INTRODUCCIÓN

Talento Humano Vital S.A.S., ha encaminado los esfuerzos al fortalecimiento de la gestión de TI de la organización, implementando nuevas herramientas y fortaleciendo las existentes, ampliando la capacidad de la infraestructura tecnológica de la organización, acatando la normatividad legal, las normas aplicables y las recomendaciones establecidos desde el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) alineándose a la norma ISO 27001-2013.

La Alta dirección acorde a los requerimientos TIC y entendiendo la importancia de la gestión seguridad de la información, se ha comprometido y se adhiere a seguir los lineamientos haciendo un camino para la implementación de un sistema de gestión de seguridad de la información conforme al modelo de seguridad y privacidad de la Información estableciendo su propia Política de Seguridad de la Información, buscando conformar un marco de confianza en el ejercicio de sus deberes con diferentes grupos de interés y aliados de negocio, dando cumplimiento a las leyes y demás normatividad vigente en concordancia con la misión y visión de la organización.

Para Talento Humano Vital S.A.S., la protección y salvaguarda de la información busca la disminución del impacto generado sobre sus activos de información, por las situaciones no deseadas que afecten negativamente el logro de los objetivos misionales y estratégicos.

1. TÉRMINOS Y DEFINICIONES

Para los propósitos de este documento se aplican los términos y definiciones presentados en la norma ISO/IEC 27000.

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27001).
Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
Activo de información es todo recurso por medio del cual se almacena, procesa, transmite, divulga, comunica, intercambia, presenta y genera la información, de igual manera la información en sí misma es un activo de información solo que esta se vale de algún medio o recurso para su gestión.
Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o organización 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)

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).

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).

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).

Riesgo: Efecto de la incertidumbre sobre los objetivos.

Un efecto es una desviación respecto a lo previsto. Puede ser positivo, negativo o ambos, y puede abordar, crear o resultar en oportunidades y amenazas.

Los objetivos pueden tener diferentes aspectos y categorías (por ejemplo: financieros, salud y seguridad, y metas ambientales) y se pueden aplicar a niveles diferentes (estratégico, en toda la organización, en proyectos, productos y procesos).

A menudo el riesgo está caracterizado por la referencia a los eventos potenciales y las consecuencias o a una combinación de ellos.

Con frecuencia, el riesgo se expresa en términos de fuentes de riesgo, eventos potenciales, sus consecuencias y sus probabilidades.

Incertidumbre es el estado, incluso parcial, de deficiencia de información relacionada con la comprensión o el conocimiento de un evento, su consecuencia o probabilidad.

Riesgo de seguridad digital: Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas ISO/IEC 27000 - 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.

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

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).

2. ROLES Y RESPONSABILIDADES EN LA SEGURIDAD DE LA INFORMACIÓN

El **Representante por la Alta Dirección** de Talento Humano Vital SAS ante el Sistema de Gestión de Seguridad de la Información es la Directora de Servicios quien debe velar por la planeación, implementación y Cumplimiento.

En sus responsabilidades están:

- Presentar soluciones y nuevas propuestas de alto impacto a la organización para su análisis y aprobación.
- Representar y atender los requerimientos de los aliados de negocio cuando soliciten visitas, solicitudes de requerimientos específicos o auditorías de tercera parte.
- Liderar la definición de las estrategias a implementar en seguridad de la información.
- Realizar la revisión por la alta Dirección al SGSI al menos una vez al año.
- Presidir las reuniones en donde se traten aspectos estratégicos y tácticos relevantes del Sistema de Gestión de Seguridad de la Información.

El **Responsable de Seguridad de la Información** es el líder del Equipo de Trabajo de Tecnología de la Información quien a su vez se apoya en expertos técnicos para la implementación, implantación, puesta en marcha, mantenimiento, supervisión y mejora continua del Sistema de Gestión de Seguridad de la Información. Este rol tiene las siguientes responsabilidades:

- Velar por la implementación, puesta en marcha y mantenimiento del Sistema de Gestión de Seguridad de la Información.
- Velar por la revisión de la estructura (políticas, procedimientos, instructivos, roles, responsables y responsabilidades) del Sistema de Gestión de Seguridad de la Información.
- Hacer seguimiento al plan de trabajo que permita el logro de los objetivos específicos de seguridad de la información Talento Humano Vital.
- Presentar los cambios, proyectos e iniciativas del SGSI al representante por la Dirección del Sistema de Gestión de Seguridad de la Información.
- Monitorear y velar por el cumplimiento del Plan Operativo de Seguridad de la Información Talento Humano Vital.
- Presentar las necesidades de recursos financieros para el desarrollo de proyectos que fortalezcan la gestión de la seguridad de la información con el fin de lograr los objetivos misionales y estratégicos Talento Humano Vital.

El **Líder Técnico de Seguridad de la Información** es la persona designada por la empresa, como un tercero proveedor TIC, quien implementa y quien mantiene

operativamente el Sistema de Gestión de Seguridad de la Información. En sus responsabilidades están:

- Aplicar conocimientos, habilidades, herramientas, y técnicas a la ejecución del Plan Operativo de Seguridad de la Información las actividades propias del proyecto, de manera que cumpla o exceda las necesidades y expectativas de los interesados en el mismo.
- Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación de la organización.
- Generar el cronograma de la implementación del Modelo de Seguridad y privacidad de la información.
- Planear e implementar las tareas, fechas y plan de trabajo para el cumplimiento de los objetivos específicos de seguridad de la información Talento Humano Vital.
- Coordinar las actividades de los colaboradores con responsabilidades críticas en el SGSI y proporcionar apoyo administrativo.
- Planear y ejecutar de los planes de trabajo propuestos del SGSI, bajo un enfoque orientado a riesgos para darle solución oportuna y escalar al responsable de seguridad de la información en caso de ser necesario.
- Trabajar de manera integrada con el grupo o áreas asignadas.
- Velar por el mantenimiento documental del SGSI, su custodia y protección.
- Contribuir al enriquecimiento en la gestión del conocimiento en materia de seguridad y privacidad de la información apoyando la documentación de las lecciones aprendidas.
- Participar en las reuniones de seguimiento y velar por la actualización de los indicadores de gestión del SGSI.

Responsables críticos de la seguridad digital: Son colaboradores que por sus funciones gestionan, administran o supervisan activos de información críticos de la empresa. A este rol pertenecen los funcionarios directivos y/o líderes de procesos, los colaboradores de THV y el responsable de infraestructura y servicios tecnológicos. En sus responsabilidades está:

- Cumplir y velar por el estricto cumplimiento de las políticas de seguridad de la información a título personal y en los colaboradores o equipos de trabajo bajo su cargo.
- Atender los requerimientos de seguridad que les soliciten y en caso de ser requerido escalarlo al líder técnico de seguridad de la información o al responsable de seguridad de la información.
- Participar en las reuniones de seguridad de la información cuando sean convocados.
- Brindar y poner a disposición sus conocimientos, habilidades y capacidades en la resolución de problemas e incidentes de seguridad de la información y de seguridad digital.

Responsables de la seguridad de la información en Talento Humano Vital SAS: Son responsables por la seguridad de la información todos los colaboradores vinculados o que son partes interesadas Talento Humano Vital SAS. Deben cumplir con las políticas de seguridad de la información y cuando identifiquen algún posible riesgo de seguridad de la información deben notificarlo a la THV o al responsable de seguridad de la información o al oficial de seguridad de la información.

3. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Talento Humano Vital SAS, empresa especializada en procesos consultoría en el manejo de pruebas de polígrafo en todas sus aplicaciones y procesos de selección de personal protege, custodia y preserva la información gestionada en sus procesos, mediante una adecuada gestión de riesgos de seguridad y privacidad de la información, incluyendo los de seguridad digital, que permitan el adecuado acceso, procesamiento, transporte, intercambio, almacenamiento, presentación, comunicación y divulgación de la información, logrando los niveles de confidencialidad, disponibilidad e integridad requeridos para dar cumplimiento a los requisitos legales y reglamentarios y, a las necesidades del cliente interno y externo. La protección, custodia y preservación de la información respalda los objetivos misionales y estratégicos Talento Humano Vital, por lo tanto, es responsabilidad de los colaboradores, contratistas, proveedores y demás partes interesadas dar cumplimiento y hacer cumplir la presente política.

Talento Humano Vital SAS, para asegurar su dirección estratégica, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

1. Minimizar el riesgo de los procesos misionales de la organización.
2. Cumplir con los principios de seguridad de la información.
3. Mantener la confianza de los colaboradores, contratistas y terceros.
4. Proteger los activos de información.
5. Fortalecer la cultura de seguridad de la información en los, terceros, contratistas, practicantes y clientes Talento Humano Vital SAS.

3.1 Justificación de la política para la gestión de seguridad de la Información

Talento Humano Vital SAS realiza esta declaración de compromiso, justificada en que para la Organización es muy importante contar con políticas de seguridad ya que son ellas quienes guiarán el comportamiento personal y profesional de los , contratistas o terceros sobre la información obtenida, generada o procesada por la organización, así mismo las políticas permitirán que la organización trabaje bajo las mejores prácticas de seguridad y cumpla con los requisitos legales a los cuales esté obligada a cumplir. Debido a la importancia y sensibilidad de la información, se incluye el sistema de seguridad de la información dentro del sistema de gestión de la organización de tal forma que le permita generar la mejora continua del sistema de seguridad, basados en la gestión de riesgos y continuidad Talento Humano Vital SAS.

3.2 Alcance/Aplicabilidad de la política para la gestión de seguridad de la información

Esta política aplica a todos los activos de información, a todos los procesos Talento Humano Vital SAS y también a sus partes interesadas internas y externas en el cumplimiento de los objetivos misionales y estratégicos.

4. POLÍTICAS GENERALES

A continuación, se establecen las políticas generales de seguridad de información que soportan el Sistema de Gestión de Seguridad de la Información Talento Humano Vital SAS:

- Talento Humano Vital SAS ha decidido definir, implementar, operar y mejorar sus políticas TIC de forma continua, alineadas, haciendo un camino para la implementación a futuro de un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades de la organización, y a los requerimientos regulatorios que le aplican a su naturaleza.
- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los colaboradores, contratistas o terceros.
- Talento Humano Vital SAS protegerá la información accedida, procesada, transportada, almacenada, presentada, comunicada y divulgada por los procesos, con el fin de minimizar los impactos negativos de detrimento y de tipo financiero, legal, operativo o reputacional como consecuencia de incidentes de seguridad de la información para lo cual se implementarán controles como mecanismos de tratamiento del correspondiente riesgo.
- Talento Humano Vital protegerá su información de las amenazas originadas por parte del personal.
- Talento Humano Vital implementa controles para la protección de las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos.
- Talento Humano Vital implementa los controles para cumplir con los niveles requeridos por esta, para la seguridad de los recursos tecnológicos y la red de datos.
- Talento Humano Vital implementa controles de acceso a la información, sistemas y recursos de red.
- Talento Humano Vital integra la seguridad de la información al ciclo de vida de los sistemas de información.
- Talento Humano Vital SAS implementa la mejora continua de la seguridad y privacidad de la información a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas.
- Talento Humano Vital SAS garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

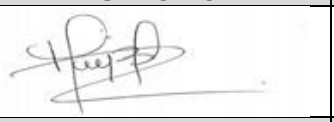
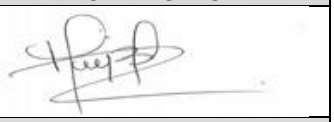
El incumplimiento a la política de Seguridad y Privacidad de la Información traerá consigo,

las consecuencias legales que apliquen a la normativa de la Organización, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

La presente política debe ser revisada y actualizada anualmente o cuando el Líder de Seguridad de la Información lo determine, teniendo como criterios los cambios relevantes en el contexto interno y externo, cuando la identificación de nuevos riesgos de seguridad de la información lo requiera o cuando el marco legal que regula las políticas nacionales en materia de Seguridad de la Información, Seguridad Digital o Gobierno Digital lo demanden.

5.CONTROL DE MODIFICACIONES Y REGISTRO DE APROBACIÓN:

VERSIÓN	FECHA VIGENCIA	RAZÓN DEL CAMBIO
01	09/08/2022	Versión Inicial

	ELABORADO POR:	REVISADO POR:	APROBADO POR:
Firma:			
Nombre:	**MARYSOL PORTILLA E.**	**MIRYANI BURBANO A.**	**MIRYANI BURBANO A.**
Cargo:	Asesor SGI	Responsable del SGI	Gerente
Fecha:	08/09/2022	13/09/2022	13/09/2022