1. OBJETIVO

Establecer los lineamientos en seguridad de la información que deben seguir los colaboradores, proveedores, contratistas y demás partes interesadas internas y externas de WEKALL, con el fin de garantizar la confidencialidad, integridad y disponibilidad de los activos de información a los que tienen acceso.

2. ALCANCE

Este documento describe las políticas de seguridad de la información establecidas por WEKALL, teniendo en cuenta los controles definidos en el Anexo A de la norma ISO/IEC 27001:2013, la ley estatutaria de protección de datos personales (Ley 1581 de 2012), sus decretos reglamentarios, y demás legislación aplicable en Colombia.

Estas políticas se aplican en todo el ámbito del Sistema de gestión de seguridad de la Información-SGSI de WEKALL, a sus procesos y personal con algún tipo de vínculo contractual; por tal motivo, tanto el Gerente, como los líderes de proceso, colaboradores, proveedores y demás partes interesadas internas y externas, independientemente de su nivel jerárquico, son responsables del cumplimiento de estas políticas de seguridad de la información.

3. COMPROMISO DE LA DIRECCIÓN

La Gerencia de WEKALL aprueba este Manual de políticas de Seguridad de la Información como muestra de su compromiso y apoyo en el diseño e implementación de controles, que garanticen la seguridad de la información en la Organización.

4. TÉRMINOS Y DEFINICIONES

Activo de información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal. [Modelo de Seguridad y Privacidad de la Información 3.0.2].

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. [ISO/IEC 27000:2012].

Auditoría: Inspección formal para verificar si se está siguiendo/cumpliendo un estándar o un conjunto de guías, que sus registros son precisos o que las metas de eficiencia y efectividad se están

cumpliendo. [ITIL® Español (España) glosario, v1.0].

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. [Guía ISO 73: 2009]

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, empresas o procesos no autorizados. [ISO/IEC 27000:2012].

Control: Medios de gestión del riesgo, incluidas las políticas, procedimientos, directrices, prácticas y estructuras organizativas, que pueden ser de carácter administrativo, técnico, de gestión o jurídico. [ISO/IEC 27000:2012].

Control de acceso: mecanismo de control para el acceso a los recursos de un sistema computarizado; un control físico o lógico diseñado para proteger contra usos o entradas no autorizadas. El control de acceso puede ser definido por el sistema (Mandatory Access control – MAC), o definido por el usuario propietario del objeto (discretionary Access control – DAC).

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una empresa autorizada. [ISO/IEC 27000:2012].

Encriptación (Cifrado, codificación): La encriptación es el proceso para volver ilegible información considera importante. La información una vez encriptada sólo puede leerse aplicándole una clave.
Se trata de una medida de seguridad que es usada para almacenar o transferir información delicada que no debería ser accesible a terceros. Pueden ser contraseñas, números de tarjetas de crédito, conversaciones privadas, etc.

Gestión de activos: Es una actividad genérica o proceso responsable del seguimiento y la notificación del valor y la propiedad de los activos a lo largo de su ciclo de vida. [ITIL® Español (España) glosario, v1.0].

Gestión de cambios: Proceso responsable del control del ciclo de vida de los cambios, permitiendo la ejecución de los cambios beneficiosos minimizando el impacto en los servicios de TI. [ITIL® Español (España) glosario, v1.0].

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperada o no deseado que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. . [ISO/IEC 27000:2012].

Información: En relación con la seguridad de la información, se refiere a cualquier información o

elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. [ISO/IEC 27000].

Integridad: Propiedad de exactitud y completitud de la información. [ISO/IEC 27000:2012].

Internet: El sistema único, interconectado, mundial de redes informáticas comerciales, gubernamentales, educativas y de otro tipo que comparten (a) el conjunto de protocolos especificado por Internet Architecture Board (IAB) y (b) los espacios de nombres y direcciones administrados por Internet Corporation para Nombres y Números Asignados (ICANN). [CSRC NIST]

Monitoreo: Verificación, supervisión, observación crítica o determinación continúa del estado, con el fin de identificar cambios respecto al nivel de desempeño exigido o esperado. [ISO/IEC 27000:2012]

Parte interesada: Persona u organización que puede afectar, verse afectada o percibirse afectada por una decisión o actividad. [ISO/IEC 27000:2012]

Política: Intención y dirección generales expresadas formalmente por la Dirección. [ISO/IEC 27000:2012]

Procedimiento: Manera especificada de llevar a cabo una actividad o un proceso. [ISO/IEC 27000:2012]

Prueba: Una actividad que verifica que un elemento de configuración, servicio de TI, proceso, etc. cumple con sus especificaciones o requerimientos acordados. [ITIL® Español (España) glosario, v1.0]

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. [ISO/IEC 27000:2012].

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. [ISO/IEC 27000:2012].

Sistema de Información: Conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes que manejan información. [ISO/IEC 27000:2012].

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o empresa. [CESID:1997]

VPN: En informática, acrónimo del Ingles Virtual Prívate Networks, es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, por ejemplo, Internet manteniendo y garantizando la protección de la información.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. [ISO/IEC 27000:2012].

5. MEDIDAS A ADOPTAR EN CASO DE INCUMPLIMIENTO

El incumplimiento de una o más políticas descritas en este documento, está sujeto a las sanciones disciplinarias, fiscales y penales que se deriven de la conducta del implicado, incluso cuando se encuentre en situaciones administrativas como permisos, licencias, vacaciones, suspensiones en ejercicio del empleo, de acuerdo con la legislación colombiana aplicable.

6. NORMATIVA

Ver documento “Normograma”.

7. CONTEXTO

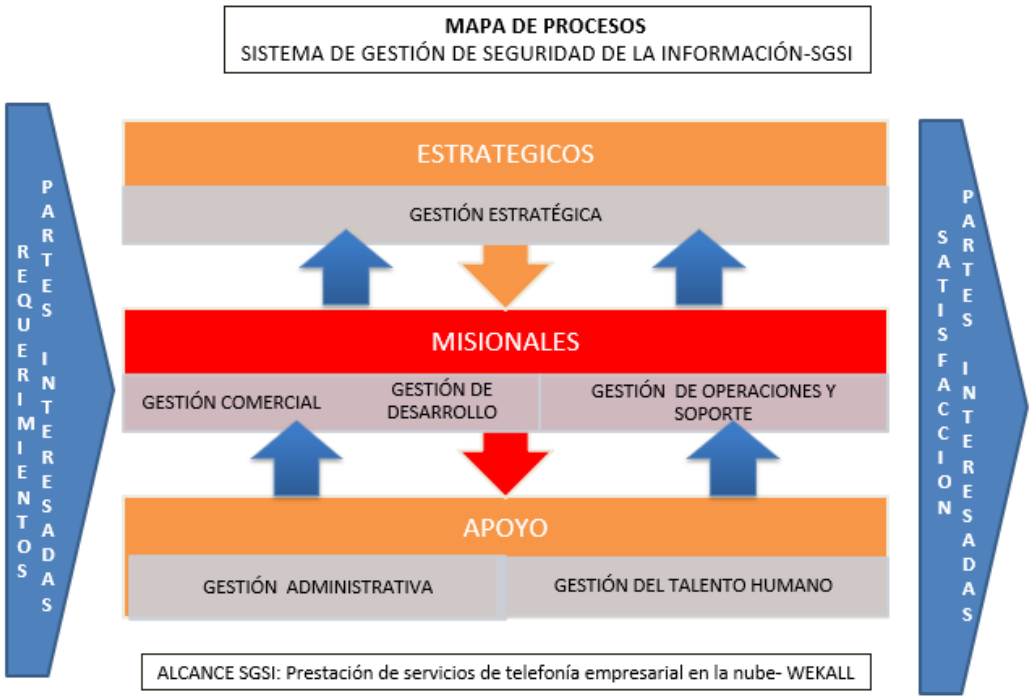
Los servicios de la nube constituyen parte importante para la transformación digital de las empresas. Gracias a ellos, es que la accesibilidad y flexibilidad en ciertos procesos, se dan de manera más fluida y a un costo mínimo de inversión inicial.

Según Forrester, empresa de investigación de mercados, ha predicho que más del 50% de las empresas empezarán a usar aplicaciones de la nube para mejorar la calidad de sus servicios. También los gastos relacionados con la computación en la nube incrementarían a una cantidad increíble para el 2020. Cifras que son entre 4 o 5 veces más altas si se comparan a las del 2009.

La Telefonía en la Nube es la evolución de la telefonía para empresas. Se pasa de un modelo tradicional que requería inversión inicial, tiempo de implementación y gastos de mantenimiento, a un modelo SaaS (Software as a Service) que es el modelo que ofrecen los prestadores de Central Virtual. Esto es, el servicio que se presta a través de un abono mensual, de implementación inmediata y sin necesidad de invertir. Los prestadores dan el servicio a través de un sistema de software, mediante un abono mensual recurrente y por eso entra dentro de la categoría de los modelos SaaS.

WEKALL establece e implementa el Sistema de Gestión de la Seguridad de la Información, alineado a su visión, estrategia, valores y misión, con el fin de preservar la confidencialidad, integridad, disponibilidad de la información y en cumplimiento de la normatividad legal.

En el siguiente mapa se observan las interrelaciones entre los procesos de la empresa sobre los cuales actúa el Sistema de Gestión de Seguridad de la Información de WEKALL:



8. ORGANIZACIÓN DE LA SEGURIDAD

8.1. ROLES Y RESPONSABILIDADES

Los roles y responsabilidades del Sistema de Gestión de Seguridad de Información se encuentran definidos en el documento “ROLES Y RESPONSABILIDADES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – SGSI EN WEKALL”.

8.2. SEPARACIÓN DE DEBERES

- Todo aquel que tenga acceso a la información de WEKALL, debe tener claramente definidas sus funciones y responsabilidades, teniendo en cuenta reducir el uso no autorizado, indebido o accidental de los activos de información.

- Todos los sistemas de información de la organización, deben implementar reglas de acceso, de forma que, haya segregación de funciones entre quien administre, opere, mantenga, audite, y, en general, tenga la posibilidad de acceder a los sistemas de información, así como entre quien otorga los privilegios y quien lo utiliza.

8.3. CONTACTO CON AUTORIDADES Y GRUPOS DE INTERÉS

- WEKALL mantendrá contacto actualizado con las autoridades competentes para el cumplimiento de la ley, organismos de control y autoridades de supervisión correspondientes. Para ello, se definirá un listado de autoridades a contactar en caso de que se sospeche de la violación de la ley o se confirme una situación de amenaza para la organización.
-
- El proceso de Gestión de operaciones y soporte en conjunto con el Oficial de Seguridad de la Información o quien haga sus veces, mantendrá contacto con grupos de interés especial, foros y asociaciones profesionales en el campo de la seguridad de la información. Lo anterior con el fin de estar al día con la información relacionada con la seguridad de la información y recibir advertencias de actualizaciones, ataques, y vulnerabilidades del software y firmware utilizado en WEKALL

9. POLÍTICAS ESPECIFICAS DE SEGURIDAD DE LA INFORMACIÓN

9.1. REVISIÓN DE LAS POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN

El manual de políticas de seguridad de la información debe ser revisado y actualizado (en caso de ser necesario) al menos una vez al año o cuando haya cambios relevantes en el contexto estratégico de WEKALL, con el fin de asegurar que estén alineados con la estrategia y necesidades de la organización. Estos documentos deben ser revisados y aprobados por la Gerencia.

9.2. CONTROL DE ACCESO

9.2.1.POLÍTICA DE CONTROL DE ACCESO

El proceso de Gestión de Operaciones y Soporte controla el acceso mediante el enfoque basado en roles, aplicando los siguientes principios:

- Lo que necesita conocer: solamente se concede acceso a la información que la persona necesita para la realización de sus tareas (diferentes tareas/roles significan diferentes cosas que se necesita saber y, en consecuencia, diferentes perfiles de acceso).
- Lo que necesita usar: solamente se concede acceso a las instalaciones de procesamiento de información (aplicaciones, procedimientos) que la persona necesita para la realización de su tarea/trabajo/rol.

9.2.2.ACCESO A REDES Y A SERVICIOS EN RED

- Se controlará el acceso de los usuarios a la red y a los servicios de red, desde los escritorios virtuales.
- Los usuarios que posean acceso a los servicios de red y los sistemas de información alojados en la nube de AWS para el servicio WEKALL, deben acogerse a lineamientos para la configuración de contraseñas definidos en este documento.
- Los proveedores que requieran acceso remoto a la infraestructura tecnológica de la empresa, deben hacerlo a través de una conexión VPN o solución definida por el proceso de Operaciones y Soporte para tal fin.

9.2.3.GESTIÓN DE ACCESO DE USUARIOS

- El Proceso de Gestión de Operaciones y Soporte asigna los roles, permisos y controla el acceso de usuarios a los sistemas de información de acuerdo con la *Matriz de roles y privilegios* donde se encuentra definidos los perfiles de usuario aprobados por los líderes.

- El acceso de terceros a información corporativa debe ser autorizado exclusivamente por el propietario del activo. Esto bajo las condiciones de confidencialidad, disponibilidad, control y auditoría.

- La solicitud de asignación, modificación y suspensión del acceso a los sistemas de información de WEKALL por inicio o terminación de contrato, es responsabilidad del líder de Talento Humano.

- El Proceso de Gestión de Operaciones y Soporte revisa semestralmente el listado de usuarios con acceso a sistemas de información de WEKALL, y lo confronta con el listado de colaboradores suministrado por el área de Talento Humano, para asegurar el acceso solo al personal autorizado según su cargo/rol.

9.2.4.USO DE INFORMACIÓN DE AUTENTICACIÓN SECRETA (RESPONSABILIDAD DE USUARIOS)

- Cada usuario es responsable de salvaguardar la contraseña de ingreso al escritorio virtual y a los sistemas de información de WEKALL

- No está permitido guardar o escribir las contraseñas en papeles físicos ni documentos de texto como bloc de notas, Word o notas de Windows.

- Las cuentas de usuarios, contraseñas o cualquier otro mecanismo de autenticación a los sistemas de información, deben ser tratadas como información confidencial de WEKALL, por lo cual no se deben divulgar, publicar ni compartir con ninguna persona.

- La contraseña escogida para el acceso a cada uno de los sistemas de información de WEKALL debe:

  ✓ Ser diferente para cada aplicación o sistema de información.

- ✓ No deberá contener datos personales o de familiares tales como nombres, apellidos, fechas de cumpleaños o alguna otra fecha importante. Tampoco debe tener una secuencia previsible de letras o números como “abcd” o “1234”, o una simple palabra en cualquier idioma.

- ✓ Las contraseñas se deben establecer teniendo en cuenta los siguientes parámetros: Deben contener mayúsculas, minúsculas, números, caracteres especiales (@, $, &, por ejemplo), y mínimo una longitud de ocho (8) caracteres.

- ✓ Las contraseñas deben ser cambiadas cada 2 meses.

- ✓ La contraseña no debe ser visible en la pantalla durante el inicio de sesión.

- ✓ No está permitido facilitar o proporcionar acceso a las aplicaciones e información a usuarios o a terceros no autorizados.

- Las herramientas autorizadas para la gestión de contraseñas son:

  - ✓ Keepass

  - ✓ Excel cifrado

9.2.5.CONTROL DE ACCESO A SISTEMAS Y APLICACIONES

- Las aplicaciones críticas de WEKALL deben contar con certificado de seguridad SSL, de forma tal que su acceso se realice mediante el protocolo HTTPS.

- Las aplicaciones críticas de WEKALL deben implementar mecanismos de protección contra intentos de ingreso mediante fuerza bruta, tales como bloqueo de cuentas por un tiempo determinado después de múltiples intentos.

- Con el fin de controlar el acceso no autorizado a sistemas y aplicaciones, las contraseñas de cuentas de administración genéricas (root, SYS, SYSADMIN, cuenta de administrador de Windows, entre otras) deben ser cambiadas anualmente, cada vez que expire el tiempo de acceso concedido a un colaborador, o cuando se dé una terminación del contrato.

- El uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones, no está permitido para fines diferentes a las actividades propias del proceso de Gestión de Operaciones y Soporte.

9.3. POLÍTICA DE COPIAS DE RESPALDO

- El proceso de Gestión de Operaciones y Soporte debe configurar inicialmente las copias de respaldo a los sistemas de información para que se realice de manera automática. Adicional a esto se deben contemplar los siguientes lineamientos:

  ✓ Se realiza seguimiento a la ejecución de las copias de respaldo y se registran las fallas de las copias de respaldo programadas, con el fin de certificar su validez y correcto funcionamiento.

  ✓ Programar periódicamente pruebas de restauración.

  ✓ Las copias de respaldo se guardan únicamente con el objetivo de restaurar información cuando por situaciones como borrado de datos, incidente de seguridad de la información, defectos en los discos de almacenamiento, problemas de los servidores o por requisitos legales, sea necesario recuperarla.

  ✓ Los colaboradores son responsables de almacenar la información que requiera copias de respaldo, en las carpetas compartidas y asignadas en los escritorios virtuales, según lo determine el proceso de Gestión de Operaciones y Soporte.

9.4. POLÍTICA PARA DISPOSITIVOS MÓVILES

- Los colaboradores o proveedores que utilizan su dispositivo móvil personal para acceder a los aplicativos, correo electrónico, servicios, entre otros deberán acatar todas las políticas aquí mencionadas, en ningún caso WEKALL accederá o copiará información catalogada como Confidencial y privada del usuario que utilice en su dispositivo personal.

- El colaborador que utilice dispositivos móviles de su propiedad para el desarrollo del objeto del contrato deberá:

- ✓ Acceder al escritorio virtual de AWS, para el desarrollo de sus funciones laborales, mediante las credenciales asignadas por WEKALL.
- ✓ Bajo ningún motivo los colaboradores de WEKALL, podrán almacenar o descargar información corporativa en sus equipos de cómputo.
- ✓ El mantenimiento de los equipos de cómputo personales, será responsabilidad del colaborador.
- ✓ En caso de pérdida o robo del equipo de cómputo, WEKALL no se hará responsable de su reposición tanto física como monetaria.
- ✓ La instalación de software en el escritorio virtual, se hará bajo el control del proceso de Operaciones y Soporte.

9.5. POLÍTICADE“BYOD”(BRINGYOUROWNDEVICE)

Teniendo en cuenta que WEKALL tiene establecido como modalidad de trabajo el “Home Office”, para el acceso de los trabajadores a sus escritorios virtuales, se definirá la Política BYOD en concordancia de la gestión de los riesgos que conlleva el uso de dispositivos personales en el ámbito laboral y con el fin de proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza esta modalidad de trabajo.

A continuación, se despliegan los lineamientos de la presente política:

- El empleado deberá contar con servicio de internet de banda ancha, para poder acceder al Amazon Workspace aprovisionado.
- Los dispositivos utilizados deberán contar con las características mínimas requeridas para el buen funcionamiento de los escritorios virtuales y de acuerdo a los lineamientos establecidos por el proceso de Gestión de Operaciones y Soporte.
- Los dispositivos utilizados deberán contar como mínimo con un antivirus.
- Durante la ejecución de sus actividades, los empleados darán cumplimiento a las políticas de seguridad de la información establecidas en el presente manual.
- Se deberá limitar el uso de aplicaciones de origen desconocido o que puedan generar indisponibilidad para el acceso a los escritorios virtuales.
- El empleado deberá verificar la seguridad física existente en el sitio propuesto, para el desarrollo de las funciones teniendo en cuenta la seguridad de la edificación y del entorno local.

- WEKALL deberá documentar cláusulas contractuales para evitar disputas acerca de derechos de propiedad intelectual de los contenidos desarrollados para la empresa y a través de los equipos de propiedad de los
- El escritorio físico de trabajo deberá cumplir con la política de escritorio limpio, descrita en el presente manual.
- El desarrollo de las funciones laborales siempre deberá realizarse desde el escritorio virtual aprovisionado, y no se debe compartir el acceso a este a personal no autorizado.
- El acceso a los sistemas de información de WEKALL, se deberá realizar desde el escritorio virtual aprovisionado por la empresa.
- Se deberá reportar cualquier incidente de seguridad que ocurra o que sea detectada cuando se esté en el desarrollo de las funciones en la modalidad “Home office”.
- WEKALL prohíbe cualquier otro tipo de acceso remoto y el uso de sistemas de información que no estén autorizados por el proceso de Gestión de Operaciones y Soporte.

9.6. POLÍTICA DE EQUIPO DESATENDIDO, ESCRITORIO LIMPIO Y PANTALLA LIMPIA

- Todos los usuarios son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren de la misma, de forma tal que solo se pueda desbloquear con la contraseña de usuario o huella dactilar en las estaciones de trabajo que cuenten con este sistema. Cuando finalice la jornada laboral, se debe cerrar sesión en los escritorios virtuales.
- Los colaboradores de WEKALL deben conservar su escritorio físico libre de información catalogada como Confidencial, que pueda ser alcanzada, copiada o utilizada por terceros o personal sin autorización, cada vez que se vayan a retirar de sus puestos de trabajo.
- El escritorio lógico debe estar libre de información catalogada como Confidencial en todo momento.
- Los puestos de trabajo deben permanecer limpios y ordenado a fin de reducir el daño causado en equipos de cómputo por prácticas inadecuadas (consumo de alimentos y/o bebidas, obstrucción de ventilación, ubicación inadecuada, entre otros).

9.7. POLÍTICAS DE TRANSFERENCIA DE INFORMACIÓN

- WEKALL firma un acuerdo de confidencialidad con los colaboradores y con terceros que tengan acceso a la información y que por alguna razón requieran conocer o intercambiar información catalogada como Confidencial. En este acuerdo quedan especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se firman antes de permitir el acceso o uso de dicha información.

- El intercambio de información con organismos de control y autoridades de supervisión se rige por las directrices de los entes externos con los que se intercambia información, tales como, tokens y firmas digitales.

- Los colaboradores deben seguir las indicaciones del Procedimiento de Clasificación, Etiquetado y Manejo de la Información de WEKALL, para la transferencia de información de acuerdo con la clasificación de la misma.

- Donde se considere apropiado, la información y los datos catalogada como Confidencial siempre deben transmitirse en forma cifrada.

- Antes de la transmisión de información, siempre se deben considerar los procedimientos que se deben utilizar entre el remitente y el destinatario, y cualquier aspecto legal de la utilización de las técnicas de cifrado.

- En WEKALL no está permitido él envió de información catalogada como confidencial o de uso interno por medio de correo electrónico sin cifrado.

9.8. POLÍTICA PARA LAS RELACIONES CON PROVEEDORES

WEKALL establece mecanismos de control en su relación con proveedores, con el objetivo de asegurar la información a la que tengan acceso o servicios que sean provistos por los mismos, y que se cumpla con las políticas de la organización.

9.8.1. Tratamiento de la Seguridad Dentro de los Acuerdos con Proveedores

- WEKALL comunicará las políticas y procedimientos de seguridad de la información a los proveedores de bienes y servicios.

- Se deben incluir en los acuerdos contractuales con proveedores, como mínimo, los siguientes requisitos de seguridad de la información:

  - ✓ Acuerdo de confidencialidad.
  - ✓ Cláusula que defina las responsabilidades que continúan después de terminado el contrato (por ejemplo, confidencialidad durante 5 años después de terminado el contrato).
  - ✓ Reporte de eventos e incidentes de seguridad de la información a través de los canales definidos en el procedimiento de gestión de incidentes de seguridad de la información.
  - ✓ Manejo de la información de acuerdo con las directrices del procedimiento de Clasificación, Etiquetado y Manejo de la Información de WEKALL
  - ✓ Autorización para la revisión de los servicios prestados por los proveedores para asegurar que los términos y condiciones de seguridad de la información de los acuerdos se cumplan.

- El proceso que adquiera el contrato debe administrar los cambios en el suministro de servicios por parte de los proveedores, manteniendo los niveles de cumplimiento de servicio y seguridad de la información establecidos con ellos, y monitoreando la aparición de nuevos riesgos.

- Los accesos de los proveedores a los sistemas de información deben ser solicitados de manera formal al proceso de Gestión de Operaciones y Soporte, por parte del proceso que adquiera el contrato. En el caso de los clientes la solicitud la debe hacer el proceso de Gestión comercial. Los accesos a los sistemas de información solo deben ser brindados a los proveedores de WEKALL, en caso de ser necesario y exclusivamente para el cumplimiento de las actividades contratadas.

- Todo sistema externo utilizado por los proveedores para acceder a la información de WEKALL, debe ser autorizado por el proceso que adquiera el contrato.

9.9. POLÍTICA SOBRE EL USO DE CONTROLES CRIPTOGRÁFICOS

- El área de Operaciones y Soporte debe determinar los algoritmos criptográficos y protocolos autorizados para uso en WEKALL, y configurar los sistemas para permitir únicamente aquellos algoritmos autorizados, teniendo en cuenta la información de los grupos de interés, con el fin de descartar algoritmos de cifrado débiles.

- Se debe considerar el uso de algoritmos de cifrado simétrico, cifrado asimétrico y/o los protocolos SSL/TLS en su versión más reciente y nuevos controles criptográficos que en el futuro estén disponibles.

9.9.1. POLÍTICA DE GESTIÓN DE LLAVES CRIPTOGRÁFICAS

- El proceso de Gestión de Operaciones y Soporte deberá establecer procesos para la gestión apropiada de las llaves en todas sus etapas: generación, almacenamiento, archivo, recuperación, distribución, retiro y destrucción. De este modo se protegen contra modificación, pérdida y divulgación de información no autorizada. Las llaves criptográficas deben ser cambiadas anualmente o cada vez que se sospeche que han perdido su confidencialidad. En el caso de los certificados SSL la periodicidad puede ser de dos o tres años.

- La administración de certificados digitales está a cargo del proceso de Gestión Administrativa, así como la administración de tokens bancarios y firmas digitales, estas serán cambiadas periódicamente, de acuerdo a lo definido por el proceso o cada vez que se sospeche que han perdido su confidencialidad.

- El periodo de vigencia de las llaves criptográficas gestionadas por terceros y utilizadas por WEKALL, lo define el tercero que las gestiona.

- Los colaboradores a quienes les sean asignados tokens, deben almacenarlos bajo llave cuando no están siendo utilizando o cuando se van a retirar de sus puestos de trabajo.

9.10. POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

- La organización controla el reporte y evaluación de los eventos e incidentes de seguridad de la información, además de la respuesta y el aprendizaje obtenido de los incidentes que se presenten en WEKALL, de acuerdo con las directrices del procedimiento de “Gestión de Incidentes de Seguridad de la Información”.

- Cualquier parte interesada tanto interna como externa, puede reportar incidentes de seguridad de la información que afecten a WEKALL.

- Cada líder de proceso debe identificar los eventos y/o incidentes de seguridad de la información a través de supervisión proactiva de los sistemas de información y tecnología de WEKALL.

- Cualquier incidente de seguridad de la información se debe registrar y se debe realizar tratamiento del mismo empleando los procedimientos establecidos por WEKALL, para tal fin.

- Cualquier dispositivo de uso personal como teléfonos inteligentes, computadores portátiles, tabletas, u otros dispositivos de cómputo que estén implicados en incidentes de seguridad de la información de WEKALL, pueden ser sometidos a cadena de custodia o protección para fines de investigación o evidencia ante procesos administrativos o legales, previa coordinación del procedimiento con el propietario del equipo.

- Para prevenir la ocurrencia de incidentes de seguridad de la información, WEKALL aplicará los procedimientos de su sistema de gestión de seguridad de la información para llevar a cabo actividades de prevención de incidentes, supervisión y filtrado de anomalías que puedan afectar a la seguridad de la información.

- El comité de incidentes de seguridad de información es el responsable de la atención oportuna de los incidentes y eventos de seguridad de la información.

9.10.1. Notificación de Incidentes de Seguridad de la Información

- Toda violación de estas políticas se debe notificar inmediatamente a Operaciones y Soporte **soporte@wekall.co**, de modo que se pueda resolver debidamente el incidente. Con lo anterior se busca reducir los riesgos de seguridad de la información, protegiendo a todas las personas, así como a la Organización.

- Se deben notificar situaciones tales como: personas ajenas no autorizadas con acceso a información de la empresa, correos maliciosos, sospechas de equipos infectados, mala utilización de recursos, mal uso de información Corporativa, alteración de información, entre otros.

9.11. POLÍTICA DE GESTIÓN DE ACTIVOS DE INFORMACIÓN

9.11.1.Inventario y Propiedad de los Activos

El Oficial de Seguridad de la Información y los Líderes de proceso, anualmente identifican y documentan los activos de información, siguiendo las indicaciones del procedimiento de gestión de activos vigente.

9.11.2.Uso Aceptable de los Activos

- Todos los colaboradores WEKALL deben etiquetar la información, y darle un manejo adecuado según su clasificación, siguiendo las directrices de la metodología de identificación, clasificación y etiquetado de información establecida por la empresa.
- Los activos de información solamente pueden ser utilizados a fines de satisfacer necesidades de negocios con el objetivo de ejecutar tareas vinculadas con la organización.

a) Uso de equipos de cómputo:

- La instalación de cualquier tipo de software en los escritorios virtuales es responsabilidad del proceso de Gestión de Operaciones y Soporte.

- Se prohíbe el uso de medios extraíbles (USB, celulares, discos externos, CD, DVD, entre otros) para almacenamiento de información corporativa, con excepción de aquellos colaboradores que, por sus funciones, sean autorizados por el Líder del proceso en conjunto con el proceso de Gestión de Operaciones y Soporte, de forma temporal o permanente.

- Toda actividad informática (escaneos de seguridad, ataques de autenticación o de denegación de servicio, etc.) no autorizada que afecte los sistemas de información de WEKALL, está prohibida y dará lugar a los procesos disciplinarios y/o legales correspondientes.

- Las claves de acceso a los sistemas de información de WEKALL son personales e intransferibles, cada colaborador debe responder por las actividades que se lleven a cabo con sus datos de identificación.

- Cualquier actividad realizada por un colaborador en los sistemas de información de WEKALL, debe ser monitoreada por el proceso de Gestión de Operaciones y Soporte. En el caso que se identifiquen riesgos de seguridad sobre la información, inmediatamente será revocada sus claves de acceso y el sistema será bloqueado.

- La seguridad física e integridad de los equipos de cómputo serán responsabilidad única y exclusiva de sus propietarios. WEKALL no será responsable por estos equipos en ningún caso.

b) Uso de la Intranet y de Internet

- El proceso de Gestión de Operaciones y Soporte, debe utilizar filtros de software y otras técnicas para restringir el acceso a información inapropiada desde los escritorios virtuales.

- El proceso de Gestión de Operaciones y Soporte es responsable del control de acceso de los usuarios a Internet desde los escritorios virtuales, así como el Oficial de Seguridad, de garantizar que los usuarios conozcan las amenazas y reciban la capacitación relacionada para reducir el riesgo de incidentes en seguridad de la información.

- El usuario debe considerar como no confiable la información recibida a través de sitios web no seguros. Ese tipo de información puede ser utilizada con fines comerciales solamente después de haber verificado su autenticidad y veracidad.

- Se prohíbe el envío, descarga o visualización de información con contenido que atente contra la integridad moral personal o corporativa desde los escritorios virtuales.

- Está prohibido, ejecutar cualquier herramienta para realizar el monitoreo de puertos o análisis de tráfico de red, a menos que sean autorizadas por el proceso de Operaciones y soporte.

- Los usuarios no deben intentar burlar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas de la organización y de la ley y serán sancionadas de acuerdo con la legislación aplicable.

- Todas las actividades realizadas en los sistemas de información de WEKALL, pueden ser monitoreadas con el fin de preservar la seguridad informática de la organización.

c) Uso del correo electrónico

- La organización provee a todos los colaboradores un correo electrónico corporativo con el dominio **wekall.co** para el ejercicio de sus labores, y el cual se debe acceder únicamente desde el escritorio virtual provisionado.

- La cuenta de correo electrónico corporativa es personal e intransferible, por ende, los usuarios son completamente responsables de todas las actividades realizadas con sus credenciales de acceso y el buzón asociado al correo de la organización.

- El correo electrónico corporativo se debe utilizar estrictamente como herramienta de comunicación de WEKALL, es decir, que debe ser usado para transmitir información relacionada única y exclusivamente con el desarrollo de las funciones misionales y de apoyo asignadas.

- Teniendo en cuenta que el correo electrónico corporativo es una herramienta para el intercambio de información necesaria que permita el cumplimiento de las funciones propias de cada cargo y no una herramienta de difusión masiva de información, no debe ser utilizada como servicio personal de mensajes o cadenas a familiares o amigos, esquemas piramidales, terrorismo, pornografía, programas piratas, proselitismo político, religioso o racial, amenazas, estafas, virus o código malicioso.

- Cada usuario del correo electrónico tiene derecho a la asignación de un espacio limitado de almacenamiento en el servidor. Por tal motivo, es responsabilidad de cada uno borrar o descargar oportunamente los correos con el fin de liberar espacio en el servidor y evitar el bloqueo del buzón.

- El correo entrante debe tratarse con extremo cuidado, debido a los riesgos de seguridad de la información inherentes. Por lo tanto, se prohíbe abrir un correo electrónico con archivos adjuntos sin que a estos se les haya realizado escaneo, para detectar la posible existencia de virus o código malicioso, en su defecto deben ser borrados antes de intentar abrirlos y reportar el posible incidente.

- El correo no solicitado o proveniente de un origen desconocido debe ser tratado con precaución y por ninguna razón debe ser respondido. Adicionalmente, se debe informar al proceso de Operaciones y Soporte, y reportarlo como un incidente de seguridad de la información.

- El servidor de correo debe estar configurado para bloquear archivos adjuntos o información nociva como archivos .exe o de ejecución de comandos.

9.11.3.Devolución de Activos

La devolución de activos por terminación o cambio de empleo, se controla por medio del *formato de paz y salvo* responsabilidad de recursos humanos.

9.11.4. Clasificación de la Información

En atención a los requisitos de la norma ISO/IEC 27001:2013, WEKALL clasifica, etiqueta y maneja la información y sus activos asociados de acuerdo con el procedimiento de Clasificación, Etiquetado y Manejo de la Información, definido en el documento *Metodología de Activos de Información*.

9.12. POLÍTICA DE GESTIÓN DE VULNERABILIDADES

Es responsabilidad del personal de Infraestructura de prevenir ataques de Ciberseguridad y Seguridad de la Información tales como:

- Malware
- Suplantación de identidad (Phishing)
- Ataques de hombre en el medio (MitM)
- Ataque de contraseña
- Ataques DNS
- Ataques DoS (Denegación del servicio)
- Inyección de SQL (SQLinjection)
- ataque de XSS (Cross Site Scripting)
- IDOR (Insecure Direct Obect Reference)

Todos los colaboradores deben informar de forma inmediata al proceso de Operaciones y Soporte, la existencia de una posible vulnerabilidad o debilidad identificada en la empresa, que pueda afectar sus los activos de información.

La identificación de vulnerabilidades a los sistemas de información por parte de un colaborador, contratista, proveedor, cliente, y demás partes interesadas (internas y externas), debe ser reportada al correo **soporte@wekall.co.**

WEKALL realizará un análisis de vulnerabilidades a sus sistemas de información como mínimo 1 vez al año; esta actividad estará a cargo de un tercero contratado para esta actividad.

Una vez se haya identificado una vulnerabilidad o debilidad dentro de la compañía, se debe ejecutar la remediación de estas lo más pronto posible, con el fin de evitar que sea explotada por una amenaza.

10. CONTROL DE CAMBIOS

Versión	Autor	Fecha	Descripción de la modificación
01	Angie Melissa Correa	12 de mayo de 2021	Versión inicial del documento
02	Angie Melissa Correa	27 de mayo del 2022	• Inclusión de políticas para la gestión de vulnerabilidades • Eliminación de partes interesadas y esquema de comunicación. • Ajuste de forma.

11. APROBACIÓN

Elaboró: Angie Melissa Correa	**Revisó:** Diana María Escobar Correa	**Aprobó:** 
Cargo: Oficial de Seguridad de la Información	**Cargo:** Operations Director	**Cargo:** CEO