LA SOCIEDAD ENDRESS+HAUSER (COLOMBIA) S.A.S.

CAPÍTULO I

POLÍTICAS Y SEGURIDAD DE PROCEDIMIENTOS

1. BASE LEGAL Y ÁMBITO DE APLICACIÓN.

El derecho a la Protección de los Datos tiene como finalidad permitir a todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en archivos o bases de datos. Este derecho constitucional se recoge en los artículos 15 y 20 de la Constitución Política; en la Ley Estatutaria 1581 de 2012, por la cual se dictan disposiciones generales para la ley de Protección de Datos Personales (LEPD); en el decreto 1074 de 2015, y capítulo 25 sección 3 Articulo 2.2.2.25.3.2. del decreto 1074 de 2015, por el cual se reglamenta parcialmente la 1581 de 2012.

Cuando el Titular de los datos presta su consentimiento para que estos formen parte de una base de datos de una institución, pública o privada, jurídica o natural, ésta se hace mediante el responsable del tratamiento de estos datos y adquiere una serie de obligaciones como son: la de tratar dichos datos con seguridad y cautela, velar por su integridad y aparecer como órgano a quien el Titular puede dirigirse para el seguimiento de la información y el control de la misma, pudiendo ejercitar los derechos de consultas y reclamos.

Si bien, la responsabilidad del tratamiento de los datos recae en el responsable del tratamiento, sus competencias se materializan en las funciones que corresponden a su personal de servicio. El personal de la institución responsable del tratamiento con acceso, directo o indirecto, a bases de datos que contienen datos personales han de conocer la normativa de protección de datos, la política de protección de datos de la organización; y deben cumplir con las obligaciones en materia de seguridad de los datos correspondientes a sus funciones y cargo.

Para velar con el cumplimiento de sus obligaciones de seguridad, la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S., nombra a la señora María Duque Pulido como encargado de seguridad para desarrollar, coordinar, controlar y verificar el cumplimiento de las medidas de seguridad recogidas en esta política.

Esta política será aplicable a todos los datos personales registrados en bases de datos que sean objeto de tratamiento por el responsable del tratamiento y se encuentra dirigida a

todos los usuarios de datos, que son tanto el personal propio como al personal externo de la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S.

Todos los usuarios identificados en el presente documento de Seguridad están obligados a cumplir con las medidas de seguridad establecidas para el tratamiento de los datos y están sujetos al deber de confidencialidad, incluso después de acabada su relación laboral o profesional con la organización responsable del tratamiento. El deber de confidencialidad, recogido en el artículo 4 literal h) de la ley de Protección de Datos (LEPD), se formaliza a través de la firma de un acuerdo de confidencialidad suscrito entre el usuario y el responsable del tratamiento.

Tipo de norma	Número y fecha de expedición	Título	Expedida por	Aplicación específica
Ley estatutaria	1581 de 2012	"Por la cual se dictan disposiciones generales para la protección de datos personales"	Congreso de la República.	Por medio de la cual desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.
Ley	1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"	Congreso de la República	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Decreto	1377 de 2013	"Por medio del cual se reglamenta parcialmente la ley 1581 de 2012"	Presidente de la República de Colombia.	Mediante la cual se reglamenta parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto	1074 de 2015	"Por medio del cual se expide el decreto único reglamentario del sector Comercio, Industria y Turismo."	Presidente de la república de Colombia.	El Ministerio de Comercio, Industria y Turismo tiene como objetivo primordial dentro del marco de su competencia: formular, adoptar, dirigir y coordinar las políticas generales en materia de desarrollo económico y social del país, relacionadas con la competitividad, integración y desarrollo de los sectores productivos de la industria.

2. DEFINICIONES ESTABLECIDAS EN EL ARTÍCULO 3 DE LA LEPD Y EL CAPÍTULO 25 SECCIÓN 1 ARTÍCULO 2.2.2.25.1.3 DEL DECRETO 1074 DE 2015.

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.

Autenticación: Procedimiento de verificación de la identidad de un usuario.

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.

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 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.

Dato público: Es el dato que no sea semiprivado, privado o sensible. 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.

Datos sensibles: Se entiende por datos sensible aquellos 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, la pertenencia a sindicatos, 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.

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.

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 seguridad: Una o varias personas designadas por el responsable del tratamiento para el control y la coordinación de las medidas de seguridad. • Sistema de información: Conjunto de bases de datos, programas, soportes y/o equipos empleados para el tratamiento de datos personales.

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.

Soporte: 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, 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.

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

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 estos 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.

3. PRINCIPIOS DE LA PROTECCIÓN DE DATOS.

El artículo 4 de la Ley de Protección de Datos (LEPD), establece unos principios para el tratamiento de datos personales que se han de aplicar, de manera armónica e integral, en el desarrollo, interpretación y aplicación de la Ley. Los principios legales de la protección de datos son los siguientes:

Principio de legalidad: El tratamiento de los datos es una actividad reglada que debe sujetarse a lo establecido en la Ley de Protección de Datos (LEPD), el Decreto 1074 de 2015 y en las demás disposiciones que la desarrollen.

Principio de finalidad: El tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular.

Principio de libertad: El tratamiento solo puede ejercerse con el consentimiento previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que revele el consentimiento. El tratamiento de los datos requiere la autorización previa e informada del Titular por cualquier medio que permita ser consultado con posterioridad, salvo en los siguientes casos que exceptúa el artículo 10 de la Ley de Protección de Datos (LEPD):

Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.

- Datos de naturaleza pública.
- Casos de urgencia médica o sanitaria.

Principio de veracidad o calidad: La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

Principio de transparencia: En el tratamiento debe garantizarse el derecho del Titular a obtener del responsable del tratamiento o del encargado del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan. En el momento de solicitar la autorización al titular, el responsable del tratamiento deberá informarle de manera clara y expresa lo siguiente, conservando prueba del cumplimiento de este deber:

- El tratamiento al cual será sometidos sus datos y la finalidad del mismo.
- El carácter facultativo de la respuesta del Titular a las preguntas que le sean hechas cuando éstas traten sobre datos sensibles o sobre datos de niños, niñas o adolescentes.
- Los derechos que le asisten como Titular. - La identificación, dirección física, correo electrónico y teléfono del responsable del tratamiento.

Principio de acceso y circulación restringida: El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la Ley de Protección de Datos (LEPD) y la Constitución. En este sentido, el tratamiento solo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la Ley. Los datos personales, salvo la información pública, no podrán estar disponibles en internet y otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente

controlable para brindar un conocimiento restringido solo a los Titulares o terceros autorizados conforme a la Ley.

Principio de seguridad: La información sujeta a tratamiento por el responsable del tratamiento o encargado del tratamiento se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. El responsable del tratamiento tiene la responsabilidad de implantar las medidas de seguridad correspondientes y de ponerlas en conocimiento todo personal que tenga acceso, directo o indirecto, a los datos. Los usuarios que accedan a los sistemas de información del responsable del tratamiento deben conocer y cumplir con las normas y medidas de seguridad que correspondan a sus funciones. En este documento se recogen estas normas y medidas de seguridad, de obligado cumplimiento para todo usuario y personal de la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S. Cualquier modificación de las normas y medidas de seguridad de datos personales por parte del responsable del tratamiento debe ser conocimiento de los usuarios.

Principio de confidencialidad: Todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo solo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la LEPD y en los términos de esta.

4. CATEGORÍAS ESPECIALES DE DATOS.

4.1 Datos sensibles

Los datos sensibles son aquellos 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, la pertenencia a sindicatos, 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.

Según el artículo 6 de la Ley Estatuaria de Protección de datos Personales (LEPD), se prohíbe el tratamiento de datos sensibles, excepto cuando:

El Titular haya dado su autorización explícita a dicho tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización.

El tratamiento sea necesario para salvaguardar el interés vital del Titular y éste se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.

El tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular.

El tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

El tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

4.2 Derechos de los niños, niñas y adolescentes.

El tratamiento de datos personales de niños, niñas y adolescentes está prohibido, excepto cuando se trate de datos de naturaleza pública, y cuando dicho tratamiento cumpla con los siguientes requisitos:

- Que responda y respete el interés superior de los niños, niñas y adolescentes.
- Que se asegure el respeto de sus derechos fundamentales.

Cumplidos los anteriores requisitos, el representante legal del niño, niña o adolescente otorgará la autorización previo ejercicio del menor a su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto.

Es tarea del Estado y las entidades educativas proveen información y capacitar a los representantes legales y tutores sobre los posibles riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del tratamiento indebido de sus datos personales, y proveer de conocimiento sobre el uso responsable y seguro de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás.

Todo responsable y encargado involucrado en el tratamiento de los datos personales de niños, niñas y adolescentes deberá velar por su uso adecuado, cumpliendo siempre con los principios y obligaciones recogidos en la LEPD y el Decreto 1074 de 2015. En todo caso, el tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes.

Los derechos de acceso, corrección, supresión, revocación o reclamo por infracción sobre los datos de los niños, niñas adolescentes se ejercerán por las personas que estén facultadas para representarlos.

4.3 Derechos de los Titulares.

De acuerdo con el artículo 8 de la LEPD y al capítulo 25 sección 4 del decreto 1074 de 2015, los Titulares de los datos pueden ejercer una serie de derechos en relación con el tratamiento de sus datos personales. Estos derechos podrán ejercerse por las siguientes personas.

- Por el Titular, quién deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición el responsable.
- Por sus causahabientes, quienes deberán acreditar tal calidad.
- Por el representante y/o apoderado del Titular, previa acreditación de la representación o apoderamiento.
- Por estipulación a favor de otro y para otro.
- Los derechos de los niños, niñas o adolescentes se ejercerán por las personas que estén facultadas para representarlos.
- Los derechos del Titular son los siguientes:

Derecho de acceso o consulta: Se trata del derecho del Titular a ser informado por el responsable del tratamiento, previa solicitud, respecto al origen, uso y finalidad que les han dado a sus datos personales.

Derechos de quejas y reclamos: La Ley distingue cuatro tipos de reclamos:

Reclamo de corrección: El derecho del Titular a que se actualicen, rectifique o modifiquen aquellos datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.

Reclamo de supresión: El derecho del Titular a que se supriman los datos que resulten inadecuados, excesivos o que no respeten los principios, derechos y garantías constitucionales y legales.

Reclamo de revocación: El derecho del Titular a dejar sin efecto la autorización previamente prestada para el tratamiento de sus datos personales.

Reclamo de infracción: El derecho del Titular a solicitar que se subsane el incumplimiento de la normativa en materia de Protección de Datos.

Derecho a solicitar prueba de la autorización otorgada al responsable del tratamiento: salvo cuando se excluya como requisito para el tratamiento según el artículo 10 de la LEPD.

Derecho a presentar ante la Superintendencia de Industria y Comercio quejas por infracciones: El Titular o causahabiente solo podrá elevar esta queja una vez haya agotado el trámite de consulta o reclamo ante el responsable del tratamiento o encargado del tratamiento.

5. AUTORIZACIÓN DE LA POLÍTICA DE TRATAMIENTO.

De acuerdo con el artículo 9 de la LEPD, para el tratamiento de datos personales se requiere la autorización previa e informada del Titular. Mediante la aceptación de la presente política, todo Titular que facilite información relativa a sus datos personales está consintiendo el tratamiento de sus datos por parte de la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S., en los términos y condiciones recogidos en la misma.

No será necesaria la autorización del Titular cuando se trate de:

Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.

- Datos de naturaleza pública.
- Casos de urgencia médica o sanitaria.
- Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
- Datos relacionados con el Registro Civil de las personas.

6. RESPONSABLE DEL TRATAMIENTO.

El responsable del tratamiento de las bases de datos objeto de esta política es la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S., cuyos datos de contacto son:

Dirección: CR 17 93 09 OF 201
Correo electrónico: maria.duque@endress.com
Teléfono: 3188133205

6.1 Las obligaciones del responsable del tratamiento.

Las obligaciones en materia de seguridad de los datos de la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S. son las siguientes:

- Coordinar e implantar las medidas de seguridad recogidas en el presente documento.

- Difundir el referido documento entre el personal afectado.
- Mantener esta política actualizada y revisada si hay cambios relevantes en el sistema de información, el sistema de tratamiento, la organización de la institución, el contenido de la información de las bases de datos o por controles periódicos realizados. De igual modo, se revisará su contenido cuando se produzca algún cambio que pueda afectar al cumplimiento de las medidas de seguridad.
- Designar uno o más responsables de seguridad e identificar a los usuarios autorizados para acceder a las bases de datos.
- Cuidar que el acceso mediante sistemas y aplicaciones informáticas se lleve a cabo mediante acceso identificado y contraseña.
- Autorizar, salvo delegación expresa a usuarios autorizados e identificados en esta política, la salida de soportes fuera de los establecimientos donde se encuentran las bases de datos; las entradas y salidas de información por red, mediante dispositivos de almacenamiento electrónico o en papel y el uso de módems y las descargas de datos.
- Verificar semestralmente la correcta aplicación del procedimiento de copias de respaldo y recuperación de datos.
- Garantizar la existencia de una lista de usuarios autorizados y perfiles de usuario.
- Analizar, junto con el responsable de seguridad correspondiente, las incidencias registradas para establecer las medidas correctoras oportunas, al menos cada dos meses.
- Realizar una auditoría, interna o externa, para verificar el cumplimiento de las medidas de seguridad en materia de protección de datos, al menos cada año.

7. TRATAMIENTO Y FINALIDADES DE LAS BASES DE DATOS.

En el desarrollo de sus actividades, la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S., trata datos personales relativos a personas naturales contenidos y tratados en bases de datos para finalidades legítimas, cumpliendo con la Constitución y la Ley.

Según lo establecido en la Ley 1581 de 2012 y según las autorizaciones impartidas por los titulares de la información, la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S. realizará operaciones con recolección de datos, su almacenamiento, uso, circulación y/o supresión, entrega de los datos a terceras entidades a título de encargados o responsables; esto según el acuerdo al que se llegue. Este Tratamiento de datos se realizará exclusivamente para las finalidades autorizadas y previstas en la presente Política y en las autorizaciones específicas otorgadas por parte del titular. De la misma forma se realizará Tratamiento de Datos Personales cuando exista una obligación legal o contractual para ello, siempre bajo los lineamientos de las políticas de Seguridad de la Información de la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S., en todos los casos los datos personales podrán ser tratados con la finalidad de adelantar los procesos de control y auditorías internas y

externas y evaluaciones que realicen los organismos de control. Así mismo y en ejecución del objeto social de la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S., los datos personales serán tratados de acuerdo con el grupo de interés y en proporción a la finalidad o finalidades que tenga cada tratamiento, como se describe a continuación:

En la siguiente tabla se muestran las bases de datos y las finalidades asignadas a cada una.

TABLA I. BASES DE DATOS Y FINALIDADES

Empleados

Los datos serán utilizados con las siguientes finalidades: Solicitud de datos concernientes a identificación personal, información de contacto, datos de carácter académico, datos del historial laboral, profesional y financiero; desarrollar adecuadamente el proceso de registro y vinculación laboral; implementar acciones de bienestar laboral; difundir ofertas laborales para participar en procesos internos de selección de personal en la Institución; comunicar información institucional; ejecutar actividades con fines estadísticos; desarrollar adecuadamente el proceso de actualización de los datos; desarrollar los procesos de inscripción en congresos; eventos o seminarios organizados por la Institución; adelantar la actualización de datos y verificación de identidad de los trabajadores y sus familiares (pareja, padres hijos); citar a los aspirantes en proceso de selección a las entrevistas programadas, realización de visitas domiciliarias, verificación de referencias laborales, personales, experiencia laboral y trayectoria profesional; Suministro de información a las empresas con la cuales se tiene convenio, al fondo de empleados, confección de artículos de dotación, envío de información a través de mensajes de texto y correos electrónicos, entrega y asignación de equipos a los colaboradores; redacción de informes de gestión humana; proceso de afiliación al sistema de seguridad social y cajas de compensación del colaborador y sus beneficiarios; entrega de referencias laborales, uso de imágenes fotográficas y videos con fines corporativos, para llevar a cabo la búsqueda de antecedentes e información relacionada en las listas vinculantes para los sistemas SAGRILAFT (Sistema de Autocontrol y Gestión del Riesgo Integral contra el Lavado de Activos, Financiación del Terrorismo y Financiamiento a la Proliferación de Armas de Destrucción Masiva) y PTEE (Programa de Transparencia y Ética Empresarial), obtención y suministro de datos de los hijos de los colaboradores en el desarrollo de actividades recreativas y de bienestar a través de la Instituciones o entidades aliadas, evaluaciones de desempeño; generación de certificaciones laborales, de ascenso, traslado, entrevista de retiro, en procesos de auditoría y control interno y externo, en la entrega de reportes obligatorios institucionales en entrevistas de retiro, desactivación de sistemas de información, uso de huellas digitales y demás datos de salud y/o datos sensibles para los fines misionales; las anteriores finalidades son enunciativas y no taxativas.

Proveedores Nacionales y Extranjeros

Los datos se utilizarán con estas finalidades: Solicitud de ofertas y propuestas económicas para adquirir productos y servicios; análisis y viabilidad de cada producto o servicio; envío de comunicaciones por texto y correos electrónicos; presentación de informes pertinentes a los diferentes entes de control; revisión y verificación de referencias comerciales; gestiones pre contractuales y contractuales; suministro de información en procesos de auditoría interna y externa que se realicen al interior de la institución; envío de información de los productos, servicios o novedades de la empresa; rastreo en bases de datos restrictivas SAGRILAFT.

Clientes Nacionales y Extranjeros

Los datos serán utilizados con las siguientes finalidades: Solicitud de ofertas y propuestas económicas para la adquisición de productos y servicios; para el análisis y viabilidad de cada producto y/o servicio; envío de comunicaciones a través de mensajes de texto y correos electrónico; presentación de informes pertinentes a los diferentes entes de control; revisión y verificación de referencias comerciales; gestiones pre contractuales y contractuales; suministro de información en procesos de auditoría interna y externa que se realicen al interior de la institución; envío de información de los productos, servicios o novedades de la fundación; rastreo en bases de datos restrictivas tales como (policía, procuraduría, contraloría, SARLAFT – Sistema de Administración de Riesgo de Lavado de Activos y Financiación del Terrorismo y las demás que la normatividad colombiana disponga) las anteriores finalidades son enunciativas y no taxativas.

Video y Vigilancia

Los datos serán utilizados con las siguientes finalidades: monitoreo y control para la vigilancia de entrada, salida y tráfico de personas dentro de la compañía, así como para el control de ingreso y salida de vehículos de los parqueaderos; monitoreo de incidentes, medida de disuasión de conductas irregulares de terceros, monitoreo y control de la prestación de los servicios institucionales; Se realizará el envío de la información otorgada y autorizada por el titular las entidades con las cuales se tienen convenios, estas transferencias estarán siempre mediadas por un documento que garantice que el tratamiento que se le dará a sus datos será el mandado por la normatividad vigente. Las anteriores finalidades son enunciativas y no taxativas.

Visitantes

Los datos se utilizarán con estas finalidades. Identificar los datos personales del visitante que ingresa a las instalaciones de la empresa, Autorizar la entrada a las diferentes áreas o dependencias, envío de información en mensajes de texto y correos electrónico con motivos

promocionales y/o informativos; Se realizará el envío de la información otorgada y autorizada por el titular las entidades con las cuales se tienen convenios, estas transferencias estarán siempre mediadas por un documento que garantice que el tratamiento que se le dará a sus datos será el mandado por la normatividad vigente. Las anteriores finalidades son enunciativas y no taxativas.

7.1 Atención a los titulares de datos.

La señora María Duque, será la encargada de la atención de peticiones, consultas y reclamos ante la cual el titular de los datos puede ejercer sus derechos, en el siguiente Correo electrónico: maria.duque@endress.com.

8. PROCEDIMIENTOS PARA EJERCER LOS DERECHOS DEL TITULAR.

8.1 Derecho de acceso o consulta.

Según el capítulo 25 sección 4 del decreto 1074 de 2015, el Titular podrá consultar de forma gratuita sus datos personales en dos casos:

- Al menos una vez cada mes calendario.
- Cada vez que existan modificaciones sustanciales de las políticas de tratamiento de la información que motiven nuevas consultas.
- Para consultas cuya periodicidad sea mayor a una por cada mes calendario, la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S., solamente podrá cobrar al Titular gastos de envío, reproducción y, en su caso, certificación de documentos. Los costos de reproducción no podrán ser mayores a los costos de recuperación del material correspondiente. Para tal efecto, el responsable deberá demostrar a la Superintendencia de Industria y Comercio, cuando ésta así lo requiera, el soporte de dichos gastos.
- El Titular de los datos puede ejercitar el derecho de acceso o consulta de sus datos mediante un escrito dirigido a la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S., enviado mediante correo electrónico maria.duque@endress.com, indicando en el asunto “ejercicio del derecho de acceso o consulta” la solicitud deberá contener los siguientes datos:
- Nombre y apellidos del Titular.
- Fotocopia de la Cédula de Ciudadanía del Titular y, en su caso, de la persona que lo representa, así como del documento acreditativo de tal representación.
- Petición en que se concreta la solicitud de acceso o consulta.
- Dirección para notificaciones, fecha y firma del solicitante.
- Documentos acreditativos de la petición formulada, cuando corresponda.

- El Titular podrá elegir una de las siguientes formas de consulta de la base de datos para recibir la información solicitada:
    - Visualización en pantalla.
    - Por escrito, con copia o fotocopia remitida por correo certificado o no.
    - Correo u otros medios electrónicos.
- Otro sistema adecuado a la configuración de la base de datos o a la naturaleza del tratamiento, ofrecido por la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S.

Una vez recibida la solicitud, la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S., resolverá la petición de consulta en un plazo máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término. Estos plazos están fijados en el artículo 14 de la LEPD.

Una vez agotado el trámite de consulta, el Titular o causahabiente podrá elevar queja ante la Superintendencia de Industria y Comercio.

8.2 Derechos de quejas y reclamos.

El Titular de los datos puede ejercitar los derechos de reclamo sobre sus datos mediante un escrito dirigido a la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S. enviado, mediante correo electrónico a maria.duque@endress.com indicando en el asunto “ejercicio del derecho queja o reclamo”, la solicitud deberá contener los siguientes datos:

Nombre y apellidos del Titular.

- Fotocopia de la Cédula de Ciudadanía del Titular y, en su caso, de la persona que lo representa, así como del documento acreditativo de tal representación.
- Descripción de los hechos y petición en que se concreta la solicitud de corrección, supresión, revocación o inflación.
- Dirección para notificaciones, fecha y firma del solicitante.
- Documentos acreditativos de la petición formulada que se quieran hacer valer, cuando corresponda.

Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga “reclamo en trámite” y el motivo del mismo, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido. La sociedad

ENDRESS+HAUSER (COLOMBIA) S.A.S., resolverá la petición de consulta en un plazo máximo de quince (15) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no se pueda atender al reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, que no podrá superar los ocho días hábiles siguientes al vencimiento del primer término. Una vez agotado el trámite de reclamo, el Titular o causahabiente podrá elevar queja ante la Superintendencia de Industria y Comercio.

9. MEDIDAS DE SEGURIDAD

La sociedad ENDRESS+HAUSER (COLOMBIA) 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, la sociedad ENDRESS+HAUSER (COLOMBIA) 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 la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S., que están recogidas y desarrolladas en este documento (Tablas II, III, IV y V).

TABLA II. MEDIDAS DE SEGURIDAD COMUNES PARA TODO TIPO DE DATOS (PÚBLICOS, SEMIPRIVADOS, PRIVADOS, SENSIBLES) Y BASES DE DATOS (AUTOMATIZADAS, NO AUTOMATIZADAS)

Auditoria

- Auditoría ordinaria (interna o externa) cada año.
- Eventuales Auditorías extraordinaria por modificaciones sustanciales en los sistemas de información.
- Informe de detección de deficiencias y propuesta de correcciones.
- Análisis y conclusiones del responsable de seguridad y del responsable del tratamiento.

- Conservación del Informe a disposición de la autoridad.

Gestión de documentos y soportes.

- Medidas como, destructora de papel que eviten el acceso indebido o la recuperación de los datos descartados, borrados o destruidos.
- Acceso restringido al lugar donde se almacenan los datos.
- Sistema de etiquetado o identificación del tipo de información.
- Inventario de los soportes en los que se almacenan bases de datos.
- Autorización del responsable para la salida de documentos o soportes por medio físico o electrónico.

Control de acceso

- Acceso de usuarios limitado a los datos necesarios para el desarrollo de sus funciones, de acuerdo con el rol que desempeña.
- Lista actualizada de usuarios y accesos autorizados.
- Autorización escrita del titular de la información para la entrega de sus datos a terceras personas, para evitar el acceso a datos con derechos distintos de los autorizados.
- Concesión, alteración o anulación de permisos por el personal autorizado.

Incidencias

- Registro de incidencias: tipo de incidencia, momento en que se ha producido, emisor de la notificación, receptor de la notificación, efectos y medidas correctoras.
- Procedimiento de notificación y gestión de incidencias.

Personal

- Definición de las funciones y obligaciones de los usuarios con acceso a los datos.
- Definición de las funciones de control y autorizaciones delegadas por el responsable del tratamiento.
- Divulgación entre el personal de las normas y de las consecuencias del incumplimiento de estas.

Políticas y Procedimientos

- Elaboración e implementación de la política de obligatorio cumplimiento para el personal.

- Contenido mínimo: ámbito de aplicación, medidas y procedimientos de seguridad, funciones y obligaciones del personal, descripción de las bases de datos, procedimiento ante incidencias, procedimiento de copias y recuperación de datos, medidas de seguridad para el transporte, destrucción y reutilización de documentos, identificación de los encargados del tratamiento.

TABLA III. MEDIDAS DE SEGURIDAD COMUNES PARA TODO TIPO DE DATOS (PÚBLICOS, SEMIPRIVADOS, PRIVADOS, SENSIBLES) SEGÚN EL TIPO DE BASES DE DATOS

BASES DE DATOS NO AUTOMATIZADAS

Archivo

Archivo de documentación siguiendo procedimientos que garanticen una correcta conservación, localización y consulta y ejercicio de los derechos de los Titulares.

Almacenamiento de documentos.

Dispositivos de almacenamiento con mecanismos que impidan el acceso a personas no autorizadas.

Custodia de documentos

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, caducidad y almacenamiento cifrado.

Telecomunicaciones

Acceso a datos mediante redes seguras.

TABLA IV. MEDIDAS DE SEGURIDAD PARA DATOS PRIVADOS SEGÚN EL TIPO DE BASES DE DATOS

BASES DE DATOS AUTOMATIZADAS Y NO AUTOMATIZADAS

Auditoría

- Auditoría ordinaria (interna o externa) cada año.
- Eventuales Auditorías extraordinaria por modificaciones sustanciales en los sistemas de información.
- Informe de detección de deficiencias y propuesta de correcciones.
- Análisis y conclusiones del responsable de seguridad y del responsable del tratamiento.
- Conservación del Informe a disposición de la autoridad.

Responsable de seguridad

- Designación de uno o varios responsables de seguridad.
- Designación de uno o varios encargados del control y la coordinación de las medidas del políticas y procedimientos.
- Prohibición de delegación de la responsabilidad del responsable del tratamiento en el responsable de seguridad.

Políticas y Procedimientos Habeas Data

- Controles al menos una vez al año de cumplimiento, consistente en la auditoria anual, así como la capacitación al personal mínimo una vez al año.

BASES DE DATOS AUTOMATIZADAS

Gestión de documentos y soportes

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

Control de acceso al lugar o lugares donde se ubican los sistemas de información.

Identificación y autenticación Mecanismo
que limite el número de intentos reiterados de acceso no autorizados.

Incidencias

Registro de los procedimientos de recuperación de los datos, persona que los ejecuta, datos restaurados y datos grabados manualmente.

Autorización del responsable del tratamiento para la ejecución de los procedimientos de recuperación.

TABLA V. MEDIDAS DE SEGURIDAD PARA DATOS SENSIBLES SEGÚN EL TIPO DE BASES DE DATOS

BASES DE DATOS NO AUTOMATIZADAS

Control de acceso

- Acceso solo para personal autorizado.
- Mecanismo de identificación de acceso.
- Registro de accesos de usuarios no autorizados.

Almacenamiento de documentos

- Archivadores, armarios u otros ubicados en áreas de acceso protegidas con llaves u otras medidas.

Copia o reproducción

- Solo por usuarios autorizados. - Destrucción que impida el acceso o recuperación de los datos.

Traslado de documentación

- Medidas que impidan el acceso o manipulación de documentos

BASES DE DATOS AUTOMATIZADAS

Gestión de documentos y soportes

- Sistema de etiquetado confidencial.

- Cifrado de datos.
- Cifrado de dispositivos portátiles cuando sean retirados.

Control de acceso

- Registro de accesos: usuario, hora, base de datos a la que accede, tipo de acceso, registro al que accede.
- Control del registro de accesos por el responsable de seguridad. Informe mensual.
- Conservación de los datos: por el periodo que las leyes impongan.

Telecomunicaciones

- Transmisión de datos mediante redes electrónicas cifradas.

9.1 Encargados de seguridad.

Los encargados de seguridad tienen las siguientes funciones:

Coordinar y controlar la implantación de las medidas de seguridad y colaborar con el responsable del tratamiento en la difusión de Políticas y Procedimientos Habeas Data.

Coordinar y controlar los mecanismos que permiten acceder a la información contenida en las bases de datos y elaborar un informe periódico sobre dicho control.

Gestionar los permisos de acceso a los datos por parte de los usuarios autorizados identificados en esta política.

Habilitar el registro de incidencias a todos los usuarios para que comuniquen y registren las incidencias relacionadas con la seguridad de los datos; así como acordar con el responsable del tratamiento las medidas correctoras y registrarlas.

Comprobar periódicamente, 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, la actualización en esta política y el cumplimiento de las medidas relacionadas con las entradas y salidas de datos.

Definir los tiempos en que se realizarán las auditorias, que NO podrán superar un año.

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

Gestionar y controlar los registros de entradas y salidas de documentos o soportes que contengan datos personales.

9.2 Usuarios.

Todas las personas que intervienen en el almacenamiento, tratamiento, consulta o cualquier otra actividad relacionada con los datos personales y sistemas de información de la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S., deben actuar de conformidad a las funciones y obligaciones recogidas en el presente apartado.

La sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S., cumple con el deber de información con su inclusión de acuerdos de confidencialidad y deber de secreto que suscriben, en su caso, los usuarios de sistemas de identificación sobre bases de datos y sistemas de información, y mediante una circular informativa dirigida a los mismos.

Las funciones y obligaciones del personal de la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S. Se definen según el tipo de actividad que desarrollan según sus funciones dentro de la institución y, específicamente, por el contenido de esta política. La lista de usuarios y perfiles con acceso a los recursos protegidos están recogidos en este documento.

Cuando un usuario trate documentos o soportes con datos personales debe custodiarlos y vigilar y controlar que personas no autorizadas no puedan acceder a ellos.

El incumplimiento de las obligaciones y medidas de seguridad establecidas Política de Habeas Data. por parte del personal al servicio de la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S., es sancionable según la normativa aplicable a la relación jurídica entre el usuario y la organización.

Las funciones y obligaciones de los usuarios de las bases de datos personales bajo responsabilidad de la sociedad ENDRESS+HAUSER (COLOMBIA) 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 la sociedad ENDRESS+HAUSER (COLOMBIA) 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: El responsable del tratamiento 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 al responsable de seguridad correspondiente que podrá 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 estos.

Obligación de notificar incidencias: Los usuarios tienen la obligación de notificar las incidencias de las que tenga conocimiento al responsable de seguridad que corresponda, quien se encargará de su gestión y resolución. Algunos ejemplos de incidencias son: la caída del sistema de seguridad informática 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, etc.

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. Cuando la información esté clasificada con nivel de seguridad sensible el sistema de etiquetado solo debe ser comprensible para los usuarios autorizados a acceder a dicha información.

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.

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 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 institución.

Deber de archivo y gestión de documentos y soportes: Los documentos y soportes deben de ser debidamente archivados con las medidas de seguridad recogidas en esta política.

10. TRANSFERENCIA DE DATOS A TERCEROS PAÍSES.

De acuerdo con el Título VIII de la LEPD, se prohíbe la transferencia de datos personales a países que no proporcionen niveles adecuados de protección de datos. Un país ofrece un nivel adecuado de protección de datos si cumple con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia según la circular 005 de 10 de agosto de 2017, que no podrán ser inferiores a los exigidos por esta ley. Esta prohibición no regirá cuando se trate de:

- Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia.
- Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del Titular por razones de salud o higiene pública.
- Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable.
- Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad.
- Transferencias necesarias para la ejecución de un contrato entre el Titular y el responsable del tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular.
- Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

En los casos no contemplados como excepción, corresponderá a la Superintendencia de Industria y Comercio proferir la declaración de conformidad relativa a la transferencia internacional de datos personales. El Superintendente está facultado para requerir

información y adelantar las diligencias tendentes a establecer el cumplimiento de los presupuestos que requiere la viabilidad de la operación.

Las transmisiones internacionales de datos personales que se efectúen entre un responsable y un encargado para permitir que el encargado realice el tratamiento por cuenta del responsable, no requerirán ser informadas al Titular ni contar con su consentimiento, siempre que exista un contrato de transmisión de datos personales.

CAPITULO II
DE LAS MEDIDAS DE SEGURIDAD

1. CUMPLIMIENTO Y ACTUALIZACIÓN.

Este es un documento interno de obligatorio cumplimiento para todo el personal de la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S., con acceso a los sistemas de información que contengan datos personales.

Esta política y Procedimientos Habeas Data, debe ser sometido a permanente revisión y actualización siempre 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. El documento debe adaptarse siempre a la normativa legal sobre seguridad de datos personales.

2. MEDIDAS DE SEGURIDAD.

Las bases de datos son accesibles únicamente por las personas designadas por la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S., y referidas en el numeral 12 de este documento.

Los responsables de seguridad de la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S., señalados en el numeral 12 del presente documento, se encargan de gestionar los permisos de acceso a los usuarios, el procedimiento de asignación y distribución que garantiza la confidencialidad, integridad y almacenamiento de las contraseñas, durante su vigencia, así como la periodicidad con la que se cambian.

A continuación, se enumeran y detallan las medidas de seguridad implementadas por la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S.

2.1 Medidas de seguridad comunes.

2.1.1 Gestión de documentos y soportes.

Los documentos y soportes en los que se encuentran las bases de datos se determinan en el inventario de documentos y soportes.

Los encargados de vigilar y controlar que personas no autorizadas no puedan acceder a los documentos y soportes con datos personales son los usuarios autorizados para acceder a estos. Los usuarios autorizados están referidos en el numeral 12 sobre bases de datos y sistemas de información del presente documento.

Los documentos y soportes deben clasificar los datos según el tipo de 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 registro de entrada y de salida de documentos y en este documento.

La identificación de los documentos y soportes de 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.

La salida de documentos y soportes que contengan datos personales fuera de los locales que están bajo el control del responsable del tratamiento debe ser autorizada por este último. Este precepto también es aplicable a los documentos o soportes anexados y enviados por correo electrónico.

El inventario de documentos y soportes de la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S. debe incluirse como anexo del presente documento.

3. CONTROL DE ACCESO.

El personal de la sociedad ENDRESS+HAUSER (COLOMBIA) 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 del tratamiento en esta política.

La sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S. almacena una lista actualizada de usuarios, perfiles de usuarios y de los accesos autorizados para cada uno. Además, tiene mecanismos para evitar el acceso a datos con derechos distintos de los autorizados. En el caso de soportes informáticos, puede consistir en la asignación de 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.

La modificación sobre datos, así como la concesión, alteración, inclusión o anulación de los accesos autorizados y de los usuarios recogidos en la lista actualizada mencionada en el párrafo anterior, corresponde exclusiva al personal autorizado.

Todo personal ajeno a la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S., que acceda a los recursos protegidos, estará sometido a las mismas condiciones y tendrá las mismas obligaciones de seguridad que el personal propio.

Los usuarios autorizados para el acceso a las bases de datos se establecen en el numeral 6 de este documento.

3.1 Ejecución del tratamiento fuera de la institución.

El almacenamiento de datos personales del responsable del tratamiento en dispositivos portátiles y su tratamiento fuera del lugar natural de trabajo requiere autorización previa de la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S., y el cumplimiento de las garantías de seguridad correspondientes al tratamiento de estos datos.

3.2 Bases de datos temporales, copias y reproducciones.

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. Cuando dejan de ser necesarias, estas bases de datos temporales o copias se borran o destruyen, impidiéndose el acceso o recuperación de la información que contienen.

Solamente el personal autorizado en el numeral 12 puede realizar copias o reproducir los documentos.

3.3 Responsable de seguridad.

De acuerdo con la normativa sobre protección de datos, la designación de los responsables de seguridad no exonera de responsabilidad al responsable del tratamiento o encargado del tratamiento.

4. AUDITORÍA.

Las bases de datos que contengan datos personales, objeto de tratamiento por la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S., clasificadas con nivel de seguridad sensible o privado, se han de someter, a una auditoria cada año, esta puede ser una auditoría interna o externa que verifique el cumplimiento de las medidas de seguridad contenidas en esta política.

Serán objeto de auditoría tanto los sistemas de información como las instalaciones de almacenamiento y tratamiento de datos.

La sociedad ENDRESS+HAUSER (COLOMBIA) 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 encontradas 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 responsable de seguridad que corresponda estudiará el informe y trasladará las conclusiones al responsable del tratamiento para que implemente las medidas correctoras. Los informes de auditoría serán adjuntados a este documento y quedarán a disposición de la Autoridad de Control.

5. MEDIDAS DE SEGURIDAD PARA BASES DE DATOS NO AUTOMATIZADAS.

5.1 Archivo de documentos.

La sociedad ENDRESS+HAUSER (COLOMBIA) 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 numeral 12 de este documento.

Se recomienda archivar los documentos considerando, entre otros, criterios como el uso de los usuarios con acceso autorizado, la actualidad de su gestión y/o tratamiento y la diferenciación entre bases de datos históricas y de administración o gestión de la institución.

Los dispositivos de almacenamiento de documentos deben disponer de llaves u otros mecanismos que dificulte su apertura, excepto cuando las características físicas de éstos lo impidan, en cuyo caso, la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S., adoptará las medidas necesarias para impedir el acceso de personas no autorizadas.

Los dispositivos se identifican y describen en el numeral 12 de la presente política.

Cuando los documentos con datos personales estén en revisión o tramitación y, por tanto, fuera de los dispositivos de almacenamiento, ya sea antes o después de su archivo, la persona responsable debe custodiarlos e impedir que personas no autorizadas puedan acceder a ellos.

Los dispositivos de almacenamiento que contengan documentos con datos personales clasificados con nivel de seguridad sensible deben encontrarse en áreas o locales 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 se precise el acceso a dichos documentos. Si no fuera posible cumplir con lo anterior, la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S., podrá adoptar medidas alternativas debidamente motivadas que se incluirán en el presente documento.

La descripción de las medidas de seguridad de almacenamiento de encuentran recogidas en el numeral 6-7 de este documento.

6. ACCESO A LOS DOCUMENTOS.

El acceso a los documentos ha de realizarse exclusivamente por el personal autorizado en el numeral 12 de la presente política, siguiendo los mecanismos y procedimientos definidos. Estos últimos deben identificar y conservar los accesos realizados a la documentación clasificada con nivel de seguridad sensible, tanto por usuarios autorizados como por personas no autorizadas tal y como se refleja en el numeral referido anteriormente.

El procedimiento de acceso a los documentos que contienen datos clasificados como sensibles 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 seguridad en cuestión de la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S.

7. MEDIDAS DE SEGURIDAD PARA BASES DE DATOS AUTOMATIZADAS.

7.1 Identificación y autenticación.

La sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S., debe instalar un sistema de seguridad informática que permita identificar y autenticar de forma correcta a los usuarios de los sistemas de información, con el fin de garantizar que solo el personal autorizado pueda acceder a las bases de datos.

También ha de establecer un mecanismo que permita la identificación personalizada e inequívoca de todo usuario que intente acceder al sistema de información y que verifique si está autorizado. La identificación se debe hacer mediante un sistema único para cada usuario que accede a la información considerando el nombre de usuario, el de empleado, el del departamento, etc. La nomenclatura utilizada para asignar nombres de usuario para acceder al sistema de información y el sistema de autenticación de usuarios se recogen en el numeral 12 de este documento.

Cuando el sistema de autenticación esté basado en la introducción de contraseña, se ha de implantar un procedimiento de asignación, distribución y almacenamiento de contraseñas; para garantizar la integridad y confidencialidad de estas últimas, se recomiendan que tengan un mínimo de ocho caracteres y contengan mayúsculas, minúsculas, números y letras. La política de contraseñas de la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S. se encuentra en el numeral 12 del presente documento.

Por otra parte, la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S. debe vigilar que las contraseñas se cambien de forma periódica, nunca por un tiempo superior a 365 días. El periodo de vigencia de las contraseñas se recoge en el ya referido numeral 12.

La sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S., también garantiza el almacenamiento automatizado, interno y cifrado, de las contraseñas mientras estén vigentes, y adoptará un mecanismo para limitar los intentos reiterados de accesos no autorizados, también detallado en el numeral 12 del documento.

8. 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 el nivel de seguridad, 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.

El sistema de registro de entrada y salida debe anexarse en este documento.

Las instalaciones de la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S. son sede de los sistemas de información con datos personales, deben protegerse para garantizar la integridad y confidencialidad de dichos datos; además, deben cumplir con las medidas de

seguridad físicas correspondientes al documento donde incluyen los datos.

sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S., debe conocer a su personal las obligaciones que les competen para proteger físicamente los documentos o soportes de las bases de datos, no permitiendo su manejo, utilización o identificación por personas no autorizadas en este documento. Los locales e instalaciones donde se ubican las bases de datos, especificando sus características físicas y las medidas de seguridad física existentes se señalan en el numeral 12 del presente documento.

Solo el personal autorizado puede acceder a los lugares donde estén instalados los equipos que dan soporte a los sistemas de información, según lo dispuesto en numeral antes referido.

9. COPIAS DE RESPALDO Y RECUPERACIÓN DE DATOS.

La sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S., ha realizado los procedimientos de actuación necesarios para hacer copias de respaldo, al menos una vez a la semana, excepto cuando no se haya actualizado los datos en ese periodo. Todas las bases de datos deben tener una copia de respaldo a partir de las cuales se puedan recuperar los datos.

De igual modo, ha establecido procedimientos para la recuperación de los datos con el objetivo de garantizar en todo momento la reconstrucción al estado en el que éstos se encontraban antes de su pérdida o destrucción. Cuando la pérdida o destrucción afecte a bases de datos parcialmente automatizadas se grabarán manualmente los datos dejando constancia de ello en este documento.

La sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S., se encargará de controlar el correcto funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y recuperación de los datos cada 6 meses.

Los procedimientos de copia y respaldo se recogen en numeral 12 de este documento.

La sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S., debe conservar respaldo de los datos y de los procedimientos de recuperación de estos en un lugar distinto al donde se encuentren los equipos donde se trate. Este lugar deberá cumplir en todo caso las mismas medidas de seguridad exigidas para los datos originales.

10. REGISTRO DE ACCESO.

De los intentos de acceso a los sistemas de información de la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S., deberá 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. Si el registro se autoriza, se guarda la información que permita identificar el registro consultado.

Los responsables de seguridad de las bases de datos automatizadas se encargan 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. 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 el responsable del tratamiento sea una persona natural y garantice que solamente él tiene acceso y trata los datos personales. Estas circunstancias deben constar expresamente en este documento.

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.

La transmisión de datos personales mediante redes públicas o inalámbricas de comunicaciones electrónicas se tiene que llevar a cabo cifrando dichos datos, o utilizando otro mecanismo similar que garantice que la información no sea inteligible ni manipulada por terceras personas.

11. FUNCIONES Y OBLIGACIONES DEL PERSONAL.

Quienes intervienen en el almacenamiento, tratamiento, consulta o cualquier otra actividad relacionada con los datos personales y sistemas de información de, deben actuar de conformidad con las funciones y obligaciones recogidas en este apartado.

La sociedad ENDRESS+HAUSER (COLOMBIA) 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, tablón 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.

La sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S., cumple con el deber de información con su inclusión de acuerdos de confidencialidad y deber de secreto que suscriben, en su caso, los usuarios de sistemas de identificación referidos en el numeral 12 sobre bases de datos y sistemas de información, y mediante una circular informativa dirigida a los mismos.

Las funciones y obligaciones del personal de la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S. se definen, según el tipo de actividad que desarrollan en la institución, específicamente, por el contenido de este documento. La lista de usuarios y perfiles con acceso a los recursos protegidos están recogidos en el numeral 12 sobre bases de datos y sistemas de información. Cuando un usuario trate documentos o soportes con datos personales debe custodiarlos y vigilar y controlar que personas no autorizadas no puedan acceder a ellos.

El incumplimiento de las obligaciones y medidas de seguridad establecidas en esta política por parte del personal al servicio de la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S. es sancionable según la normativa aplicable a la relación jurídica entre las partes.

Las funciones y obligaciones de los usuarios de las bases de datos personales bajo responsabilidad de la sociedad ENDRESS+HAUSER (COLOMBIA) 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 la organización 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 estos.

Funciones de control y autorizaciones delegadas: El responsable del tratamiento puede delegar el tratamiento de datos a terceros, para que actúe como encargado del tratamiento, mediante un contrato de transmisión de datos. Cuando se firmen contratos de transmisión de datos, estos se anexarán en el presente documento.

- Las obligaciones relacionadas con las medidas de seguridad implantadas
- Acceder a las bases de datos solo con la autorización y cuando sea necesario para ejercer 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 seguridad 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 estos.
- Obligación de notificar incidencias: Los usuarios tienen la obligación de notificar las incidencias de las que tenga conocimiento a los responsables de seguridad, quienes se encargarán de su gestión y resolución. Algunos ejemplos de incidencias son: la caída del sistema de seguridad informática 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 pérfida 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, etc.
- 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. Cuando la información esté clasificada con nivel de seguridad sensible el sistema de etiquetado solo debe ser comprensible para los usuarios autorizados a acceder a dicha información.
- 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. Los ordenadores portátiles deben controlarse siempre para evitar su pérdida o sustracción.

Uso limitado de Internet y correo electrónico: El envío de información por vía electrónica y el personal de Internet se limita al desempeño de sus actividades al interior de la sociedad ENDRESS+HAUSER (COLOMBIA) 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 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 propiedad de la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S.
- Deber de archivo y gestión de documentos y soportes: Los documentos y soportes deben archivarse con las medidas de seguridad establecidas en este capítulo.

12. BASES DE DATOS Y SISTEMAS DE INFORMACIÓN.

Las bases de datos almacenadas y tratadas por la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S. se recogen en la siguiente tabla (Tabla I), donde se indica el nivel de seguridad y el sistema de tratamiento de cada una de ellas.

Tabla I. Bases de datos y nivel de seguridad

Bases de datos	Nivel de seguridad
Empleados	Alto
Proveedores nacionales y extranjeros	Básico
Clientes nacionales y extranjeros	Básico
Video y vigilancia	Alto
Visitantes	Básico

La siguiente tabla (Tabla II) recoge la estructura de las bases de datos de la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S.

Tabla II. Estructura de las Bases de datos

Nombre de la base de datos	Empleados
Responsable del tratamiento	La sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S. NIT: 900.896.981-1 Dirección: CR 17 93 09 OF 201 Teléfono: 3188133205 Correo electrónico: maria.duque@endress.com

Encargado de consultas y reclamos	María Duque
Tipo de datos	Sensibles
Control de acceso físico	Usuarios autorizados
Control de acceso lógico	Usuarios y contraseñas
Copias de respaldo	Diario

Nombre de la base de datos	**Proveedores nacionales y extranjeros**
Responsable del tratamiento	La sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S. NIT: 900.896.981-1 Dirección: CR 17 93 09 OF 201 Teléfono: 3188133205 Correo electrónico: maria.duque@endress.com
Encargado de consultas y reclamos	María Duque
Tipo de datos	Básicos
Control de acceso físico	Usuarios autorizados
Control de acceso lógico	Usuarios y contraseñas
Copias de respaldo	Diario

Nombre de la base de datos	**Clientes nacionales y extranjeros**
Responsable del tratamiento	La sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S. NIT: 900.896.981-1 Dirección: CR 17 93 09 OF 201 Teléfono: 3188133205 Correo electrónico: maria.duque@endress.com
Encargado de consultas y reclamos	María Duque
Tipo de datos	Básicos
Control de acceso físico	Usuarios autorizados
Control de acceso lógico	Usuarios y contraseñas
Copias de respaldo	Diario

Nombre de la base de datos	Video y vigilancia
Responsable del tratamiento	La sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S. NIT: 900.896.981-1 Dirección: CR 17 93 09 OF 201 Teléfono: 3188133205 Correo electrónico: maria.duque@endress.com
Encargado de consultas y reclamos	María Duque
Tipo de datos	Sensibles
Control de acceso físico	Usuarios autorizados
Control de acceso lógico	Usuarios y contraseñas
Copias de respaldo	Diario

Nombre de la base de datos	Visitantes
Responsable del tratamiento	La sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S. NIT: 900.896.981-1 Dirección: CR 17 93 09 OF 201 Teléfono: 3188133205 Correo electrónico: maria.duque@endress.com
Encargado de consultas y reclamos	María Duque
Tipo de datos	Básicos
Control de acceso físico	Usuarios autorizados
Control de acceso lógico	Usuarios y contraseñas
Copias de respaldo	Diario

El nombramiento de los responsables de seguridad no exonera al responsable del tratamiento o encargado del tratamiento de sus obligaciones.

La sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S., identifica en este documento, a los encargados del tratamiento, así como las condiciones del encargo. 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.

12.1 PROCEDIMIENTO DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE INCIDENCIAS

La sociedad ENDRESS+HAUSER (COLOMBIA) 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.

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

Cuando una persona tenga conocimiento de una incidencia que afecte o pueda afectar la confidencialidad, disponibilidad e integridad de la información protegida de la institución deberá comunicarlo, de manera inmediata, a los responsables de seguridad, 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.

Tras comunicar la incidencia, se debe solicitar al responsable de seguridad correspondiente un acuse de recibo donde conste la notificación de la misma con todos los requisitos enumerados anteriormente.

La sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S., crea un registro de incidencias que debe contener: el tipo de incidencia, fecha y hora de esta, 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 responsable de seguridad de la base de datos y debe incluirse como anexo en el presente documento.

Asimismo, debe implementar los procedimientos para la recuperación de los datos, 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.

12.2 Reporte.

Todos los incidentes y eventos sospechosos deben reportarse lo antes posible a través de los canales internos establecidos por la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S. Si la información sensible o confidencial se pierde, se divulga a personal no autorizado o se sospecha de alguno de estos eventos, se debe notificar al responsable de la información de forma inmediata. Los funcionarios deben reportar a su jefe directo y/o al Oficial de Protección de Datos Personales cualquier daño o pérdida de computadores o cualquiera otro dispositivo, cuando estos contengan datos personales en poder de la Entidad. A menos que exista una solicitud de la autoridad competente debidamente razonada y justificada, ningún funcionario debe divulgar información sobre sistemas de cómputo, y redes que hayan sido afectadas por un delito informático o abuso de sistema. Para entregar información o datos según orden de autoridad, Oficina Asesora Jurídica deberá intervenir para dar el asesoramiento adecuado.

El responsable de la información debe garantizar que se tomen acciones para investigar y diagnosticar las causas del incidente y que el proceso de gestión del incidente sea documentado, apoyado con Oficina de Tecnologías e Informática.

13. CONTROL DE ACCESO Y VIDEO VIGILANCIA

Control acceso: Las áreas donde se ejecutan procesos relacionados con información confidencial o restringida deben contar con controles de acceso que sólo permitan el ingreso a los colaboradores autorizados y que permita guardar la trazabilidad de los ingresos y salidas.

Video Vigilancia: La Entidad cuenta con cámaras de video vigilancia que tienen como finalidad dar cumplimiento a las políticas de seguridad física, cumpliendo con los parámetros establecidos en la Guía para la Protección de Datos Personales en Sistemas de Videovigilancia, expedidos por la SIC como autoridad de control. Las imágenes deberán ser conservadas por un tiempo máximo de 20 días. En caso de que la imagen respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.

14. 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.

Antes de iniciar la destrucción se realizará un acta o se llevará el registro en un libro o agenda, en dicha a notación se describirá el documento objeto de destrucción, la fecha, hora y firma de las dos personas que evidencian la destrucción.

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 en dispositivos portátiles deben estar cifrados cuando estén fuera de las instalaciones controladas por la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S. Cuando no sea posible el cifrado, se debe evitar el tratamiento de datos personales con este tipo de dispositivos; pero se podrá proceder al tratamiento cuando sea necesario, adoptando medidas de seguridad que tengan en cuenta los riesgos e incluyéndolas en este documento.

15. INFRACCIONES Y SANCIONES.

Según el Capítulo II de la Ley Estatutaria 1581 de 2012 de Protección de Datos, la Superintendencia de Industria y Comercio puede sancionar por incumplir la normativa sobre protección de datos al responsable o al encargado del tratamiento. Las posibles sanciones son:

Multas de carácter personal e institucional hasta por el equivalente a dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó.

Suspensión de las actividades relacionadas con el tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar.

Cierre temporal de las operaciones relacionadas con el tratamiento tras el término de suspensión sin adoptar los correctivos ordenados por la Superintendencia de Industria y Comercio.

Cierre inmediato y definitivo de la operación que involucre el tratamiento de datos sensibles.

16. VIGENCIA

Las bases de datos responsabilidad de la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S., se tratarán durante el tiempo razonable y necesario para la finalidad para la que se recaban los datos. Una vez cumplida la finalidad o finalidades del tratamiento, y sin perjuicio de normas legales que dispongan lo contrario. la sociedad ENDRESS+HAUSER (COLOMBIA) S.A.S. Procederá a la supresión de los datos personales en su posesión salvo que exista una obligación legal o contractual que requiera su conservación. Por todo ello, el presente documento entra en vigencia el 03/12/2024.

Nota: Este documento ha cambiado en su totalidad.

_____

Maria Duque Pulido
Controller
Endress+Hauser (Colombia) S.A.S.