FUNDACION PEDALAZOS QUE CONSTRUYEN

POLÍTICA PARA LA SEGURIDAD DE LA INFORMACIÓN

31 Julio de 2020

POLÍTICA PARA LA SEGURIDAD DE LA INFORMACIÓN

En virtud del fuerte compromiso de la **Fundación Pedalazos Que Construyen** con el adecuado tratamiento de datos personales, garantizando además de la salvaguarda y seguridad de la información, e ejercicio del Habeas Data, la empresa establece la presenta Política aplicables para la seguridad de la información en la organización.

1. OBJETIVO

La presente Política establece las directrices generales para la Seguridad de la Información al interior de la **Fundación Pedalazos Que Construyen** con el objetivo de brindar las condiciones de seguridad necesarias que impidan la adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento a la información que es tratada por la **Fundación Pedalazos Que Construyen**.

2. ALCANCE

Esta Política de Seguridad de la Información será aplicada en todos los aspectos administrativos, de gestión, logísticos y de control fijados por la empresa, que deben ser cumplidos por los directivos, funcionarios, contratistas, terceros que presten sus servicios, empleados de terceros proveedores que estén regulados por términos contractuales, y en general todas aquellas personas que tengan algún tipo de relación con la manipulación de información en la **Fundación Pedalazos Que Construyen**.

3. POLÍTICAS ESPECÍFICAS PARA EL TRATAMIENTO DE DATOS PERSONALES.

3.1 INSTALACIÓN DE SOFTWARE

Propósito: Minimizar el riesgo de exposición y de infección por malware, evitando a su vez posibles sanciones por el uso de software sin licenciar.

Política

Los trabajadores no deben instalar software en los dispositivos de la compañía sin la respectiva autorización. Las peticiones de instalación de software deben ser aprobadas por el administrador de la red y el proceso de instalación debe ser realizado por personal calificado de la compañía.

Todo software que sea instalado debe tener licenciamiento comercial, ser de licenciamiento libre (open source, free, trial), o en su defecto la licencia debe provenir del departamento de tecnología.

3.2 USO DE DISPOSITIVOS DE ALMACENAMIENTO EXTERNO

Propósito: Minimizar el riesgo de exposición de información de la empresa o de infección por malware contenido en dispositivos externos de almacenamiento (Discos Duros externos, USBs, CDs, Diskettes, Teléfonos Celulares, Reproductores Multimedia, etc.).

Política

Está prohibido el uso de dispositivos de almacenamiento personales dentro de la infraestructura tecnológica de la compañía. En caso de requerirse alguno de estos dispositivos, se deben solicitar a modo de préstamo a los jefes de área correspondientes.

Una vez se termine de realizar la labor requerida con el dispositivo se debe eliminar toda la información contenida en el mismo, realizar una limpieza con un software de antivirus y retornarse al encargado.

3.3 USO DE CORREO ELECTRÓNICO Y COMUNICACIONES PERSONALES

Propósito: Prevenir daños y perjuicios en la imagen o el nombre de la organización por el manejo incorrecto de los servicios de comunicación.

Política

Los diferentes medios de comunicación a disposición de los trabajadores no deben ser utilizados para la distribución de mensajes con contenido ofensivo, racista, discriminatorio, pornográfico, sexual, político, etc. Los empleados que reciban comunicaciones con este contenido deben eliminarlo inmediatamente y reportar el incidente si es de origen interno.

Utilizar los correos empresariales para comunicaciones personales está prohibido. En especial si es para la distribución de mensajes cadena, spam o de alguna forma comerciales.

Los empleados no deben esperar privacidad alguna en contenido que almacenen o envíen como parte de los servicios de comunicación de la compañía. El no cumplimiento de las condiciones mencionadas anteriormente es considerado una falta disciplinaria y puede ser objeto de sanción.

3.5 COPIAS DE SEGURIDAD

Propósito: Evitar la pérdida de información de la empresa. :

Política

Las copias de seguridad de la información se tomarán de forma manual cada 180 días, a las bases de datos con información que contengan dichas bases. Las copias de respaldo se almacenarán en medios disco extraíble, Dropbox del SG-SST si la base de datos hace parte del mismo como evidencia del sistema y en el sistema zoho docs de Google Chrome que cuenta con clave de acceso y serán custodiadas por un periodo igual a dos años.

Los funcionarios responsables de la gestión del almacenamiento y respaldo de la información deberán proveer los recursos necesarios para garantizar el correcto tratamiento de esta.

Los dueños o responsables de los activos de información tecnológicos y recursos informáticos deben definir las estrategias para la correcta y adecuada generación, retención, y rotación de las copias de respaldo de la información.

Los dueños o responsables de los activos de información tecnológicos y recursos informáticos deben velar por el cumplimiento de los procedimientos de respaldo de la información.

MANEJO DE CLAVES

Propósito: El propósito de esta política es establecer un estándar de generación de contraseñas seguras, la protección de dichas contraseñas y su frecuencia de cambio.

Política

Todas las contraseñas de nivel de sistema (root, administrador, usuarios de windows, etc., bases de datos), deben ser cambiadas al menos cada tres meses.

Todas las contraseñas de nivel de usuario (correo, cuentas personales), deben ser cambiadas al menos cada seis meses.

Todas las contraseñas utilizadas deben seguir las condiciones descritas a continuación: Contener al menos tres de los siguientes caracteres: Minúsculas, Mayúsculas, Números, Caracteres especiales (e.g. #$%&/(“!.;), la longitud de la contraseña debe ser de al menos 8 caracteres, la contraseña no debe estar compuesta únicamente de palabras de diccionario, se deben evitar contraseñas tradicionales como password, 123456, qwerty, asdfg, etc.

Como base del correcto manejo de claves y contraseñas se presentan una serie de recomendaciones para el manejo correcto de las mismas:

- Siempre utilice contraseñas diferentes para los servicios de la compañía y sus cuentas personales no relacionadas al ámbito laboral.
- No comparta sus contraseñas con ningún tercero, incluso si este pertenece a la organización.
- Las contraseñas nunca deben estar escritas en texto plano (jamás archivos llamados claves.txt y en el escritorio).

- No revele las contraseñas por medios de comunicación desprotegidos como correo, mensajería instantánea, SMS, etc.
- Evite utilizar la opción de recordar contraseña en navegadores y programas internos.

3.6 REGISTRO DE ACTIVIDAD Y SUPERVISIÓN

Propósito: Registrar eventos y generar evidencia.

Política

Se producirán revisiones regulares y cuidadosas a los registros de eventos que se graban de las actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

Los registros de información se protegerán contra la manipulación y el acceso no autorizado. Las actividades del administrador del sistema y de la red serán registradas.

Estos registros serán protegidos y regularmente revisados.

Los relojes de todos los sistemas de informática relevantes serán sincronizados a una fuente de tiempo de referencia única.

3.7 LA SEGURIDAD FÍSICA Y AMBIENTAL

Propósito: Evitar el acceso físico no autorizado, daños e interferencia para la información de la organización y las instalaciones de procesamiento de información.

Política

El equipo de cómputo se encuentra en un sitio dispuesto para tal fin, cuenta con un transformador de corriente y supresor de picos como protección para fallas de energía. El equipo no está expuesto al medio ambiente ni tiene luz solar directa. Las bases de datos en papel se encuentran dentro del folder del sistema SG-SST, el cual esta guardado en un armario bajo llave y no expuesto ni al medio ambiente ni daños ambientales.

Los equipos, la información o el software no se sacarán de las instalaciones de la empresa sin la previa autorización. Se aplicará seguridad a los activos fuera de las instalaciones, teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.

Todos los elementos del equipo que contienen los medios de almacenamiento deberán ser verificados para garantizar que los datos sensibles y el software con licencia se han eliminado o sobrescrito de forma segura antes de su eliminación o reutilización.

Los usuarios deberán asegurarse de que el equipo que no cuenta con vigilancia tenga la protección adecuada.

Los puestos de trabajo deben estar limpios de papeles, soportes de almacenamiento extraíbles y cuando un computador este desatendido deberá bloquearse la pantalla.

Cuando sea apropiado, papeles y medios de información deben estar asegurados en armarios especiales, especialmente en horas fuera de las normales de trabajo.

3.8 ACCESO A DATOS SENSIBLES DE LOS EMPLEADOS. Y/O CONTRATISTAS, DONADORES, VOLUNTARIOS Y PARTICIPANTES.

Propósito: Garantizar que los datos sensibles relacionados con los datos de la salud, creencias religiosas, políticas, sexuales, entre otros de los trabajadores, voluntarios, participantes, beneficiarios y donadores**,** solo puedan ser conocidos por el personal competente y pertinente en virtud de sus funciones, teniendo en cuenta el principio de Acceso Restringido.

Política:

Las finalidades para las que son tratados los datos sensibles en la empresa son limitadas y especificadas en las respectivas autorizaciones otorgadas por el titular de la información.

De forma general, el tratamiento de datos sensibles en la empresa, estará limitado únicamente a las divisiones: División administrativa y el representante legal atendiendo las finalidades particulares autorizadas por el titular.

La empresa de forma particular y en los respectivos manuales de funciones según el cargo, determinará aquellos cargos particulares que podrán tener acceso a datos de carácter sensible, sin que ese acceso signifique una violación a la política de seguridad de acceso restringido.

Igualmente, aplican los mecanismos de seguridad identificados previamente como de acceso restringido a los datos personales.

3.9 SEGURIDAD DE LA INFORMACIÓN ENTORNO AL RECURSO HUMANO

En tratamiento de los datos personales, antes, durante y después de la relación laboral, se regirá por las siguientes reglas:

- **La** Fundación Pedalazos Que Construyen informará a las personas interesadas en participar en un proceso de selección, las reglas aplicables al tratamiento de los datos personales que suministre el interesado durante el respectivo proceso de selección, así como de aquellos datos que se obtengan durante la realización del mismo.

- El tratamiento de los datos suministrados por los interesados en las vacantes de **La Fundación Pedalazos Que Construyen,** y los obtenidos del proceso de selección, será únicamente la informada en la autorización al aspirante.

- La empresa realizará estudios de seguridad previos a la contratación de nuevo personal para la empresa.

- La empresa contará con un proceso de eliminación de las hojas de vida de los candidatos (titulares) sobre los que ya no se tenga interés en conservar contacto, teniendo en cuenta las herramientas de archivística tales como tablas de valoración documental, tablas de retención documental y cuadros de comparación documental.

- Una vez seleccionada un aspirante para ocupar un cargo en la **Fundación Pedalazos Que Construyen,** se celebrará el respectivo contrato de trabajo, acuerdo de confidencialidad y se le asignará cuando el cargo lo requiera, un usuario con un perfil definido relacionado directamente con el cargo a desempeñar, el cual le permitirá el acceso a la información personal tratada por la empresa, cuando el cargo así lo requiera.

- Seleccionado el candidato para el cargo, la empresa almacenará los datos personales del trabajador en una carpeta identificada con el nombre de cada persona. A esta carpeta solo tendrá acceso el Área de Gestión Humana y Administrativa y con la finalidad de gestionar la relación laboral entre la empresa y el empleado.

- Para cuando **la Fundación Pedalazos Que Construyen,** requiera contratar servicios externos para el tratamiento de datos durante la relación contractual con los trabajadores, podrá requerirse la transferencia de datos personales a un tercero que se denominará Encargado, Para este caso, la empresa seguirá los lineamientos para la selección de Encargados en la transmisión de datos personales contenidos en esta política.

- Una vez se termine el contrato de trabajo, la empresa suscribirá un acuerdo de confidencialidad con el ex trabajador para salvaguardar la confidencialidad de la información personal manipulada por el ex trabajador; así como solicitará la entrega formas de perfiles y contraseñas que le hayan sido asignadas durante la ejecución del contrato de trabajo.

- Terminada la relación laboral, la **Fundación Pedalazos Que Construyen** igualmente procederá a almacenar los datos personales de sus datos en un archivo general, sometiendo tal información a medidas y niveles de seguridad altas, atendiendo la calidad de los datos que dicho archivo puede contener.

3.10 CONFIDENCIALIDAD CON TERCEROS

Propósito: Establecer los requerimientos de confidencialidad en las relaciones con proveedores, contratistas, en particular con empleados y los terceros en general.

Política

Para el desarrollo de las relaciones contractuales, comerciales y laborales, se debe exigir a los terceros la aceptación de los acuerdos de confidencialidad definidos por la organización. En dichos acuerdos se debe establecer el compromiso de salvaguardar la información, velar por su correcto uso, impedir el uso no autorizado de dicha información y guardar reserva. Se debe estipular a su vez la información que es objeto de protección dentro del acuerdo y su temporalidad.

Los acuerdos deben incluirse dentro de los contratos celebrados entre la organización y terceros, como parte integral del contrato o firmarse como un acuerdo independiente. La aceptación de las condiciones de confidencialidad es indispensable para conceder al tercero el acceso a la información protegida.

3.11 SELECCIÓN DE ENCARGADOS PARA TRANSMISIÓN DE DATOS PERSONALES-

Propósito: Garantizar que en los eventos en los que se realicen transmisiones de datos personales, se elija el encargado teniendo en cuenta las prerrogativas que trata la normativa sobre protección de datos personales.

Política

Cuando la FUNDACION PEDALAZOS QUE CONSTRUYEN como responsable del tratamiento de datos personales, cuando realice Transmisión de datos personales, es de imperativo cumplimiento por parte de la empresa, seguir los siguientes lineamientos:

- Determinar cuál será el alcance del tratamiento que se permitirá realizar al Encargado.
- Evaluar la competencia y capacidad del Encargado para realizar el tratamiento que se le encomendará-
- Revisar el manual de políticas de tratamiento de datos personales propias del Encargado.
- Examinar las medidas de seguridad implementadas por el Encargado para el tratamiento de los datos personales, y su compatibilidad con los estándares determinados por la **Fundación Pedalazos Que Construyen**.
- Suscribir un contrato de transmisión de datos personales.
- Realizar auditorías para medir el nivel de protección de los datos personales en la ejecución del contrato de transmisión.

3.12 REVISIONES DE LA SEGURIDAD DE LA INFORMACIÓN

Propósito: Garantizar que la seguridad informática sea implementada y aplicada de acuerdo con las políticas y procedimientos de la organización.

Política

Los sistemas de información son revisados regularmente a través de Auditorias para cerciorarse que se da cumplimiento a las políticas y normas de seguridad de la información de la entidad.

4. PROCESO PARA LA ATENCIÓN DE INCIDENTES

Toda vez que se presente algún incidente con la seguridad de la información tratada por la **Fundación Pedalazos Que Construyen**, deberá adelantarse el siguiente procedimiento:

1). **Reporte del Incidente:** Ocurrido el incidente de seguridad, la primera persona que tenga conocimiento del mismo, deberá inmediatamente presentar dirigido al área o persona encargada de la seguridad de la información, Área Administrativa; así como en el menor tiempo posible presentar un informe detallado sobre los hechos que del mismo se conocen.

2). **Comunicación del Incidente ante la SIC:** Todo incidente de seguridad de la información, deberá ser reportado ante la Superintendencia de Industria y Comercio, específicamente ante el Registro Nacional de Bases de Datos -RNBD-. El reporte de los incidentes es una obligación de la **Fundación Pedalazos Que Construyen**, quien deberá realizarlo una vez haya sido notificados de la ocurrencia del mismo por parte de cualquier área de la compañía.

3). **Reunión del comité de Seguridad de la información:** El área o persona encargada de la seguridad de la información, ÁREA ADMINSITRATIVA conformara de forma extraordinaria la reunión de miembros de la Junta Directiva para la seguridad de la información, en el cual se desarrollarán los siguientes ítems.

   a. **Emisión del concepto técnico:** Evaluados los Hechos del caso se deberá dar un concepto técnico que determina todas las contingencias surgidas en el caso en concreto.
   b. **Identificación de la falencia:** Como resultado del concepto técnico, se deberá identificar plenamente la falencia que dio paso al incidente de seguridad de la información.
   c. **Toma de Medidas:** El comité deberá tomar las medias y los correctivos necesarios para evitar futuros incidentes.

5. MODIFICACIÓN DE LAS POLÍTICAS

La FUNDACION PEDALAZOS QUE CONSTRUYEN, se reserva el derecho de modificar la presente Política de Seguridad de la información en cualquier momento, comunicando de forma oportuna a todas aquellas personas que estén relacionadas o que participen en la manipulación de la información de la empresa para su correcta implementación.

6. VIGENCIA

La presente Política rige a partir del 01 de julio de 2020.