POLÍTICAS INTERNAS DE SEGURIDAD

TABLA DE CONTENIDO

1. OBJETIVO....4
1.1. Alcance y objetivos específicos....4
2. BASE LEGAL Y ÁMBITO DE APLICACIÓN....5
3. DEFINICIONES....5
4. CLASIFICACIÓN DE LA INFORMACIÓN....8
5. CUMPLIMIENTO Y ACTUALIZACIÓN....9
6. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN....9
6.1. Política organizacional de la seguridad de la información....9
6.2. Políticas de gestión de activos....10
6.3. Responsable de administrar las bases de datos....11
6.4. Políticas de seguridad del recurso humano....11
6.5. Políticas de control de acceso....12
6.5.1. Identificación y autenticación....12
6.5.2. Política de cifrado....13
6.5.3. Ejecución del tratamiento fuera de las instalaciones....14
6.5.4. Bases de datos temporales....14
6.6. Medidas de seguridad física y del medio ambiente....14
6.6.1. Áreas seguras....14
6.6.2. Seguridad de los equipos....14
6.6.3. Archivo de documentos....15
6.7. Políticas de seguridad de las operaciones....16
6.7.1. Procedimientos operacionales y responsabilidades....16
6.7.2. Gestión de la entrega de servicios de terceros....17
6.7.3. Protección contra códigos maliciosos....17
6.7.4. Entrada y salida de documentos o soportes....18
6.7.5. Control de acceso físico....18
6.8. Copias de respaldo y recuperación de datos....19
6.9. Política de seguridad en las redes de comunicaciones....20
6.9.1. Gestión de seguridad en las redes....20

6.9.2. Transferencia de información....20
6.9.3. Navegación en internet....21
6.9.4. Política de uso de mensajería instantánea y redes sociales....21
6.9.5. Política de uso de correo electrónico....21
6.10. Supervisión de eventos de seguridad....22
6.11. Políticas de adquisición, desarrollo y mantenimiento de los sistemas....23
6.12. Pruebas no funcionales....23
7. FUNCIONES Y OBLIGACIONES DEL PERSONAL....23
8. BASES DE DATOS Y SISTEMAS DE INFORMACIÓN....26
9. PROCEDIMIENTO DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE INCIDENCIAS....27
10. MEDIDAS PARA EL TRANSPORTE, DESTRUCCIÓN Y REUTILIZACIÓN DE DOCUMENTOS Y SOPORTES 28
11. POLÍTICAS DE CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN....28
12. POLÍTICAS DE AUDITORÍAS....29
13. MEDIDAS DE SEGURIDAD....29
14. DISPOSICIÓN FINAL....32
15. APÉNDICE....32
16. ELABORACIÓN Y APROBACIÓN DEL DOCUMENTO....33
17. HISTÓRICO DE DOCUMENTOS....33

1. OBJETIVO

Establecer las directrices a aplicar para el manejo de la información, así como dar a conocer cuáles son los requisitos básicos de seguridad de la información a través de los principios de confidencialidad, integridad y disponibilidad, para establecer controles efectivos sobre todas las actividades que se desarrollan en ALERGOLOGOS DE OCCIDENTE S.A.S., con el fin de que todos los involucrados en la operación o que prestan servicios garanticen el buen uso de los sistemas, herramientas, recursos y datos a los que tienen acceso.

Así como, presentar los lineamientos de control que aplican a todos los usuarios que tengan acceso de manera interna o externa a la información creada, procesada o utilizada por ALERGOLOGOS DE OCCIDENTE S.A.S., estableciendo las políticas de seguridad que se aplican a todos los sistemas de información, las redes, e instalaciones en las que procesan, almacenan o transmiten información, independiente del medio o formatos utilizados.

1.1. Alcance y objetivos específicos

Para la implementación de la presente política se tendrán en cuenta buenas prácticas y disposiciones legales, tales como: estándares internacionales de seguridad (ISO 27001:2013), la Ley 1581 de 2012 y normas complementarias, así como, las directrices establecidas por la Superintendencia de Industria y Comercio mediante la Guía de para la Implementación del Principio de Responsabilidad Demostrada (Accountability), otras Guías y actos administrativos.

Aunado a lo anterior, se tendrá en cuenta que la organización se enfrenta a amenazas relativas a la seguridad, en especial relacionados con el fraude asistido por computadores y las acciones de personas, los cuales cada vez son más comunes, ambiciosos y sofisticados. A continuación, se describen los principales objetivos específicos:

- Establecer y capacitar al personal de ALERGOLOGOS DE OCCIDENTE S.A.S. en seguridad de la información, buscando una mejor cultura en este aspecto, así como en el compromiso con la adopción de buenas prácticas, el reporte de incidentes de seguridad y la identificación de riesgos.
- Minimizar y mitigar el efecto de los incidentes de seguridad de información en ALERGOLOGOS DE OCCIDENTE S.A.S..
- Mantener los sistemas y los recursos tecnológicos adecuados, que fortalezcan la seguridad de la información.
- Establecer los fundamentos para el desarrollo y la implantación de un Sistema de Gestión de Seguridad de Información.
- Definir la conducta a seguir en lo relacionado con el acceso, uso, manejo y administración de los recursos de información.

- Establecer y comunicar la responsabilidad en el uso de los activos de información, que soportan los procesos y sistemas de la organización.

2. BASE LEGAL Y ÁMBITO DE APLICACIÓN

ALERGOLOGOS DE OCCIDENTE S.A.S., con el objeto de garantizar el adecuado cumplimiento de la Ley Estatutaria 1581 de 2012 de Protección de Datos (LEPD) y normas concordantes, adopta estas Políticas Internas de Seguridad donde se recogen las medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a los registros con el fin de mitigar los riesgos relacionados con la adulteración, pérdida, consulta o uso y acceso no autorizado o fraudulento de la información, de acuerdo con los principios de seguridad y confidencialidad recogidos en el artículo 4 literales g) y h) de la LEPD.

Las disposiciones de este documento se aplican a las bases de datos objeto de responsabilidad de ALERGOLOGOS DE OCCIDENTE S.A.S., así como a los sistemas de información, mecanismos de almacenamiento y equipos empleados en el tratamiento de los datos, que deban ser protegidos de acuerdo con la normativa vigente, sin importar el medio, formato o presentación. De igual forma aplican para todas las personas que participan en el tratamiento, tales como: usuarios (empleados, accionistas, clientes, entre otros), socios, proveedores y entes de control que accedan independiente de su ubicación (interna o externa), a cualquier activo de información de la organización.

El cumplimiento de las políticas de la seguridad de la información es obligatorio y todos los usuarios de la información deben entender su rol, y asumir su responsabilidad respecto a los riesgos de seguridad de la información y la protección de esta.

Por consiguiente, cualquier situación en la que se comprometa la integridad, confidencialidad y disponibilidad de la información resultará en una acción disciplinaria, que pueden llegar hasta la terminación del contrato laboral por justa causa y/o un posible establecimiento de un proceso judicial bajo las leyes nacionales que apliquen, sin perjuicio de acciones civiles y/o penales a que haya lugar.

3. DEFINICIONES

Acceso autorizado: Autorización concedida a un usuario para el uso de determinados recursos. En dispositivos automatizados es el resultado de una autentificación correcta, generalmente mediante el ingreso de usuario y contraseña.

Activo de información: Es toda aquella información que, sin importar su presentación, medio o formato, en el que sea creada, utilizada o almacenada, tiene valor e importancia dentro de la organización y sirve de soporte a las actividades de negocio y la toma de decisiones.

Autenticación: Procedimiento de acreditación por medios electrónicos de la identidad de una persona o ente, del contenido y voluntad expresa en sus operaciones, transacciones y documentos, y de la integridad y autoría de aquellos.

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el tratamiento de datos personales.

Aviso de privacidad: Comunicación verbal o escrita generada por el responsable, dirigida al Titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.

Base de Datos: Conjunto organizado de datos personales que sea objeto de tratamiento.

Confidencialidad: Hace referencia a la protección de información cuya divulgación no está autorizada.

Contraseña: Seña secreta que permite el acceso a dispositivos, información o bases de datos antes inaccesibles. Se utiliza en la autentificación de usuarios que permite el acceso autorizado.

Control de acceso: Mecanismo que permite acceder a sitios, dispositivos, información o bases de datos mediante la autentificación.

Copia de respaldo: Copia de los datos de una base de datos en un soporte que permita su recuperación.

Dato Personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

Disponibilidad: La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso.

Encargado del tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento.

Identificación: Proceso de reconocimiento de la identidad de los usuarios.

Incidencia: Cualquier anomalía que afecte o pueda afectar a la seguridad de los datos, constituyendo un riesgo para la confidencialidad, disponibilidad o integridad de las bases de datos o de los datos personales que contienen.

Información: Toda forma de comunicación o representación de conocimiento mediante datos digitales, escritos en cualquier medio, ya sea magnético, papel, visual u otro que genere ALERGOLOGOS DE OCCIDENTE S.A.S..

Integridad: La información debe ser precisa, coherente y completa desde su creación hasta su destrucción.

Perfil de usuario: Grupo de usuarios a los que se da acceso.

Recurso protegido: Cualquier componente del sistema de información, como bases de datos, programas, soportes o equipos, empleados para el almacenamiento y tratamiento de datos personales.

Responsable de administrar base de datos: Una o varias personas designadas por ALERGOLOGOS DE OCCIDENTE S.A.S., para el control y la coordinación de las medidas de seguridad de las bases de datos que gestiona.

Oficial de protección de Datos: Es la persona natural que asume la función de coordinar la implementación del marco legal en protección de datos personales, que dará trámite a las solicitudes de los Titulares, para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012.

Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos, que para los efectos de las políticas planteadas corresponde ALERGOLOGOS DE OCCIDENTE S.A.S..

Sistema de información: Conjunto de elementos (bases de datos, programas, soportes y/o equipos de cómputo, personas) empleados para el tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo.

Soporte: Mecanismos de almacenamiento o material en cuya superficie se registra información o sobre el cual se pueden guardar o recuperar datos, como el papel, la cinta de video, el CD, el DVD, el disco duro, las memorias USB, etc.

Usuario: Sujeto autorizado para acceder a los datos o recursos, o proceso que accede a los datos o recursos sin identificación de un sujeto.

Titular: Persona natural cuyos datos personales sean objeto de Tratamiento.

Transferencia: La transferencia de datos tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país.
Transmisión: Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento por el encargado por cuenta del responsable.

Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

4. CLASIFICACIÓN DE LA INFORMACIÓN

Pública: Información que puede ser conocida por todos los miembros enmarcados en el alcance y el público en general. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

Interna: Información que requiere la organización para la ejecución de su objeto social y puede ser accedida solamente por los colaboradores de ALERGOLOGOS DE OCCIDENTE S.A.S. para el cumplimiento de las actividades diarias, alineadas a las funciones y responsabilidades del cargo o de la prestación de servicios de terceros y su conocimiento es de carácter general. Su disponibilidad a terceros es únicamente mediante un acuerdo contractual que exprese la necesidad de su uso para efectos del cumplimiento de este y lo cual no debe ser divulgada.

Confidencial: Información de uso exclusivo de un grupo de colaboradores de ALERGOLOGOS DE OCCIDENTE S.A.S. en función de sus labores y que no puede ser conocida por otros empleados o terceros sin autorización del Responsable de administrar la base de datos. También se refiere a un dato personal que por su naturaleza íntima o reservada solo interesa a su titular y para su tratamiento requiere de su autorización previa, informada y expresa. Bases de datos que contengan datos como Números telefónicos y correos electrónicos personales; datos laborales, sobre infracciones administrativas o penales, administrados por administraciones tributarias, entidades financieras y entidades gestoras y servicios comunes de la Seguridad Social, bases de datos sobre solvencia patrimonial o de crédito, bases de datos con información suficiente para evaluar la personalidad del titular, bases de datos de los responsables de operadores que presten servicios de comunicación electrónica.

Reservada: Información que solo debe tener acceso personal específico, pues la revelación al público puede causar daño a la reputación, marca o estrategias de organización. También, hace referencia a aquellos datos

personales cuyo conocimiento o divulgación puede interesar no solo a su titular sino a cierto sector personas o a la sociedad en general, como son el dato financiero o crediticio de actividad comercial. De igual forma son datos privados que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

5. CUMPLIMIENTO Y ACTUALIZACIÓN

ALERGOLOGOS DE OCCIDENTE S.A.S., realizará permanente revisión y actualización de la presente política siempre y que se produzcan cambios en: los sistemas de información, el sistema de tratamiento, la organización o el contenido de la información de las bases de datos, que puedan afectar a las medidas de seguridad implementadas. Asimismo, deberá adaptarse en todo momento a la normativa legal en materia de seguridad de datos personales.

6. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

ALERGOLOGOS DE OCCIDENTE S.A.S., implementará las siguientes instrucciones las cuales brindan orientación sobre las actividades y herramientas que se deben implementar para la seguridad de la información, de acuerdo con los requisitos de la organización y las leyes y reglamentos pertinentes.

6.1. Política organizacional de la seguridad de la información

El Comité de Seguridad de la Información, será responsable de la planeación, implantación y mantenimiento de las Políticas de Seguridad de la información. Así como, de difundir las políticas entre los usuarios.

El Responsable de la Seguridad de la Información, estará a cargo de la implantación, mejoras, mantenimiento, verificación y cumplimiento de la Política de Seguridad de la Información. Adicional tienen las siguientes funciones:

- Coordinar y controlar la implementación de las medidas de seguridad, y colaborar con la difusión del Manual de Políticas de Seguridad de la Información.
- Coordinar y controlar los mecanismos que permiten acceder a la información contenida en las bases de datos.
- Gestionar los permisos de acceso a los datos por parte de los usuarios autorizados identificados.
- Habilitar el registro de incidencias a todos los usuarios, para que comuniquen las incidencias relacionadas con la seguridad de los datos; así como acordar con el Oficial de Protección de Datos las medidas correctivas.
- Comprobar, al menos cada seis meses, la validez y vigencia de la lista de usuarios autorizados, la existencia y validez de las copias de seguridad para la recuperación de los datos, como también con el cumplimiento de

las medidas relacionadas con las entradas y salidas de datos.

- Recibir y analizar el informe de auditoría para elevar sus conclusiones y proponer medidas correctivas al responsable del tratamiento.

El Responsable de administrar las bases de datos será el encargado de controlar y coordinar la adecuada aplicación de las políticas del tratamiento de los datos una vez almacenados en una base datos específica; y poner en práctica las directrices que dicte ALERGOLOGOS DE OCCIDENTE S.A.S., el Comité o Responsable de Seguridad de la Información y el Oficial de Protección de datos.

El Oficial de Protección de Datos será el Encargado de velar por la implementación efectiva de las políticas y procedimientos relacionados con la gestión de datos personales dentro de ALERGOLOGOS DE OCCIDENTE S.A.S..

6.2. Políticas de gestión de activos

ALERGOLOGOS DE OCCIDENTE S.A.S. mantendrá un inventario de los activos de información asociados a los procesos de la organización. Cada activo estará claramente identificado, así como su responsable y propietario de la información, como también su clasificación (en cuanto a seguridad) deben ser acordados y documentados. Los documentos y soportes en los que se encuentran las bases de datos deben ser debidamente archivados y tratados, acorde a los tiempos establecidos como se determine en el formato FR-01 Tablas de retención documental.

Los responsables y propietarios de la información deben garantizar que todos los activos de información reciban un apropiado nivel de protección basados en su valor, sensibilidad, riesgo de pérdida o compromiso, y/o requerimientos legales de retención. Así como, de vigilar y controlar que personas son las autorizadas a acceder a los documentos y soportes con datos personales son los responsables de administrar las bases de datos, los cuales están referidos en el " Anexo 1 PL-01 Organización Bases de Datos" sobre bases de datos y sistemas de información del presente manual.

Los documentos y soportes deben catalogar los datos según la clasificación (Publica, Interna, Confidencial o Reservada) de la información que contienen, ser inventariados y ser accesibles solo por el personal autorizado, salvo que las características de estos hagan imposible la identificación referida, en cuyo caso se dejará constancia motivada en el formato FR-09 Entrada y de salida de documentos.

Los líderes de los procesos son responsables de reportar los nuevos activos de información y garantizar que los activos más relevantes de su proceso sean identificados y valorados.

La identificación de los documentos y soportes que contengan datos personales sensibles debe realizarse utilizando sistemas de etiquetado comprensibles y con significado que permita a los usuarios autorizados identificar su contenido y que dificulten la identificación para el resto de las personas.
Los colaboradores deberán cumplir con los lineamientos establecidos en el ciclo del dato, con el fin de establecer la disposición de los medios (Memorias USB, discos magnéticos, CD/DVD, etc.) cuando ya no sean requeridos, así como de la eliminación segura de la información contenida en ellos.

La salida de documentos y soportes que contengan datos personales fuera de las instalaciones o equipos de la organización deben estar bajo control y se autoriza por el Responsable de administrar la base de datos. Este precepto también es aplicable a los documentos o soportes anexados y enviados por correo electrónico.

Todos los colaboradores (Internos y externos) deberán devolver los activos de información asignados a su cargo una vez finalice la relación contractual.

El inventario de documentos y soportes de ALERGOLOGOS DE OCCIDENTE S.A.S., debe incluirse como anexo del presente manual.

6.3. Responsable de administrar las bases de datos

ALERGOLOGOS DE OCCIDENTE S.A.S., ha designado a los responsables de seguridad de la información en las bases de datos física y automatizados encargados de implementar y controlar las medidas de seguridad de la información contenidas en el presente manual. La designación de los responsables de seguridad de la información no exonera de responsabilidad al Responsable del tratamiento o Encargado del tratamiento.

6.4. Políticas de seguridad del recurso humano

ALERGOLOGOS DE OCCIDENTE S.A.S. debe proveer los mecanismos necesarios para asegurar que sus colaboradores cumplan con sus responsabilidades en seguridad de la información desde su ingreso hasta su retiro, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información y de las instalaciones.

Por lo anterior, los contratos de los colaboradores y contratistas deben tener cláusulas que indiquen las responsabilidades correspondientes para con la seguridad de la información. Así como, en el tratamiento de datos personales que no tengan naturaleza de públicos, debido a que están obligados a garantizar la reserva de la información.

Los colaboradores deben recibir una copia del presente documento para su conocimiento y certificación de su comprensión y entendimiento. En los casos cuando el colaborador o tercero cambie de rol o cargo se deberán retirar los permisos que este tenga y realizar la nueva asignación de perfil para las nuevas labores. Cuando un

colaborador trate documentos o soportes que contiene datos personales tiene el deber de custodiarlos, así como de vigilar y controlar que personas no autorizadas no puedan tener acceso a ellos.

Al finalizar la contratación, el jefe del colaborador o responsable del tercero debe coordinar y asegurar que los accesos físicos y lógicos sean eliminados y la información pertinente sea entregada.

6.5. Políticas de control de acceso

6.5.1. Identificación y autenticación

El personal de ALERGOLOGOS DE OCCIDENTE S.A.S. solamente debe acceder a aquellos datos y recursos necesarios para el desarrollo de sus funciones y sobre los cuales se encuentren autorizados por el Responsable de administrar la base de datos.

ALERGOLOGOS DE OCCIDENTE S.A.S. se ocupa del almacenamiento actualizado de usuarios, de los perfiles de usuarios, y de los accesos autorizados para cada uno de ellos. Además, tiene mecanismos para evitar el acceso a datos con derechos distintos de los autorizados. En el caso de dispositivos informáticos los permisos de acceso consisten en la asignación de usuario y contraseñas, y en el caso de documentos, en la entrega de llaves o mecanismos de apertura de dispositivos de almacenamiento donde se archive la documentación.

Para la autorización de acceso a los sistemas de información en producción y a las redes de ALERGOLOGOS DE OCCIDENTE S.A.S. el área de recursos humanos o jefe directo deberá solicitar su creación, actualización o retiro de los permisos autorizados a los usuarios al área de sistemas. En consecuencia, al finalizar la contratación todas las credenciales de acceso a los sistemas de información de la organización deberán ser retiradas y/o deshabilitadas.

El área de sistemas deberá realizar, al menos dos veces al año, una conciliación de usuarios con el fin de eliminar o bloquear los que ya no tienen relación contractual con la organización, así como también las cuentas redundantes o innecesarias.

El acceso a los sistemas de información se debe llevar a cabo mediante usuarios únicos, identificados y con contraseña. Por consiguiente, no está permitido el uso de un mismo código de acceso por varios usuarios, los usuarios son responsables de todas las actividades realizadas con su código de acceso, los usuarios no deben divulgar ni permitir que otros utilicen sus credenciales, al igual se prohíbe utilizar las credenciales de acceso de otros usuarios. Adicional, cuando el usuario ingrese por primera vez con la contraseña asignada deberá cambiarla y para garantizar la integridad y confidencialidad de estas últimas, estas deben tener un mínimo de ocho caracteres, debe ser alfanumérica contener mayúsculas, minúsculas, números y sin espacios en blanco. Adicional, se debe garantizar el almacenamiento automatizado, interno y cifrado, de las contraseñas, así como

vigilar que estás se cambien de forma periódica (por ejemplo: 30, 60, 90 o 180 días), así como, adoptar un mecanismo para limitar los intentos reiterados de accesos no autorizados y bloquear el acceso tras tres intentos.

Se debe garantizar que los usuarios realicen el inicio de sesión seguro (doble factor, OTP, tarjeta inteligente, biométrico, etc.) en todos los sistemas de información de la compañía.

ALERGOLOGOS DE OCCIDENTE S.A.S., también garantiza el almacenamiento automatizado, interno y cifrado, de las contraseñas, así pues, adoptará un mecanismo para limitar los intentos reiterados de accesos no autorizados y bloquear el acceso tras tres intentos.

La modificación sobre algún dato o información, así como la concesión, alteración, inclusión o anulación de los accesos autorizados y de los usuarios, corresponde de manera exclusiva al personal autorizado.

Cualquier personal ajeno a ALERGOLOGOS DE OCCIDENTE S.A.S., que, de forma autorizada y legal, tenga acceso a los recursos protegidos estará sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

Las estaciones de trabajo deben ser bloqueadas mediante las políticas implementadas por medio del directorio activo, mientras se encuentran desatendidas, así como se debe garantizar el cumplimiento de escritorio y pantalla limpios.

El acceso a los documentos debe realizarse exclusivamente por el personal autorizado, siguiendo los mecanismos y procedimientos definidos. Estos últimos deben identificar y conservar los accesos realizados a la documentación clasificada como Confidencial o Reservada, tanto por usuarios autorizados como por personas no autorizadas de manera permanente, tal y como se refleja en el numeral referido anteriormente.

El procedimiento de acceso a los documentos que contienen datos clasificados como Confidencial o Reservados implica el registro de accesos a la documentación, la identidad de quien accede, el momento en que se produce el acceso y los documentos a los que se han accedido. El acceso a documentos con este tipo de datos se realiza por personal autorizado; si se realiza por personas no autorizadas deberá supervisarse por algún usuario autorizado o por el Responsable de administrar la base de datos.

6.5.2. Política de cifrado

Cuando se realicen conexiones remotas se implementará canales de comunicación segura a través de los servicios que el proveedor contratado por la compañía ofrezca (por ejemplo: VPN, RTC, RDSI, ADSL, etc.) y definirá los parámetros de seguridad para su configuración.

ALERGOLOGOS DE OCCIDENTE S.A.S. tendrá implementado en todos los equipos portátiles y dispositivos removibles que se utilicen fuera de las instalaciones mecanismos de cifrado o en su defecto los usuarios deberán proteger el documento mediante contraseña.

Cuando se requiera el intercambio de información Confidencial o Reservada de ALERGOLOGOS DE OCCIDENTE S.A.S. con clientes o terceros, está deberá enviarse cifrada.

6.5.3. Ejecución del tratamiento fuera de las instalaciones

El almacenamiento de datos personales en dispositivos portátiles y su tratamiento fuera de la organización requiere una autorización previa por parte de ALERGOLOGOS DE OCCIDENTE S.A.S., y el cumplimiento de las garantías de seguridad correspondientes al tratamiento de este tipo de datos.

6.5.4. Bases de datos temporales

Las bases de datos temporales o copias de documentos creadas para trabajos temporales o auxiliares deben cumplir con el mismo nivel de seguridad que corresponde a las bases de datos o documentos originales. Una vez que dejan de ser necesarias, estas bases de datos temporales o copias deben ser borradas o destruidas, impidiéndose así el acceso o recuperación de la información que contienen.

6.6. Medidas de seguridad física y del medio ambiente

6.6.1. Áreas seguras

Las áreas físicas utilizadas para soportar toda la operación de la organización deberán estar provistas de los controles adecuados (por ejemplo: Puertas, cerraduras, lectores de tarjetas, biométricos, entre otros.) según el tipo información que manejen.

La infraestructura tecnológica sin importar su ubicación debe estar físicamente protegida contra amenazas de acceso no autorizado y amenazas ambientales para prevenir exposición, daño o pérdida de la información e interrupción de las actividades.

Los centros de cómputo y de cableado deben contar con mecanismos que permitan garantizar que se cumplen los requerimientos ambientales (temperatura, humedad, etc.) especificados por los fabricantes de los equipos.

6.6.2. Seguridad de los equipos

Los equipos de cómputo (Dispositivos móviles) deberán contar con guaya de seguridad cuando se encuentren en el lugar de trabajo asignado, así como, deberán contar con autorización previa cuando van a salir de las

instalaciones. Todos los equipos de cómputo deben ser conectados a una red eléctrica regulada. El área de sistemas o tecnología debe realizar al menos una vez al año un mantenimiento preventivo a todos los equipos de cómputo.

Cuando un equipo de cómputo (Dispositivos móviles) va a ser reutilizado deberá haberse surtido un proceso de eliminación segura de la información confidencial y software con licencia que no se requiera. Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.

Los recursos informáticos de ALERGOLOGOS DE OCCIDENTE S.A.S. son exclusivamente para propósitos laborales y deben ser tratados como activos dedicados a proveer las herramientas para realizar el trabajo requerido.

Todo el software usado en ALERGOLOGOS DE OCCIDENTE S.A.S. debe tener su respectiva licencia y acorde con los derechos de autor.

Los recursos tecnológicos y el software asignados a los usuarios son responsabilidad de cada uno. Cuando un colaborador se encuentra en periodo de vacaciones o tiene una incapacidad no podrá retirar de las instalaciones el equipo portátil que tenga asignado a su cargo, salvo previa autorización del jefe inmediato. Cuando se utilice la impresora debe recogerse inmediatamente las copias, evitando dejar éstas en las bandejas de salida.

6.6.3. Archivo de documentos

ALERGOLOGOS DE OCCIDENTE S.A.S., fija los criterios y procedimientos de actuación que se deben utilizar para el archivo de documentos que contengan datos personales conforme a la Ley. Los criterios de archivo garantizan la conservación, localización y consulta de los documentos y hacen posible los derechos de consulta y reclamo de los Titulares. Estos criterios y procedimientos se recogen en el “Anexo 1 PL-01. Organización Bases de Datos”.

Los documentos deben ser archivados considerando, entre otros, criterios como el grado de utilización de los usuarios con acceso autorizado a los mismos, la actualidad de su gestión y/o tratamiento y la diferenciación entre bases de datos históricas y de administración o gestión de la empresa.

Los sitios de almacenamiento de documentos deben disponer de llaves u otros mecanismos que controlen su apertura, excepto cuando las características físicas de éstos lo impidan, en cuyo ALERGOLOGOS DE OCCIDENTE S.A.S. adoptará medidas alternas para impedir el acceso de personas no autorizadas.

Cuando los documentos que contienen datos personales se encuentren en proceso de revisión o tramitación y, por tanto, fuera de los dispositivos de almacenamiento, ya sea antes o después de su archivo, la persona que se encuentre a cargo de estos debe custodiarlos e impedir en todo caso que personas no autorizadas puedan acceder a ellos. La destrucción de documentos se debe hacer mediante mecanismos que realicen un corte adecuado del papel, que garantice que el documento no se pueda restaurar.

Los dispositivos de almacenamiento que contengan documentos con datos personales clasificados como Confidencial o Reservada deben encontrarse en áreas o lugares en las que el acceso esté protegido con puertas de acceso con sistemas de apertura de llave u otros mecanismos similares. Estas áreas deben permanecer cerradas cuando no sea necesario el uso de dichos documentos. Si no fuera posible cumplir con lo anterior, ALERGOLOGOS DE OCCIDENTE S.A.S., podrá adoptar medidas alternativas debidamente motivadas.

Las descripciones de las medidas de seguridad de almacenamiento se encuentran recogidas en el “Anexo 1 PL-01. Organización Bases de Datos”.

Las medidas de seguridad deben ser apropiadas considerando varios factores como entre otros, los siguientes: los niveles de riesgos del tratamiento; la naturaleza o sensibilidad de los datos; la magnitud del daño que se puede causar a los titulares y al responsable; la cantidad de información; el tamaño de la organización; los recursos disponibles y el monitoreo y seguimiento a la confiabilidad los servicios de computación en la nube (CEN); el origen de los datos personales, las operaciones de tratamiento que se ejecutarán, y las categorías de datos que serán objeto del tratamiento. Todas estas, deben ser objeto de revisión, evaluación y mejoras permanentes.

6.7. Políticas de seguridad de las operaciones

6.7.1. Procedimientos operacionales y responsabilidades

Al finalizar la jornada laboral o durante ausencias temporales de los usuarios, estos deben asegurarse de que los escritorios o mesas de trabajo queden despejados. Por lo tanto, todos los documentos deben ser guardados en archivadores, cajones o compartimentos bajo llave.

Con el fin de evitar cambios no autorizados cuando se requiera la implementación o actualización de nuevos sistemas de información se deberá tener separados los ambientes de producción, pruebas, desarrollo y de contingencia.

Los colaboradores no deben, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros usuarios, o dañar o alterar los recursos informáticos.

6.7.2. Gestión de la entrega de servicios de terceros

Todos los terceros que presten servicios a ALERGOLOGOS DE OCCIDENTE S.A.S. deberán acogerse a las políticas de seguridad de la información establecidas.

Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada tercero que tenga acceso, procese, almacene, comunique o suministre componentes de los sistemas de información.

Los acuerdos con terceros deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.

En el caso de que, por motivos directamente relacionados con el puesto de trabajo, el tercero entre en posesión de información confidencial o reservada contenida en cualquier tipo de soporte, deberá entenderse que dicha posesión es estrictamente temporal, con obligación de secreto y sin que ello le confiera derecho alguno de posesión, titularidad o copia sobre dicha información. Por consiguiente, cuando exista la necesidad de otorgar acceso a terceras partes a la información de ALERGOLOGOS DE OCCIDENTE S.A.S., se establecerán los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, restringiendo al mínimo necesario, los permisos a otorgar.

En el caso de que un tercero requiera realizar tratamiento de información a través de sus propias maquinas el tercero deberá certificar por escrito que todo el software utilizado para sus actividades es licenciado. De igual forma, para el tratamiento de datos personales, los terceros deberán certificar el cumplimiento de la Ley de Protección de Datos Personales. Ley 1581 de 2012.

6.7.3. Protección contra códigos maliciosos

ALERGOLOGOS DE OCCIDENTE S.A.S. dispondrá de software de detección de códigos maliciosos y de reparación, así como, de toma de conciencia sobre la seguridad de la información, y en controles apropiados de gestión de cambios y de acceso al sistema. Se deberá considerar las siguientes directrices: Implementar controles para evitar o detectar el uso de software no autorizado (por ejemplo: Política formal, listas blancas de aplicaciones); sitios web malicioso o que se sospecha que lo son (por ejemplo, listas negras); reducir las vulnerabilidades de las que pueda aprovecharse el software malicioso, por ejemplo, por medio de la gestión de la vulnerabilidad técnica; llevar a cabo revisiones regulares del software y del contenido de datos de los sistemas que apoyan los procesos críticos del negocio; se debería investigar formalmente la presencia de archivos no aprobados o de enmiendas no autorizadas.

En el caso del software de detección deberá asegurar su instalación y actualización regular, así como, la reparación del software malicioso para analizar los computadores y medios como una medida de control o en

forma rutinaria; el análisis realizado deberá incluir: el análisis de cualquier archivo recibido por la red o por cualquier forma de medio de almacenamiento, para detectar el software malicioso, antes de uso; el análisis de los adjuntos y descargas de los correos electrónicos, para determinación del software malicioso antes de uso; este análisis se deberá llevar a cabo en diferentes lugares, por ejemplo, en los servidores de los correos electrónicos, en los computadores de escritorio y cuando se ingresa a la red de la organización; el análisis de páginas web, para determinar el software malicioso.

De igual modo, deberá establecer la definición de procedimientos y responsabilidades relacionadas con la protección contra el software malicioso en los sistemas, formación acerca del uso de dichos procedimientos, reporte y recuperación de ataques de software malicioso; la preparación de planes de continuidad del negocio apropiados, para la recuperación de ataques de software malicioso, incluidos todos los datos necesarios, copias de respaldo del software y disposiciones para recuperación; la implementación de procedimientos para recolectar información en forma regular (por ejemplo: la suscripción a listas de correos o la verificación de sitios web que suministran información acerca de nuevo software malicioso).

Deberá implementar procedimientos para verificar información relacionada con el software malicioso, y asegurarse de que los boletines de advertencia sean exactos e informativos; deberá asegurar que se usan fuentes calificadas (por ejemplo: publicaciones respetables, sitios o proveedores en Internet confiables que producen software de protección contra software malicioso, para diferenciar entre falsas alarmas (Hoaxes) y software malicioso real); todos los usuarios deben concientizarse del problema de las falsas alarmas (Hoaxes) y qué hacer en caso de recibirlas.

6.7.4. Entrada y salida de documentos o soportes

La entrada de documentos o soportes debe registrarse indicando el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen según la clasificación de la información, la forma de envío y la persona responsable de la recepción. La salida o envío de documentos o soportes, debidamente autorizada, ha de registrarse indicando el tipo de documento o soporte, la fecha y hora, el receptor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen según el nivel de seguridad, la forma de envío y la persona responsable del envío. La entrada y salida de documentos, se deja registrado en el formato FR-09 Entrada y salida de documentos.

6.7.5. Control de acceso físico

Los lugares que son sede de los sistemas de información que contienen datos personales deben estar debidamente protegidos con el fin de garantizar la integridad y confidencialidad de dichos datos; asimismo, han de cumplir con las medidas de seguridad, correspondientes al documento o soporte acorde con la clasificación de la información que contiene.

ALERGOLOGOS DE OCCIDENTE S.A.S. tiene el deber de poner en conocimiento de su personal las obligaciones que les competen con el objetivo de proteger físicamente los documentos o soportes en los que se encuentran las bases de datos, no permitiendo su manejo, utilización o identificación por personas no autorizadas en el presente manual.

6.8. Copias de respaldo y recuperación de datos

ALERGOLOGOS DE OCCIDENTE S.A.S. establecerá medidas de respaldo de la información a través de mecanismos como (File Server, NAS, Nube, etc.) los cuales deberán quedar custodiados y poseer un método de backup inteligente (Incremental, diferencial, total, comprimida, espejo, etc.).

ALERGOLOGOS DE OCCIDENTE S.A.S. debe producir registros exactos y completos de las copias de respaldo, y procedimientos de restauración documentados; el alcance (por ejemplo, copias de respaldo completas o diferenciales) y la frecuencia con que se hagan las copias de respaldo deberán reflejar los requisitos del negocio de la organización, los requisitos de la seguridad de la información involucrada, y la criticidad de la información para la operación continua de la organización.

De igual modo, las copias de respaldo se deberán almacenar en un lugar remoto, a una distancia suficiente que permita escapar de cualquier daño que pueda ocurrir en el sitio principal; a la información de respaldo se le deberá dar un nivel apropiado de protección física y del entorno, de coherencia con las normas aplicadas en el sitio principal.

ALERGOLOGOS DE OCCIDENTE S.A.S. se encargará de poner a prueba regularmente los medios de respaldo para asegurar que se puede depender de ellos para uso de emergencia en caso necesario; esto se deberá combinar con una prueba de los procedimientos de restauración, y se deberá verificar contra el tiempo de restauración requerido. La prueba de la capacidad para restaurar datos de los que se ha hecho una copia de respaldo se deberá hacer en medios de prueba dedicados, no sobrescribiendo el medio original, en caso de que el proceso de elaboración de copias de respaldo o de restauración falle y cause daño o pérdida de datos irreparables; en situaciones en las que la confidencialidad tiene importancia, las copias de respaldo deberán estar protegidas por medio de cifrado.

ALERGOLOGOS DE OCCIDENTE S.A.S. debe monitorear la ejecución de las copias de respaldo y darles tratamiento a las fallas de las copias de respaldo programadas, para asegurar que se realiza de manera completa y de acuerdo con las políticas de copias establecidas para las mismas.

Las disposiciones relativas a copias de respaldo para sistemas y servicios individuales se deberán probar con regularidad para asegurar que cumplan los requisitos de los planes de continuidad de negocio. En el caso de sistemas y servicios críticos, las disposiciones relativas a copias de respaldo deberán abarcar toda la

información de sistemas, aplicaciones y datos necesarios para recuperar el sistema completo en caso de desastre.

Se deberá determinar el período de retención de la información esencial del negocio, teniendo en cuenta cualquier requisito para copias de archivo que se van a retener permanentemente.

6.9. Política de seguridad en las redes de comunicaciones

6.9.1. Gestión de seguridad en las redes

ALERGOLOGOS DE OCCIDENTE S.A.S. dispondrá de un adecuado nivel de seguridad sobre las redes internas y externas con al ánimo de bloquear cualquier tipo de amenaza por este medio, y evaluará los casos en los que se requiera tener el canal cifrado para la comunicación con sedes o terceros, cuando esto aplique.

El ancho de banda de la red y la capacidad de almacenamiento son limitados; por lo tanto, los usuarios no deben realizar acciones que malgasten los recursos de información ni utilizarlos para actividades personales que monopolicen los recursos injustamente en detrimento de los demás usuarios.

El acceso a datos personales a través de redes de comunicaciones, públicas o privadas, debe someterse a medidas de seguridad equivalentes al acceso local de datos personales.

Las claves de acceso a las redes inalámbricas deben ser cambiadas por el área de sistemas en intervalos recurrentes o de manera inmediata por eventos que atenten contra la seguridad de la red, así como, se debe poseer segmentada la red con los diferentes métodos que ofrezca el proveedor de seguridad.

6.9.2. Transferencia de información

Cuando se realicen acuerdos con organizaciones para el intercambio de información, se especificará el grado de sensibilidad de la información involucrada y las consideraciones de seguridad sobre la misma.

La transmisión de datos personales mediante redes públicas o inalámbricas de comunicaciones electrónicas se llevará a cabo cifrando dichos datos, o utilizando otro mecanismo (Por ejemplo: cifrado por contraseñas o llaves) que garantice que la información no sea inteligible ni manipulada por terceras personas.

El uso de la información por parte de terceros ya sea local o remotamente, deberá ser formalizado por medio de acuerdos y/o cláusulas que hagan obligatorio el cumplimiento de la presente política.

Todos los usuarios son responsables de proteger la confidencialidad e integridad de la información y deberán tener especial cuidado en el uso de los diferentes medios en el intercambio de información que puedan generar una divulgación o modificación no autorizada.

6.9.3. Navegación en internet

ALERGOLOGOS DE OCCIDENTE S.A.S. deberá adoptar medidas para impedir la ejecución o descarga de aplicaciones, así como bloquear sitios que generen peligro y demás fuentes que puedan atentar contra la seguridad de la información.

La navegación en Internet debe realizarse de forma razonable y con propósitos laborales. No se permite la navegación a sitios con contenidos contrarios a la ley o que representen peligro para la organización tales como: pornografía, terrorismo, hacktivismo, segregación racial.

Cuando se requiera acceder a una página con fines laborales y se encuentre bloqueada por los mecanismos de seguridad se deberá informar al área de sistemas, con el fin de realizar un análisis de riesgos y con ello determinar su habilitación.

La descarga de archivos de Internet debe ser con propósitos laborales y de forma razonable para no afectar el servicio.

6.9.4. Política de uso de mensajería instantánea y redes sociales

Ningún mensaje publicado por los colaboradores, en un grupo de discusión de Internet, red social, boletín electrónico o en cualquier otro sistema de información público, representa la posición de ALERGOLOGOS DE OCCIDENTE S.A.S., por lo tanto, los usuarios deberán abstenerse de manifestar opiniones en representación de la organización. Excepto las publicaciones explícitamente autorizadas por la alta gerencia. Por lo tanto, cualquier foto subida o comentario en Facebook, Twitter, Instagram o cualquier otra red social es responsabilidad exclusiva del que la emite y no compromete a la organización.

La carga de cualquier tipo de archivo (fotografía, audio, texto, etc.) por parte de los colaboradores a cualquier red social deberá ser con fines netamente laborales e informativos para garantizar la integridad y privacidad de la información, así mismo, deberá poseer autorización escrita por parte de ALERGOLOGOS DE OCCIDENTE S.A.S. para realizar esta acción.

6.9.5. Política de uso de correo electrónico

Los usuarios del correo electrónico de ALERGOLOGOS DE OCCIDENTE S.A.S. son responsables de evitar prácticas o usos que puedan comprometer la seguridad de la información.

No está permitido el envío a cuentas de correo electrónico personales o sitios de almacenamiento masivo en internet la información propia de la organización clasificada como Confidencial o Reservada que corresponda a clientes, terceros, y/o colaboradores.

Las cuentas de correo electrónico son propiedad de ALERGOLOGOS DE OCCIDENTE S.A.S., las cuales son asignadas a personas que tengan algún tipo de vinculación con la organización, quienes deben utilizar este servicio única y exclusivamente para las tareas propias de la función desarrollada. Por lo tanto, Todos los mensajes enviados y/o recibidos pueden ser sujetos a análisis y conservación permanente por parte de la organización.

No está autorizado el envío de cadenas de correo, correos masivos con archivos adjuntos de gran tamaño que puedan afectar y/o congestionar la red, ni el envío de correos con contenido que atenten contra la integridad y dignidad de las personas y el buen nombre de ALERGOLOGOS DE OCCIDENTE S.A.S..

Todos los correos electrónicos deben contener la nota de seguridad y aviso de cumplimiento de ley de protección de datos personales que la organización determine con respecto al manejo del contenido. El usuario es responsable del contenido del mensaje enviado y de cualquier otra información adjunta al mismo.

6.10. Supervisión de eventos de seguridad

De los accesos a los sistemas de información ALERGOLOGOS DE OCCIDENTE S.A.S., guarda, como mínimo, la identificación del usuario, la fecha y hora en que se lleva a cabo, la base de datos a la que se accede, el tipo de acceso y si ese acceso ha sido autorizado o no autorizado, esta información se podrá obtener por medio de los siguientes métodos de obtención de datos (IP, MAC ADRESS, log de trazabilidad, etc.). En caso de que el registro haya sido autorizado, se guarda la información que permita identificar el registro consultado, estos archivos deberán ser resguardados para su posterior consulta en caso tal de que se materialice un riesgo de seguridad e la información y deba ser presentado como evidencia ante las entidades respectivas.

El área de sistemas se encargará de controlar los mecanismos que permiten el registro de acceso, revisar con carácter mensual la información de control registrada y elaborar un informe de las revisiones realizadas y los problemas detectados el cual será suministrado al Responsable de administrar la Base de Datos. Además, deben impedir la manipulación o desactivación de los mecanismos que permiten el registro de acceso.

Los datos que contiene el registro de acceso deben conservarse, al menos, durante dos años.

No será necesario el registro de acceso cuando los datos se encuentren en equipos de cómputo y se garantice que solamente él tiene acceso y trata los datos personales una sola persona.

ALERGOLOGOS DE OCCIDENTE S.A.S. puede supervisar y registrar todos los aspectos de sus sistemas informáticos incluyendo, entre otros, la supervisión de sitios de Internet visitados por usuarios, la supervisión de charlas y foros de noticias, la supervisión de descargas de archivos y todas las comunicaciones enviadas y recibidas por los mismos utilizando los recursos tecnológicos de la organización.

6.11. Políticas de adquisición, desarrollo y mantenimiento de los sistemas

Cuando se implementen sistemas hechas a la medida o adaptados para ALERGOLOGOS DE OCCIDENTE S.A.S., los desarrolladores o terceros que realicen esta actividad deben establecer, documentar y mantener principios para la construcción de sistemas seguros y aplicarlos a cualquier actividad de implementación de sistemas de información.

Para el desarrollo de nuevos sistemas se debe crear y mantener una metodología que controle el ciclo completo del desarrollo y un mantenimiento seguro. Los requerimientos de seguridad de la información deben ser identificados previos al diseño de los sistemas de tecnología de la información.

Los nuevos desarrollos o cambios significativos de las aplicaciones deberán ser sometidos a pruebas de análisis de vulnerabilidad antes de salir a producción.

Los datos en los ambientes de desarrollo y pruebas se deben seleccionar, proteger y controlar cuidadosamente.

Si el sitio web de la organización captura datos personales mediante formularios este debe contar con la opción de un check box para que el usuario acepte el tratamiento de sus datos, adicional el sitio deberá contar con el protocolo SSL.

6.12. Pruebas no funcionales

ALERGOLOGOS DE OCCIDENTE S.A.S. propenderá porque se realice, al menos una vez al año, un análisis de vulnerabilidades, así como, pruebas de rendimiento, estrés, penetración y hacking ético para todos los sistemas y servicios de la compañía, en caso de poseer proveedores externos deberá solicitarse a estos los resultados de dichos análisis, también, realizar pruebas anuales de ingeniería social para todos los colaboradores.
Es responsabilidad del área de sistemas implementar las actualizaciones de los sistemas operativos y dispositivos de red que sean liberados por los fabricantes.

7. FUNCIONES Y OBLIGACIONES DEL PERSONAL

Todas las personas que intervienen en el almacenamiento, tratamiento, consulta o cualquier otra actividad relacionada con los datos personales y sistemas de información de ALERGOLOGOS DE OCCIDENTE S.A.S., deben actuar de conformidad a las funciones y obligaciones recogidas en el presente apartado.

ALERGOLOGOS DE OCCIDENTE S.A.S., debe informar a su personal de servicio de las medidas y normas de seguridad que compete al desarrollo de sus funciones, así como de las consecuencias de su incumplimiento, mediante cualquier medio de comunicación que garantice su recepción o difusión (correo electrónico, cartelera de anuncios, etc.). De igual modo, debe poner a disposición del personal el presente documento para que puedan conocer la normativa de seguridad y sus obligaciones en esta materia en función del cargo que ocupan.

ALERGOLOGOS DE OCCIDENTE S.A.S. cumple con el deber de informar con la inclusión de acuerdos de confidencialidad y deber de secreto que suscriben, en su caso, los usuarios de sistemas de identificación referidos en el "Anexo 1 PL-01. Organización Bases de Datos" sobre bases de datos y sistemas de información, y mediante una circular informativa dirigida a los mismos.

Las funciones y obligaciones del personal de ALERGOLOGOS DE OCCIDENTE S.A.S., se definen, con carácter general, según el tipo de actividad que desarrollan y, específicamente, por el contenido de este documento. Con carácter general, cuando un usuario trate documentos o soportes que contiene datos personales tiene el deber de custodiarlos, así como de vigilar y controlar que personas no autorizadas no puedan tener acceso a ellos.

El incumplimiento de las obligaciones y medidas de seguridad establecidas en este documento por parte del personal al servicio de ALERGOLOGOS DE OCCIDENTE S.A.S., es sancionable de acuerdo a la normativa aplicable a la relación jurídica existente entre el usuario y ALERGOLOGOS DE OCCIDENTE S.A.S..

Las funciones y obligaciones de los usuarios de las bases de datos personales bajo responsabilidad de ALERGOLOGOS DE OCCIDENTE S.A.S., son las siguientes:

Deber de secreto: Aplica a todas las personas que, en el desarrollo de su profesión o trabajo, acceden a bases de datos personales y vincula tanto a usuarios como a prestadores de servicios contratados; en cumplimiento de este deber, los usuarios de ALERGOLOGOS DE OCCIDENTE S.A.S. no pueden comunicar o relevar a terceras personas, datos que manejen o de los que tengan conocimiento en el desempeño o cargo de sus funciones, y deben velar por la confidencialidad e integridad de los mismos.

Funciones de control y autorizaciones delegadas: ALERGOLOGOS DE OCCIDENTE S.A.S. puede delegar el tratamiento de datos a terceros, para que actúe como encargado del tratamiento, mediante un contrato de transmisión de datos.

Obligaciones relacionadas con las medidas de seguridad implantadas:

- Acceder a las bases de datos solamente con la debida autorización y cuando sea necesario para el

ejercicio de sus funciones.

- No revelar información a terceras personas ni a usuarios no autorizados. Observar las normas de seguridad y trabajar para mejorarlas.
- No realizar acciones que supongan un peligro para la seguridad de la información.
- No sacar información de las instalaciones de la organización sin la debida autorización.

Uso de recursos y materiales de trabajo: Debe estar orientado al ejercicio de las funciones asignadas. No se autoriza el uso de estos recursos y materiales para fines personales o ajenos a las tareas correspondientes al puesto de trabajo. Cuando, por motivos justificados de trabajo, sea necesaria la salida de dispositivos periféricos o extraíbles, deberá comunicarse a los Responsables de administrar las bases de datos que podrán autorizarla y, en su caso, registrarla.

Uso de impresoras, escáneres y otros dispositivos de copia: Cuando se utilicen este tipo de dispositivos debe procederse a la recogida inmediata de las copias, evitando dejar éstas en las bandejas de éstos.

Obligación de notificar incidencias: Los usuarios tienen la obligación de notificar las incidencias de las que tenga conocimiento a los Responsables de administrar las bases de datos u Oficial de protección de datos, quienes se encargarán de su gestión y resolución. Algunos ejemplos de incidencias son: la caída de los sistemas de información o módulos que permitan el acceso a los datos personales a personas no autorizadas, el intento no autorizado de la salida de un documento o soporte, la pérdida de datos o la destrucción total o parcial de soportes, el cambio de ubicación física de bases de datos, el conocimiento por terceras personas de contraseñas, la modificación de datos por personal no autorizado, entre otros.

Deber de custodia de los soportes utilizados: Obliga al usuario autorizado a vigilar y controlar que personas no autorizadas accedan a la información contenida en los soportes. Los soportes que contienen bases de datos deben identificar el tipo de información que contienen mediante un sistema de etiquetado y ser inventariados.

Responsabilidad sobre los terminales de trabajo y portátiles: Cada usuario es responsable de su propio terminal de trabajo; cuando esté ausente de su puesto, debe bloquear dicho terminal (ej. protector de pantalla con contraseña) para impedir la visualización o el acceso a la información que contiene; y tiene el deber de apagar el terminal al finalizar la jornada laboral. Asimismo, los ordenadores portátiles han de estar controlados en todo momento para evitar su pérdida o sustracción.

Uso limitado de Internet y correo electrónico: El envío de información por vía electrónica y el uso de Internet por parte del personal está limitado al desempeño de sus actividades en ALERGOLOGOS DE OCCIDENTE S.A.S..

Salvaguarda y protección de contraseñas: Las contraseñas proporcionadas a los usuarios son personales e intransferibles, por lo que se prohíbe su divulgación o comunicación a personas no autorizadas. Cuando el

usuario accede por primera vez con la contraseña asignada es necesario que la cambie. Cuando sea necesario restaurar o recuperar la contraseña, el usuario debe comunicarlo al administrador del sistema.

Copias de respaldo y recuperación de datos: Debe realizarse copia de seguridad de toda la información de bases de datos personales de la empresa.

Deber de archivo y gestión de documentos y soportes: Los documentos y soportes deben de ser debidamente archivados con las medidas de seguridad establecidas en el numeral 6 del presente manual.

Uso de dispositivos móviles de la organización: Todo usuario que tenga en su poder cualquier dispositivo móvil propiedad de ALERGOLOGOS DE OCCIDENTE S.A.S. debe ser responsable por cualquier daño físico que pueda tener el dispositivo y tiene la responsabilidad de asignar una contraseña de bloqueo segura. En caso de pérdida o robo deberá dar aviso inmediato a las áreas respectivas y se considerará como un incidente de seguridad de la información. En estos dispositivos no deberá instalar aplicaciones que no estén autorizadas.

Uso de dispositivos móviles personales: Cuando el usuario utilice el dispositivo para actividades de la organización tiene la responsabilidad de asignar una contraseña de bloqueo segura, esto con la finalidad de impedir que personas ajenas tengan acceso a la información de ALERGOLOGOS DE OCCIDENTE S.A.S. contendida en él. El área de sistemas deberá definir las condiciones sobre las cuales se autorizará a un colaborador habilitar el correo corporativo en su dispositivo móvil. Para el uso de equipos portátiles personales en horario laboral y su utilización en actividades de administración y procesamiento de información de la organización el usuario deberá solicitar autorización.

Manejo de memorias externas: Los puertos de los equipos de cómputo deben estar bloqueados. Sin embargo, para aquellos equipos que se autorice la habilitación de los puertos para conectar dispositivos externos como USB, discos duros, tarjetas SD, Celulares o cualquier otro dispositivo, se recomienda usar lo mínimo posible esta opción, ya que estos pueden contener virus o software malicioso que puede afectar el equipo. Adicional, como por este medio también puede extraerse información no autorizada, es responsabilidad de los usuarios los incidentes de la información que administres y de los daños que esto pueda causar.

8. BASES DE DATOS Y SISTEMAS DE INFORMACIÓN

Las bases de datos almacenadas y tratadas por ALERGOLOGOS DE OCCIDENTE S.A.S., se recogen en el “Anexo 1 PL-01. Organización Bases de Datos”, en el cual se presentan las siguientes características de cada una de ellas:

- Nombre de la Base de Datos
- Información contenida
- Finalidades
- Tipo de Dato

- Sistema de tratamiento
- Cantidad de Titulares
- Origen y procedencia de los datos
- Encargados del Tratamiento
- Responsable de administrar la base de datos
- Control de Acceso
- Sistema de identificación y autenticación.

Nota: El nombramiento de los Responsables de Administrar las Bases de Datos no exonera al responsable del tratamiento o encargado del tratamiento de sus obligaciones.

ALERGOLOGOS DE OCCIDENTE S.A.S. identifica en el "Anexo 1 PL-01. Organización Bases de Datos" al Oficial de Protección de Datos. Cuando exista contrato de transmisión de datos, los encargados del tratamiento se identifican en el anexo sobre transmisión de datos de este documento. Los encargados del tratamiento deberán cumplir con las funciones y obligaciones relacionadas con las medidas en materia de seguridad recogidas en el presente documento.

9. PROCEDIMIENTO DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE INCIDENCIAS

ALERGOLOGOS DE OCCIDENTE S.A.S. establece un procedimiento de notificación, gestión y respuesta de incidencias con el fin de garantizar la confidencialidad, disponibilidad e integridad de la información contenida en las bases de datos que están bajo su responsabilidad.

Todos los usuarios y responsables de procedimientos, así como cualquier persona que tenga relación con el almacenamiento, tratamiento o consulta de las bases de datos recogidas en este documento, deben conocer el procedimiento para actuar en caso de incidencia. Algunos ejemplos de incidencias son: caída de sistemas de seguridad que permita el acceso a los datos personales a personas no autorizadas, el intento no autorizado de la salida de un documento o soporte, la pérdida de datos o la destrucción total o parcial de soportes, el cambio de ubicación física de bases de datos, el conocimiento por terceras personas de contraseñas, la modificación de datos por personal no autorizado, entre otros.

El procedimiento de notificación, gestión y respuesta ante incidencias es el siguiente:

- Cuando una persona tenga conocimiento de una incidencia (perdida, hurto y/o acceso no autorizado) que afecte o pueda afectar la confidencialidad, disponibilidad e integridad de la información protegida de la empresa o alguno de los Encargados deberá comunicarlo, de manera inmediata, al Oficial de Protección de Datos, describiendo detalladamente el tipo de incidencia producida, e indicando las personas que hayan podido tener relación con la incidencia, la fecha y hora en que se ha producido, la

persona que notifica la incidencia, la persona a quién se le comunica y los efectos que ha producido.

- Una vez comunicada la incidencia ha de solicitar al Oficial de Protección de Datos un acuse de recibo en el que conste la notificación de la incidencia con todos los requisitos enumerados anteriormente.
- ALERGOLOGOS DE OCCIDENTE S.A.S., crea un registro de incidencias que debe contener: el tipo de incidencia (Fraude Interno o externo, Daños a activos físicos, Fallas tecnológicas, Ejecución y administración de procesos), fecha y hora de ésta, persona que la notifica, persona a la que se le comunica, efectos de la incidencia y medidas correctoras cuando corresponda. Este registro es gestionado por el Oficial de Protección de Datos, remitirse al FR-08 Registro de incidentes de seguridad.
- Asimismo, debe implementar los procedimientos para la recuperación de los datos cuando aplica, indicando quien ejecuta el proceso, los datos restaurados y, en su caso, los datos que han requerido ser grabados manualmente en el proceso de recuperación.
- Adicionalmente, el Oficial de Protección de Datos debe informar a la Superintendencia de Industria y Comercio, mediante el RNBD dentro de los 15 días hábiles siguientes de haber sido detectado.
- Finalmente, ALERGOLOGOS DE OCCIDENTE S.A.S. notificará del incidente a los Titulares, cuando se identifique que puedan verse afectados de manera significativa.

10. MEDIDAS PARA EL TRANSPORTE, DESTRUCCIÓN Y REUTILIZACIÓN DE DOCUMENTOS Y SOPORTES

Cuando corresponda desechar cualquier documento (original, copia o reproducción) o soporte que contenga datos personales debe procederse a su destrucción o borrado, a través de la implementación de medidas orientadas a evitar el acceso o recuperación de la información contenida en dicho documento o soporte, en el FR-01 Tabla de retención documental, se define el tipo de disposición que se le debe dar a cada uno de los documentos que se incluyen en el sistema de gestión de protección de datos.

Cuando se lleve a cabo el traslado físico de documentos o soportes deben adoptar las medidas necesarias para impedir el acceso indebido, la manipulación, la sustracción o la pérdida de la información. El traslado de soportes que contengan datos personales se realiza cifrando la información, o utilizando cualquier otro mecanismo que garantice que no se manipule ni se acceda a la misma.

Los datos contenidos en dispositivos portátiles deben estar cifrados cuando se hallen fuera de las instalaciones que están bajo control de ALERGOLOGOS DE OCCIDENTE S.A.S., cuando no sea posible el cifrado, se debe evitar el tratamiento de datos personales mediante este tipo de dispositivos; sin embargo, se podrá proceder al tratamiento cuando sea estrictamente necesario, adoptando para ello medidas de seguridad que tengan en cuenta los riesgos asociados a la actividad.

11. POLÍTICAS DE CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN

Todos los recursos de información y los procesos asociados deben contar con actividades de contingencia e instalaciones de procesamiento de información con redundancia suficiente para soportar la disponibilidad de los servicios misionales y críticos para el funcionamiento de la organización.

Se deben desarrollar, documentar, implementar y probar, al menos una vez al año, los procedimientos para asegurar una recuperación razonable y a tiempo, de la información crítica, sin disminuir los niveles de seguridad establecidos.

12. POLÍTICAS DE AUDITORÍAS

Las auditorias llevadas a cabo sobre los sistemas de información y las instalaciones de almacenamiento deberán ser coordinadas, planificadas y debidamente socializadas a las partes objeto de revisión, con el fin de minimizar las interrupciones en los procesos de negocio.

Las bases de datos que contengan datos personales, objeto de tratamiento por ALERGOLOGOS DE OCCIDENTE S.A.S., clasificadas con nivel de seguridad sensible o privado, se han de someter, al menos una vez al año, a una auditoría interna o externa que verifique el cumplimiento de las medidas de seguridad contenidas en este manual.

ALERGOLOGOS DE OCCIDENTE S.A.S., realizará una auditoría extraordinaria siempre que se realicen modificaciones sustanciales en el sistema de información que puedan afectar al cumplimiento de las medidas de seguridad, con el fin de verificar la adaptación, adecuación y eficacia de estas.

Las auditorías concluirán con un informe de auditoría que contendrá:

- El dictamen sobre la adecuación de las medidas y controles a la normativa sobre protección de datos.
- La identificación de las deficiencias halladas y la sugerencia de medidas correctoras o complementarias necesarias.
- La descripción de los datos, hechos y observaciones en que se basen los dictámenes y las recomendaciones propuestas.

El Oficial de Protección de Datos estudiará el informe y trasladará las conclusiones al Responsable de administrar las bases de datos para que implemente las medidas correctoras.

13. MEDIDAS DE SEGURIDAD

ALERGOLOGOS DE OCCIDENTE S.A.S., con el fin de cumplir con el principio de seguridad consagrado en el artículo 4 literal g) de la LEPD, ha implementado medidas técnicas, humanas y administrativas necesarias para

garantizar la seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Por otra parte, ALERGOLOGOS DE OCCIDENTE S.A.S., mediante la suscripción de los correspondientes contratos de transmisión, ha requerido a los encargados del tratamiento con los que trabaje la implementación de las medidas de seguridad necesarias para garantizar la seguridad y confidencialidad de la información en el tratamiento de los datos personales.

A continuación, se exponen las medidas de seguridad implantadas por ALERGOLOGOS DE OCCIDENTE S.A.S. que están recogidas y desarrolladas en su PL-02 Políticas Internas de Seguridad (Tablas I, II, III y IV).

TABLA I: Medidas de seguridad comunes para todo tipo de datos (pública, privada, confidencial, reservada) y bases de datos (automatizadas, no automatizadas)	
Gestión de documentos y soportes	1. Medidas que eviten el acceso indebido o la recuperación de los datos que han sido descartados, borrados o destruidos. 2. Acceso restringido al lugar donde se almacenan los datos. 3. Autorización del responsable de Administrar las bases de datos para la salida de documentos o soportes por medio físico o electrónico. 4. Sistema de etiquetado o identificación del tipo de información. 5. Inventario de soportes.
Control de acceso	1. Acceso de usuarios limitado a los datos necesarios para el desarrollo de sus funciones. 2. Lista actualizada de usuarios y accesos autorizados. 3. Mecanismos para evitar el acceso a datos con derechos distintos de los autorizados. 4. Concesión, alteración o anulación de permisos por el personal autorizado
Incidencias	1. Registro de incidencias: tipo de incidencia, momento en que se ha producido, emisor de la notificación, receptor de la notificación, efectos y medidas correctoras. 2. Procedimiento de notificación y gestión de incidencias.
Personal	1. Definición de las funciones y obligaciones de los usuarios con acceso a los datos. 2. Definición de las funciones de control y autorizaciones delegadas por el responsable del tratamiento. 3. Divulgación entre el personal de las normas y de las consecuencias del incumplimiento de éstas.
Manual Interno de Seguridad	1. Elaboración e implementación del Manual de obligado cumplimiento para el personal. 2. Contenido mínimo: ámbito de aplicación, medidas y procedimientos de seguridad, funciones y obligaciones del personal, descripción de las bases de datos, procedimiento ante incidencias, identificación de los encargados del tratamiento.

TABLA II: Medidas de seguridad comunes para todo tipo de datos

(pública, privada, confidencial, reservada) según el tipo de bases de datos	
Bases de datos no automatizadas	
Archivo	1. Archivo de documentación siguiendo procedimientos que garanticen una correcta conservación, localización y consulta, que permitan el ejercicio de los derechos de los Titulares.
Almacenamiento de documentos	1. Dispositivos de almacenamiento con mecanismos que impidan el acceso a personas no autorizadas.
Custodia de documentos	1. Deber de diligencia y custodia de la persona a cargo de documentos durante la revisión o tramitación de estos.
Bases de datos automatizadas	
Identificación y autenticación	1. Identificación personalizada de usuarios para acceder a los sistemas de información y verificación de su autorización. 2. Mecanismos de identificación y autenticación; Contraseñas: asignación y caducidad.
Telecomunicaciones	1. Acceso a datos mediante redes seguras.

TABLA III: Medidas de seguridad para datos privados según el tipo de bases de datos	
Bases de datos no automatizadas	
Auditoría	1. Auditoría ordinaria (interna o externa) cada dos meses. 2. Auditoría extraordinaria por modificaciones sustanciales en los sistemas de información. 3. Informe de detección de deficiencias y propuesta de correcciones. 4. Análisis y conclusiones del responsable de seguridad y del responsable del tratamiento.
Responsable de seguridad	1. Designación de uno o varios Administradores de las bases de datos. 2. Designación de uno o varios encargados del control y la coordinación de las medidas del Manual Interno de Seguridad. 3. Prohibición de delegación de la responsabilidad del Responsable del tratamiento en los Administradores de las bases de datos.
Manual Interno de Seguridad	1. Controles periódicos de cumplimiento.
Bases de datos automatizadas	
Gestión de documentos y soportes	1. Registro de entrada y salida de documentos y soportes: fecha, emisor y receptor, número, tipo de información, forma de envío, responsable de la recepción o entrega.

Control de acceso	1. Control de acceso al lugar o lugares donde se ubican los sistemas de información.
Identificación y autenticación	1. Mecanismo que limite el número de intentos reiterados de acceso no autorizados. 2. Mecanismos de cifrado de datos para la transmisión.
Incidencias	1. Registro de los procedimientos de recuperación de los datos, persona que los ejecuta, datos restaurados y datos grabados manualmente. 2. Autorización del responsable del tratamiento para la ejecución de los procedimientos de recuperación.

TABLA IV: Medidas de seguridad para datos sensibles según el tipo de bases de datos	
Bases de datos no automatizadas	
Control de acceso	1. Acceso solo para personal autorizado. 2. Mecanismo de identificación de acceso. 3. Registro de accesos de usuarios no autorizados. 4. Destrucción que impida el acceso o recuperación de los datos.
Almacenamiento de documentos	1. Archivadores, armarios u otros ubicados en áreas de acceso protegidas con llaves u otras medidas. 2. Medidas que impidan el acceso o manipulación de documentos almacenados de forma física.
Bases de datos automatizadas	
Control de acceso	1. Sistema de etiquetado confidencial.
Identificación y autenticación	1. Mecanismos de cifrado de datos para la transmisión y almacenamiento.
Almacenamiento de documentos	1. Registro de accesos: usuario, hora, base de datos a la que accede, tipo de acceso, registro al que accede 2. Control del registro de accesos por el responsable de seguridad. Informe mensual.
Telecomunicaciones	1. Acceso y transmisión de datos mediante redes electrónicas seguras. 2. Transmisión de datos mediante redes cifrados (VPN).

14. DISPOSICIÓN FINAL

El presente manual ha sido aprobado por ALERGOLOGOS DE OCCIDENTE S.A.S., como responsable del tratamiento de datos, aceptando su contenido, ordenando su ejecución y cumplimiento, con carácter general por todo el personal de la empresa, y en particular, por aquellos a los referidos en este documento.

15. APÉNDICE

- Estándar Internacional ISO/IEC 27001:2013.
- Ley estatutaria 1581 de 2012.

16. ELABORACIÓN Y APROBACIÓN DEL DOCUMENTO

REVISIÓN Y APROBACIÓN DEL DOCUMENTO			
Elaborado por:	*PROTECDATA COLOMBIA*	**Aprobado por:**	
		Cargo	
Fecha:	**2022-08-02**	**Fecha:**	

17. HISTÓRICO DE DOCUMENTOS

FECHA	**VERSIÓN**	**DESCRIPCIÓN DEL CAMBIO**