continuity, y 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 deberá llevar 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 definido por el Risk Leader in Information Security and Continuity. 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 definido por el Líder de Riesgos en Seguridad de la Información y Continuidad.

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 IT Services Manager y del área de Ingeniería de Software e Infraestructura.

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 activen 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 debe establecer 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 re uso cuando ya no se requieran los activos.

Así mismo es deber de la Empresa, a través de las actividades que lleve a cabo el área de Ingeniería de Software e Infraestructura en cabeza del IT Infrastructure Lead , ejecutar la obtención de los respaldos o backup de los activos de información ofrecidos como producto a los clientes. Deberá establecerse por el IT Infrastructure Lead, 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, deberán 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 deberá definir y mantener 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 este entre la dirección de Operaciones TIC e Ingeniería de Software e Infraestructura, consolidándose el inventario como un activo de información de la Empresa. Debe verificarse según los procedimientos de control que despliegue el Risk Leader in Information Security and Continuity. 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: Se establece que, en la Empresa, los empleados podrán acceder a las redes inalámbricas desde sus equipos de cómputo portátiles, entendiéndose que tendrán acceso mínimo a una conexión desde su puesto de trabajo. No está permitido que se acceda a las redes inalámbricas de la Empresa desde teléfonos móviles, tabletas u otros dispositivos personales. Así mismo se establece que los empleados, a través de las redes de datos de la Empresa y de los enlaces a internet provistos por la Organización, podrán solo acceder a las cuentas de correo de la Empresa, y, aquellos roles autorizados a la plataforma productiva en internet, para cada uno de los ambientes a los que tiene el acceso otorgado.

Podrán los visitantes a las sedes de la Empresa acceder a una red inalámbrica de visitantes configurada con tal propósito y solo bajo autorización del Software Engineering and Infrastructure Director o su delegado, desde equipos de cómputo personales. Nunca podrán acceder a la red principal de datos de la Empresa. Se restringe a los visitantes el acceso a las redes inalámbricas desde teléfonos móviles.

Los empleados de la Empresa tienen autorización en el ejercicio de sus funciones sólo del uso del equipo de cómputo que se le ha asignado. No está permitido el uso, la conexión a la red de la Empresa ni la descarga de los activos de información de la Empresa en equipos de cómputo personales. El equipo de cómputo personal 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. Se delega estas actividades de definición, configuración y monitoreo al IT Services Manager.

No está permitido, que ningún empleado, salvo el CEO y el IT Infrastructure Lead, y su equipo, 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. El IT Infrastructure Lead junto con el IT Services Manager deberán definir e implementar los procedimientos necesarios para instrumentar las definiciones aquí planteadas.

Herramientas colaborativas: Entendiendo que en la Empresa se han establecido como herramientas fundamentales de comunicación y de gestión a los activos de información una o varias plataformas colaborativas (Google WorkSpace y Microsoft Teams), es menester poder asegurar el uso de estas 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 de telefonía 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. El Risk Leader in Information Security and Continuity realizará esta evaluación de riesgos con el apoyo del área de Gestión Humana.

Herramientas de Antivirus: La Empresa debe evaluar, definir e implementar 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 establecerse, por el IT Services Manager, los 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 en conjunto con el Risk Leader in Information Security and Continuity y el IT Infrastructure Lead,, 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, el área de Operaciones TIC es la encargada de establecer 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: Es responsabilidad del Software Engineering and Infrastructure Director y del IT Services Manager la definición de los procedimientos para llevar a cabo la creación, modificación, suspensión o eliminación de

usuarios y contraseñas sobre las plataformas a cargo. Tales procedimientos serán desplegados por el Technical Support Leader y/o el IT Infrastructure Leadde la Empresa. 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 y al Risk Leader in Information Security and Continuity los accesos no debidos que hayan identificado.

Suministro del control de acceso: En cabeza del Technical Support Leader (para los equipos de cómputo personal) y del IT Infrastructure Lead (para la plataforma wolkvox, y la infraestructura de red) de las áreas de Operaciones TIC e Ingeniería de Software e Infraestructura de la Empresa, con el aval del IT Services Manager, del IT Infrastructure Lead , o en su defecto, del IT Operations Director y del Software Engineering and Infrastructure Director, está la definición de los procedimientos para la gestión de asignación, modificación, revisión o revocación de derechos y/o privilegios a cada uno de los usuarios creados. 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 8 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. Es labor del Risk Leader in Information Security and Continuity de la Empresa junto con el IT Infrastructure Lead identificar los componentes de la plataforma sobre los cuáles no es posible la asignación de esta definición de contraseñas, e informar al comité directivo de seguridad de la información, para que se evalúe el riesgo y se determine la acción de tratamiento posible.

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, y debe ser documentado por la Dirección de Ingeniería de Software e Infraestructura 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 99,6% del tiempo del mes.

Para lograr el cumplimiento de esta oferta de disponibilidad, la Empresa, en cabeza de la Dirección de Operaciones TIC 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, en cabeza de la Dirección de Ingeniería de Software e Infraestructura 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.

Es responsabilidad del Risk Leader in Information Security and Continuity, así como del IT Services Managerdefinir 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.

Es la responsabilidad del Risk Leader in Information Security and Continuity presentar al comité directivo de seguridad y continuidad un informe mensual de los eventos registrados, el tratamiento dado y las acciones de gestión del riesgo que se viene formulando para la mitigación de tales riesgos.

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 a cargo del área de Gestión Humana en la empresa.
- 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: Las Direcciones de Operaciones TIC, Ingeniaría de Software e Infraestructura y el Risk Leader in Information Security and Continuity , serán los encargados de definir los mecanismos de cifrado de información más apropiados frente a las necesidades de la Empresa, con base en el análisis de riesgos en seguridad de la información y continuidad, considerando los criterios de autenticidad, confidencialidad e integridad y no repudio en las comunicaciones o en el tratamiento de la información.

Como estándar de cifrado se establecen las siguientes metodologías recomendadas por la industria **(AES, 3DES con una dimensión a partir de 256 bits y RSA con una dimensión a partir de 2048 bits)** para los diferentes activos y sistemas de información pertenecientes a Wolkvox en donde sea pertinente aplicar el uso de controles criptográficos. Adicionalmente se tienen en cuenta la normatividad colombiana vigente frente a la protección de los datos, estándares aplicables y la tecnología existente.

Gestión de Llaves: Las Direcciones de Operaciones TIC, Ingeniería de Software e Infraestructura y el Risk Leader in Information Security and Continuity serán los encargados de definir las directricesde las llaves de cifrado. Asimismo, 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 realizado por el Risk Leader in Information Security and Continuity, 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 da la información de la empresa en cabeza del IT Operations Director y el Risk Leader in Information Security and Continuity. 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, por la Dirección Administrativa, 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 por parte del Risk Leader in Information Security and Continuity 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 deberá establecer unos 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.

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. (en adelante, WOLKVOX o la Empresa), 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 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.