

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

VELEZLAB SAS, entendiendo que la información es el activo más valioso para nuestra organización y conscientes de la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información, buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado, con sus clientes y con sus proveedores, todo esto enmarcado en el estricto cumplimiento de lo establecido por el Artículo 15 de la constitución política colombiana, por la ley 1266 de 2008: ley de habeas data, por la Ley 1581 de 2012, y demás normas complementarias y reglamentarias establecida por las leyes colombianas.

VELEZLAB SAS, ha establecido la presente política general de seguridad de la información, con el objetivo de proteger y garantizar la integridad, confidencialidad y disponibilidad de la información a la que tenemos acceso.

De acuerdo con lo anterior, esta política aplica a VELEZLAB SAS, sus funcionarios, clientes externos, terceros, aprendices, practicantes, proveedores, socios de negocios y en general, a todos los que de alguna manera tengan acceso a información relacionada con VELEZLAB SAS.

VELEZLAB SAS, en el marco de su sistema de gestión de seguridad de la información y su política general de seguridad de la información, ha definido las siguientes políticas:

- 1. Ciclo de vida de la información:**
 - a.** Creación y vigencia.
 - b.** Publicación.
 - c.** Almacenamiento
 - d.** Destrucción final.
- 2. Niveles de información, de acuerdo con la Confidencialidad:**
 - a.** Confidencial: Información disponible solo para la alta gerencia de la organización.
 - b.** Restringida: Información disponible solo para jefaturas de la organización.
 - c.** De uso interno/ Privada: Información de acceso común y restringido a la organización. En algunos casos con cláusula de confidencialidad.
 - d.** Público: De acceso común a la organización y al público en general.
- 3. Acceso a la información basado en roles.**
- 4. Salvaguarda de la información con los medios idóneos y seguros.**

Principios de seguridad de la información

VELEZLAB SAS, en el marco de su sistema de gestión de seguridad de la información y su política general de seguridad de la información, ha definido los siguientes principios de seguridad de la información:

- VELEZLAB SAS protegerá la información generada, procesada y/o resguardada por los procesos de su negocio, su infraestructura tecnológica y activos, del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
- VELEZLAB SAS protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- VELEZLAB SAS protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, de las amenazas originadas por parte del personal de la empresa.
- VELEZLAB SAS protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- VELEZLAB SAS controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y de las redes de datos, en las instalaciones de la organización y en los accesos externos autorizados.
- VELEZLAB SAS implementará controles y/o perfiles de acceso a la información, sistemas y recursos de red, en las instalaciones de la organización y en los accesos externos autorizados.
- VELEZLAB SAS garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- VELEZLAB SAS garantizará una mejora efectiva de su modelo de seguridad, a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información.
- VELEZLAB SAS garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en la atención y gestión del impacto que puedan generar los eventos desfavorables y perjudiciales que se presenten.
- VELEZLAB SAS garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas, y en el marco de las leyes.

Definición de las políticas

- 1. Ciclo de vida de la información:**
 - a. Creación y vigencia.
 - b. Publicación.
 - c. Almacenamiento
 - d. Destrucción final.
- 2. Niveles de información, de acuerdo con la Confidencialidad:**
 - a. Confidencial: Información disponible solo para la alta gerencia de la organización.
 - b. Restringida: Información disponible solo para jefaturas de la organización.
 - c. De uso interno/ Privada: Información de acceso común y restringido a la organización. En algunos casos con cláusula de confidencialidad.
 - d. Público: De acceso común a la organización y al público en general. Toda la información y/o documentos que tengan firmas digitalizadas, se deben manejar en formato .pdf, para garantizar su integridad y confidencialidad.
- 3. Acceso a la información basado en roles:**
 - a. En el sistema de almacenamiento NAS, se tiene definido perfiles de lectura y/o escritura de acuerdo a permisos de acceso asignado a cada usuario, según documento “listado de usuarios permisos NAS”, para todos los documentos digitales de la organización.
 - b. En los aplicativos CRM, Isolución, y Sistema UNO, se tienen asignados permisos y roles para cada usuario.
- 4. Salvaguarda de la información con los medios idóneos y seguros:**
 - a. En Sistema de gestión de calidad se tiene establecido un procedimiento mediante el instructivo GC-INT-02: Ejecución de copias de seguridad, con el objetivo de salvaguardar toda la información digital que se requiere mantener de forma segura y recuperable.
 - b. El control de ejecución de copias de seguridad se evidencia en el registro GC-FOR-03: Control de ejecución de copias de seguridad.
 - c. Se establece que los archivos de los pc’s que requieran respaldo, deberán estar almacenados en el sistema de almacenamiento NAS, en sus respectivas carpetas. Toda la información y/o documentos que no se encuentren en el NAS, no tendrán respaldo y/o backup.
 - d. Los responsable de los registros físicos se encuentran identificados en el GC-FOR-04 Cuadro Control de Registros por proceso, igualmente el responsable de los demás documentos que aplican al SGC tales como procedimientos, instructivos, caracterizaciones y demás, se encuentran bajo el cuidado de los Responsables de cada proceso y el Área de Calidad en la medida en que se administran.

Términos y definiciones

- 1.** Información: Activo más valioso de la organización, que procede de diferentes fuentes, y en diferentes soportes como papel o medios digitales.
- 2.** Activos de la información: Son todos los datos o información de propiedad de VELEZLAB SAS, sensible para la organización, que hace parte fundamental de la misión de la empresa y que se encuentran almacenados en medios físicos y/o virtuales.
- 3.** Sistema de información: Conjunto de datos que interactúan entre sí con un fin común y que ayudan a administrar, recolectar, recuperar, procesar, almacenar y distribuir información relevante para los procesos fundamentales y misionales de VELEZLAB SAS.
- 4.** Sistema De Gestión De La Seguridad De La Información: Herramienta de que nos permite conocer, gestionar y minimizar, los posibles riesgos que atentan contra la seguridad de la información en VELEZLAB SAS.
- 5.** Tecnología de la información: Conjunto de medios, hardware, y/o software operados por VELEZLAB SAS o por terceros en su nombre y que permiten la captura, producción, almacenamiento, tratamiento, y presentación de información necesaria para el cumplimiento y operación de la misión de la organización.
- 6.** Cadena de custodia: Conjunto de procedimientos y controles que se aplican a los datos y/o a los activos de la información con el fin de preservarla y asegurar su total confidencialidad, integridad y disponibilidad.
- 7.** Confidencialidad: La información será protegida y no está a disposición, ni se revela a individuos, entidades o procesos no autorizados.
- 8.** Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso, garantizando que esta información permanece inalterada y completa.
- 9.** Disponibilidad: Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
- 10.** Niveles de clasificación de la información, de acuerdo a la disposición en el almacenamiento:
 - Física:** Almacenamiento de documentos impresos en carpetas, AZ, archivadores, escritorios con llave, etc.
 - Virtual:** Disposición de documentos electrónicos en almacenamientos como el NAS, Drive, Cloud, etc.

Referencias:

1. ISO 27001:2005. Sistemas de gestión de Seguridad en la Información – Requerimientos
2. <https://www.significados.com/sistema-de-informacion/>
3. https://www.ecured.cu/Tecnolog%C3%ADas_de_la_informaci%C3%B3n_y_las_comunicaciones.
4. <https://actualicese.com/10-puntos-que-debe-conocer-sobre-la-ley-de-habeas-data/>
5. https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Cartilla_Ley_1266_de_2008_Habeas_Data.pdf