POLITICA DE SEGURIDAD DE LA INFORMACIÓN Y PROTECCION DE DATOS PERSONALES

Bogotá, Carrera 15 No 76-60 oficina 402 edificio el Lago
Tel. 6085154 - 4601729, Cel. 3202359596
gerente@soluciones-humanas.com

TABLA DE CONTENIDO

1. INTRODUCCIÓN

SERVICIOS EN SOLUCIONES HUMANAS SAS identifica la información como un componente indispensable para la operación de la compañía, razón por la cual se debe establecer unas políticas que aseguren que la información es protegida de una manera adecuada independientemente de la forma en la que ésta sea manejada, procesada o almacenada.

Este documento describe las políticas y normas de seguridad de la información y protección de datos personales definidas por SERVICIOS EN SOLUCIONES HUMANAS SAS, que son de obligatorio cumplimiento por parte de sus proveedores y contratistas. Se constituyen como parte fundamental para la seguridad de la información y protección de datos personales de SERVICIOS EN SOLUCIONES HUMANAS SAS y se convierten en la base para la implantación de los controles, procedimientos y estándares. La Seguridad de la Información es una prioridad para SERVICIOS EN SOLUCIONES HUMANAS SAS y por tanto es responsabilidad de todos los colaboradores y proveedores por SERVICIOS EN SOLUCIONES HUMANAS SAS velar por que no se realicen actividades que contradigan la esencia y el espíritu de cada una de estas políticas.

La seguridad de la información es la protección de la información de manera preventiva contra las amenazas o riesgos existentes que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e Integridad de la misma.

1. OBJETIVO.

Establecer las políticas que regulan la seguridad de la información y datos personales de SOLUCIONES HUMANAS S.A.S y presentar en forma clara y coherente los elementos que conforman la política de seguridad.

2. ALCANCE.

Las políticas y normas de seguridad de la información y protección de datos personales cubren los aspectos administrativos y de control que deben ser cumplidos por proveedores y contratistas que trabajen o tengan relación con SERVICIOS EN SOLUCIONES HUMANAS SAS, y en relación con el adecuado nivel de acceso, uso, divulgación y conservación aplicables a los siguientes recursos informáticos:

Información: Es un activo de SERVICIOS EN SOLUCIONES HUMANAS SAS, que comprende información física, verbal, biométrica o electrónica (bases de datos, manuales, videos, grabaciones, correos electrónicos, imágenes, firmas y certificados digitales entre otros).
Software: Aplicaciones, herramientas de oficina y de desarrollo y utilitarios desarrollados, adquiridos y autorizados por SERVICIOS EN SOLUCIONES HUMANAS SAS.
Físicos y ambientales: Equipos Centrales de Cómputo, estaciones de trabajo fijas o móviles, impresoras y escáner, equipos de comunicaciones, medios magnéticos de almacenamiento externo, equipos para suministro de electricidad.
Servicios: Comunicaciones telefónicas, internet, correo electrónico.

3. DEFINICIONES.

Acceso Remoto: Acceso a redes informáticas desde una ubicación remota. Las conexiones de acceso remoto pueden originarse tanto desde la red propia de la empresa como de una ubicación remota que se encuentra por fuera de la red de la empresa. Las redes VPN constituyen un ejemplo de tecnologías de acceso remoto.

Acción correctiva: Remediación de los requisitos o acciones que dieron origen al establecimiento de no una conformidad, de tal forma que no se vuelva a presentar.

Acción preventiva: Disposición de operaciones que buscan de forma preliminar, que no se presente en su ejecución, desarrollo e implementación una no conformidad.

Acceso a la Información Pública Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).

Activo de Información: Cualquier componente (sea humano, tecnológico, software, etc.) que sustenta uno o más procesos de negocios de una unidad o área de negocio. En otras palabras, es todo aquello que tiene valor para la organización. En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Algoritmo de cifrado: También denominado "algoritmo criptográfico". Secuencia de instrucciones matemáticas usadas para transformar textos o datos no cifrados en textos o datos cifrados y viceversa. Consulte Criptografía sólida.

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000)

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Análisis de seguridad de la red: Proceso mediante el cual se buscan vulnerabilidades en los sistemas de una entidad de manera remota a través del uso de herramientas manuales o automatizadas. Análisis de seguridad que incluyen la exploración de sistemas internos y externos, así como la generación de informes sobre los servicios expuestos a la red. Los análisis pueden identificar vulnerabilidades en sistemas operativos, servicios y dispositivos que pudieran utilizar personas malintencionadas.

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)

Auditoría Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3). En el contexto del control de acceso, la autorización es el otorgamiento de derechos de acceso u otros derechos similares a un usuario, programa o proceso. La autorización define lo que un individuo o programa puede hacer después de un proceso de autenticación satisfactorio.

Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de tratamiento (Ley 1581 de 2012, art 3).

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009)

Confidencialidad: Propiedad que determina que la información no está disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Contraseña predeterminada: Contraseña de las cuentas de usuario, servicio o administración de sistemas predefinidas en un sistema, aplicación o dispositivo asociado con la cuenta predeterminada. Las contraseñas y cuentas predeterminadas son de dominio público y, en consecuencia, es fácil averiguarlas.

Control de acceso: Mecanismo que limita la disponibilidad de información o de los recursos necesarios para su procesamiento sólo a personas o aplicaciones autorizadas.

Control de cambios: Procesos y procedimientos para revisar, probar y aprobar cambios a los sistemas y el software en función del impacto que puedan tener antes de su implementación.

Cuentas predeterminadas: Cuenta de inicio de sesión que se encuentra predefinida en un sistema, aplicación o dispositivo que permite obtener acceso por primera vez al momento en que el sistema comienza a funcionar. El sistema también puede generar cuentas predeterminadas adicionales como parte del proceso de instalación.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos Personales Públicos: 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, 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. (Decreto 1377 de 2013, art 3)

Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)

Datos Personales Mixtos: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos Personales Sensibles: Se entiende por datos sensibles 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. (Decreto 1377 de 2013, art 3)

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

Encargado del Tratamiento de Datos: 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. (Ley 1581 de 2012, art 3)

Evaluación del riesgo Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

Evento de seguridad de la información Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la

seguridad. Una ocurrencia que una organización considera que posee implicaciones potenciales a la seguridad de un sistema o su entorno.

Gestión de incidentes de seguridad de la información Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Gestión del riesgo Actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.

Incidente de seguridad de la información Un evento o serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

Información Pública Reservada Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

Integridad Propiedad de salvaguardar la exactitud y estado completo de los activos.
Ley de Habeas Data: Se refiere a la Ley Estatutaria 1266 de 2008.

Mecanismos de protección de datos personales: Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

Plan de continuidad del negocio Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Plan de tratamiento de riesgos Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Registro Nacional de Bases de Datos: Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)

Responsabilidad Demostrada: Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

Responsable del Tratamiento de Datos: 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. (Ley 1581de 2012, art 3).

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

Riesgo residual: Nivel restante del riesgo después del tratamiento del riesgo.

Seguridad de la Información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además puede involucrar otras propiedades tales como, autenticidad, trazabilidad, no repudio y fiabilidad.

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Titulares de la información: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)

Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

Tratamiento del riesgo: Proceso de selección e implementación de medidas para modificar el riesgo.

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información un sistema de tratamiento de la información sea asociado de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

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

Valoración del riesgo: Proceso global de análisis y evaluación del riesgo.

4. DOCUMENTOS DE REFERENCIA.

- Ley 1581 de 2012
- ISO/IEC 27001:2013
- ISO/IEC 27002:2013

5. POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

En SERVICIOS EN SOLUCIONES HUMANAS SAS la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones, razón por la cual existe un compromiso expreso de protección como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad.

SERVICIOS EN SOLUCIONES HUMANAS SAS, los proveedores y colaboradores se comprometen a implementar y mantener como parte del desarrollo de su modelo de gestión de seguridad de la información, programas y planes de capacitación, entrenamiento y concientización en sus respectivas compañías, de manera que se minimice la ocurrencia y el impacto de incidentes de seguridad de la información.

SERVICIOS EN SOLUCIONES HUMANAS SAS ha establecido las siguientes Políticas Generales de Seguridad de la Información, las cuales representan su visión en cuanto a la protección de sus activos de Información:

SERVICIOS EN SOLUCIONES HUMANAS SAS, los proveedores y colaboradores implantarán controles para proteger la información contra violaciones de autenticidad, accesos no autorizados, la perdida de integridad y que garanticen la disponibilidad requerida por los clientes y usuarios de los servicios ofrecidos por la compañía.

Todos los proveedores y colaboradores serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido. Las violaciones a las Políticas y Controles de Seguridad de la Información serán reportadas, registradas y monitoreadas.

5.1SEGURIDAD EN LOS RECURSOS HUMANOS

5.1.1 Política de Seguridad para la Selección de los Recursos Humanos

Objetivo:

Establecer mecanismos que aseguren la comprensión de los derechos, deberes y las responsabilidades en relación a seguridad de la información y protección de datos personales asegurando que estos cuenten con las competencias necesarias en el momento de la contratación.

Directrices:

La selección del personal de SOLUCIONES HUMANAS S.A.S, se realizará por medio del PSRP-SI-001 PROCEDIMIENTO DE SELECCION Y RETIRO DE PERSONAL el cual incluye estudio de seguridad avanzado (Visita Domiciliaria. Poligrafía Pre empleo, Referenciación: Personal, laboral y Académica y Verificación bases de datos) y la comprobación de las competencias necesarias requeridas para el desempeño del cargo vacante, confirmando la veracidad de la información suministrada por el candidato, antes de su vinculación.

Por lo menos una vez al año se asegurará de que todo empleado que acceda a información y datos personales de SOLUCIONES HUMANAS S.A.S o de sus clientes, acepta el cumplimiento de las políticas de seguridad de la información, por medio de la firma del Anexo de seguridad de la información y acuerdo de confidencialidad y no divulgación de la información y datos personales, para el desarrollo de acuerdo a los roles y privilegios asignados.

Todo empleado debe asegurarse de leer, comprender y firmar cada uno de los acuerdos relacionados con las responsabilidades de seguridad de la información y datos personales para poder iniciar la relación contractual.

Cualquier incumplimiento a las Políticas de seguridad de información traerá consigo las consecuencias que apliquen según los acuerdos contractuales, reglamentos y otros de tipo disciplinario o Legal incluyendo lo establecido en las normas que competen al Gobierno Nacional en cuanto a Seguridad de la Información se refiere.

5.1.2 Política de Seguridad para la terminación o cambio de empleo.

Objetivo:

Establecer mecanismos que aseguren los deberes y las responsabilidades de empleados en relación a seguridad de información, los cuales permanecen válidos en el proceso de cambio o terminación del empleo en SOLUCIONES HUMANAS S.A.S.

Directrices:

En caso retiro del empleado o contratista se informará inmediatamente al Ingeniero de Sistemas para la desactivación de accesos lógicos y otros a los cuales tenga acceso. Por lo menos una vez al año se realizará la verificación del estado de los usuarios en los recursos tecnológicos o sistemas de información y el cumplimiento de las disposiciones.

Los acuerdos de confidencialidad y no divulgación de la información y datos personales, se mantienen vigentes inclusive una vez finalizada la relación contractual.

5.1.3 Política de toma de conciencia, educación y formación en Seguridad de la Información.

Objetivo:
Desarrollar la estrategia generar conciencia y compromiso frente a seguridad de la información y protección de datos personales y el cumplimiento de sus responsabilidades, para empleados y otras partes interesadas.

Directrices:
La Gerencia destinará los recursos suficientes para la ejecución de un Programa de Capacitación, para la sensibilización y toma de conciencia en SOLUCIONES HUMANAS S.A.S, sobre políticas, reglamentos, normas y procedimientos y las responsabilidades frente a seguridad de la información o cuando estos tengan actualizaciones de los empleados o terceros interesados, para lograr el entendimiento y toma de conciencia en seguridad de información, disminuir vulnerabilidades y amenazas relacionadas con el recurso humano.

5.2 GESTIÓN DE ACTIVOS

5.2.1 Política de Gestión de Activos.

Objetivo:
Establecer la forma como se mantiene el nivel de protección adecuada de los activos de información de acuerdo con su importancia en la Empresa.

Directrices:
SOLUCIONES HUMANAS S.A.S como propietario de la información, proveerá los recursos necesarios en la aplicación de controles para preservar la confidencialidad, la integridad y la disponibilidad. Será responsabilidad de cada empleado, los activos asociados a su proceso y su correcto uso en la empresa. El acceso a la información se verá reflejado en las Ficha Técnica de Acceso a la Información ubicadas de manera visible para todos los colaboradores.

Los activos de información serán identificados, clasificados y protegidos de acuerdo a su valor o la funcionalidad que cumple.

Para la clasificación y etiquetado de la información se realizará en cumplimiento con la Ficha Técnica de Clasificación de la Información descrita a continuación:

	FICHA TÉCNICA DE CLASIFICACIÓN DE LA INFORMACIÓN	Código: FCIA- SI-001
		Versión 2.0
		Página 1

Persona / Cargo	Información a la que puede acceder				
	1	2	3	4	5
Milena y Martha Coordinadoras	X	X	X	X	X
Adriana - Asistente		X		X	X
Jorge y Giselle - Psicólogos Planta		X		X	
Psicólogos - Freelance		X		X	
Aprendiz Mercadeo		X			
Asesores y Consultores Proveedores		X		X	

Niveles de acceso a la información					
Alto	1	2	3	4	5
Medio		2		4	
Bajo				4	

Tipos de Información			
Información Clasificada	1	3	
Información Confidencial	2	5	
Información de Uso Interno	4		

CÓD..	Información
1.	Carpetas de Proveedores y Empleados
2.	Hojas de Vida remitidas clientes, autorizaciones del personal remitido, visitas domiciliarias (hojas de vida reclutadas en los procesos de selección)
3.	Contabilidad, nomina, cuentas de cobro, impuestos, documentación tributaria, documentos de la empresa, propuestas, cotizaciones tablas de precios, control de clientes (documentos)
4.	Formatos de uso interno
5.	Estudios de seguridad, confiabilidad, socioeconómicos (consolidados) VETTING

Para los activos de información dispuestos de manera electrónica se contemplará el uso de los servicios de Cloud, o almacenamiento en la nube permitiendo únicamente almacenamiento en el sistema corporativo. Para realizar uso del almacenamiento Cloud se podrá verificar el Manual Cloud Servicios en Soluciones Humanas S.A.S.

5.2.2 Política de Uso aceptable de los activos.

Objetivo:
Establecer las Medidas de protección adecuada de los activos de información y los recursos tecnológicos, mediante la asignación a usuarios finales de acuerdo al desarrollo de funciones.

Directrices:
Todo empleado de SOLUCIONES HUMANAS S.A.S tendrá a su disposición el uso de activos de información y recursos tecnológicos que los contienen de acuerdo a las funciones laborales que así lo requieran y según las características definidas en el inventario de activos de Información.
Para su uso, acepta y se acoge a las Políticas de Seguridad de la Información y las disposiciones relacionadas a continuación:

Todo empleado usara cuentas de usuario para acceder a sistemas de información, aplicaciones y servicios la cual es de uso personal e intransferible. El empleado será responsable de todas las acciones o transacciones efectuadas con dicha cuenta de usuario.

Los empleados no podrán hacer uso de dispositivos personales, copiar, distribuir o cambiar las configuraciones de los recursos tecnológicos y deberán utilizar únicamente los programas y equipos autorizados por la empresa, quienes es la única autorizada para instalar o configurar software y equipos bajo licenciamiento legal. La descarga, instalación o uso de software ilegal o sin licenciar será considerada como una violación a las Políticas de Seguridad de la Información y datos personales de SOLUCIONES HUMANAS S.A.S.

El empleado no podrá hacer uso de estos recursos para transmitir, almacenar y/o procesar información que atente contra la propiedad intelectual, los derechos de autor o derechos de protección de datos personales.

Todo empleado deberá realizar la devolución de todos los activos de información físicos y electrónicos en el proceso de desvinculación por medio del ACTA DE ENTREGA DEL CARGO.

5.3 CONTROL DE ACCESO

5.3.1 Política de control de acceso a redes y servicios de red.

Objetivo:
Definir las pautas generales para un acceso controlado y seguro únicamente a los usuarios autorizados a la información a los servicios de procesamiento de información, equipos y demás activos propiedad de la empresa.

Directrices:
Solo se permitirá el acceso de los usuarios a la red y a los servicios de red a los equipos suministrados por SOLUCIONES HUMANAS S.A.S y únicamente a la información necesaria para los que haya sido autorizados para el desarrollo de sus funciones. No se permitirá el acceso de visitantes, cuando sea requerido trabajar con recursos compartidos, dicho recurso debe estar justificado y autorizado.

El acceso a la información y a los servicios de procesamiento de información de SERVICIOS EN SOLUCIONES HUMANAS SAS debe ser asignado de acuerdo a la identificación previa de requerimientos de seguridad y a los procesos del negocio.

Los privilegios asignados a los usuarios deben ser revisados mínimos dos veces al año por el proveedor encargado de la administración de TI, para garantizar que no se tengan privilegios no autorizados y estos se encuentren de acuerdo a las funciones de los cargos.
Para evitar el acceso de usuarios no autorizados, robo, perdida o puesta en peligro de la información y de los servicios de procesamiento de la información, se debe concienciar a los empleados sobre sus responsabilidades acorde con los siguientes lineamientos para el uso de contraseñas y a la seguridad del equipo del usuario.

5.5.2 Política de control de acceso a usuarios.

Objetivo:
Establecer los lineamientos para la administración, el acceso controlado y seguro únicamente a los usuarios autorizados.

Directrices:
SOLUCIONES HUMANAS S.A.S contará con un método de autenticación por medio de usuario y contraseña, el proveedor encargado de TI será responsable de la creación de acceso de usuarios utilizando identificadores de usuario únicos, que permita identificarlos por sus acciones evitando la existencia de múltiples perfiles de acceso.

Las contraseñas deben contener dígitos numéricos, letras mayúsculas y minúsculas y símbolos tales como !# ^ %&*()$_+|~=\`{}[]@:";'<>?,./. y La longitud de las contraseñas es de 8 caracteres como mínimo. En caso de que algún sistema no soporte el estándar definido de contraseñas, se deberá realizar sensibilización a los usuarios para que cumplan con dicho estándar.

La contraseña inicial emitida a un nuevo usuario o su restablecimiento, debe tener un valor único, secreto y entregada por el canal establecido, sólo debe ser válida para la primera sesión y posteriormente debe cambiarse al usarla por primera vez, bajo total responsabilidad de dicho usuario.

Para la transferencia de la información con terceros relacionada a estudios de seguridad VETTING (Socioeconómico y visita domiciliaria), pruebas de polígrafo, informes de evaluación se establecen medidas de acceso con contraseñas teniendo en cuenta: contraseña de acceso a los archivos especificadas de la siguiente manera:

-Código de estudio de seguridad + Inicial en mayúscula del nombre + Inicial en mayúscula del apellido. Ejemplo: (2205MC)

En el caso de retiro del empleado, el coordinador de selección y operaciones remitirá la solicitud al proveedor encargado de TI para inhabilitar la cuenta de usuario e indicará si se requiere generar copia de seguridad de la información del empleado.

En caso de ausencias temporales del empleado, debido a vacaciones o licencias que superen los 15 días hábiles, el coordinador de selección y operaciones informará inmediatamente al proveedor encargado de TI quien deberá inhabilitar las cuentas de usuario.

5.4 CUMPLIMIENTO

5.4.1 Política de Confidencialidad o de No divulgación

Objetivo:
Asegurar que se comunique las responsabilidades de los empleados para mantener la confidencialidad y no divulgación de la información de SOLUCIONES HUMANAS S.A.S o de sus Clientes.

Directrices:
Todos los proveedores y contratistas o colaboradores que tengan acceso a la información y o la procesen deben leer, entender, aceptar y generar un compromiso con el cumplimiento de las disposiciones contenidas en los acuerdos de confidencialidad y manejo de datos personales y sensibles definidos por la compañía, los cuales reflejan los compromisos de protección y buen uso de la información.
Para el caso de los proveedores, los respectivos contratos deben incluir una cláusula de confidencialidad y manejo de datos personales y sensibles, de igual manera cuando se permita el acceso a la información y/o a los recursos de SERVICIOS EN SOLUCIONES HUMANAS SAS a personas o entidades externas.
Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso de contratación, razón por la cual dichas cláusulas deben hacer parte integral de los acuerdos.
Todos los contratistas que tengan acceso a la información de SERVICIOS EN SOLUCIONES HUMANAS SAS, tienen estrictamente prohibido compartir dicha información con terceras partes sin contar con la aprobación previa y por escrito de SERVICIOS EN SOLUCIONES HUMANAS SAS, de

lo contrario puede incurrir en las sanciones y penas establecidas legalmente. Esta obligación prevalecerá aún después del vínculo contractual.

5.5 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

5.5.1 Política de Gestión de Incidentes y mejora en la seguridad de la información.

Objetivo:
Asegurar que los eventos o incidentes de seguridad que se presenten con los activos de información sean comunicados y atendidos oportunamente.

Directrices:
Todo empleado debe reportar en el menor tiempo posible eventos o incidentes que afecten a la seguridad, la confidencialidad o la disponibilidad de la información, así como la violación a las políticas de seguridad haciendo uso de los canales definidos para emprender las acciones previstas como lo son: correo electrónico, llamadas telefónicas a la gerencia directamente.

Se considera un incidente de Seguridad de la información, una posible violación a las políticas de seguridad de la información o fallas en los controles, la ocurrencia de un acto intencional o no intencional que se pueda considerar como un evento de seguridad y que comprometa la preservación de la confidencialidad, disponibilidad y/o integridad de la información.

Dependiendo del incidente de seguridad la empresa estará en capacidad de contratar a un tercero para realizar los procedimientos correspondientes para mitigar, o remediar los incidentes de la mejor y más rápida manera.

5.5.2 RIESGOS RELACIONADOS CON TERCEROS

Objetivo:
Establecer los lineamientos para asegurar la protección y el acceso controlado de los activos de información por parte de proveedores

Directrices:
Los proveedores y contratistas o colaboradores deben identificar los posibles riesgos que pueden generar el acceso, procesamiento, comunicación o gestión de la información y la infraestructura

para su procesamiento, en forma independiente y de acuerdo al servicio que se preste por parte de los proveedores con el fin de establecer los mecanismos de control necesarios para controlar la seguridad de la información.

Los controles que se establezcan como necesarios a partir del análisis de riesgos, deben ser comunicados y aceptados por los proveedores, previamente a la entrega de los accesos requeridos.

Los contratos que se firmen con contratistas, en los que se tiene acceso a recursos informáticos, deben hacer referencia expresa a la aceptación de las políticas de seguridad.

6. CONTROL DE CAMBIOS

Fecha	Versión	Revisión	Control de cambios
02/05/2018	1.0	Operaciones	Creación del documento
09/02/2019	2.0	Consultor SI	Modificación y agregación de políticas de seguridad, modificación de estructura del documento

7. TABLA DE APROBACIONES.

Elaboró	Revisó	Aprobó
Hernán Felipe Contreras **Consultor en Seguridad de la Información**	Milena Camacho Vargas **Coordinadora Selección y Operaciones**	Martha Camacho **Coordinadora Administrativa**