POLITICAS DE MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN

LATAMSEC SECURITY LTDA

2020

POLÍTICAS DE MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN.

En virtud del fuerte compromiso de la empresa **LATAMSEC SECURITY LTDA.,** 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 empresa.

1. OBJETIVO

Establecer las políticas que regulan la seguridad de la información en la empresa **LATAMSEC SECURITY LTDA.,** y presentar en forma clara y coherente los elementos que conforman la política de seguridad que deben conocer, acatar y cumplir todos los empleados, contratistas, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con la empresa.

2. ALCANCE

Las Políticas de Seguridad de la Información son aplicables para todos los aspectos administrativos y de control que deben ser cumplidos por los empleados, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la empresa **LATAMSEC SECURITY LTDA.,** para el adecuado cumplimiento de sus funciones y para conseguir un adecuado nivel de protección de las características de calidad y seguridad de la información, aportando con su participación en la toma de medidas preventivas y correctivas, siendo un punto clave para el logro del objetivo y la finalidad de dicha política. Los usuarios tienen la obligación de dar cumplimiento a las presentes políticas emitidas y aprobadas por la empresa.

3. POLÍTICAS ESPECÍFICAS PARA EL TRATAMIENTO DE DATOS PERSONALES.

3.1 POLITICA DE INSTALACIÓN DE SOFTWARE O HARDWARE

Objetivo: Minimizar el riesgo de exposición y de infección por malware, evitando a su vez posibles sanciones por el uso de software sin licenciar o computadores que no están permitidos por la directriz de la empresa.

Procedimiento:

Los trabajadores o contratistas no deben instalar software en los dispositivos de la empresa 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 administración de la empresa.

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 administración.

3.2 POLITICA PARA USO DE DISPOSITIVOS MOVILES DE ALMACENAMIENTO

Objetivo: Minimizar el riesgo de hurto de la información de la empresa o de infección por malware contenido en dispositivos móviles o externos de almacenamiento (Discos Duros extraíbles, USB, CD, Teléfonos Celulares, tabletas Reproductores Multimedia, etc.).

Procedimiento

Está restringida la copia de archivos en dispositivos de almacenamiento personales dentro de la infraestructura tecnológica de la empresa. En caso de requerirse alguno de estos dispositivos, se debe informar al administrador que información será almacenada por parte del contratista para su uso externo.

Una vez se termine de realizar la labor o contrato requerido con el dispositivo, empleado o contratista se debe eliminar toda la información contenida en el mismo, realizar una limpieza con

un software de antivirus o auditar que esa información no repose en los dispositivos personales externos.

3.3 USO DE INTERNET

Objetivo: El propósito de esta política es definir los estándares para el monitoreo y limitación de la navegación por Internet desde cualquier dispositivo en la red de la empresa. Estos estándares están diseñados para asegurar que los empleados o contratistas utilicen el Internet de forma segura y responsable.

Procedimiento

La administración permite el acceso a servicio a internet, estableciendo lineamientos que garanticen la navegación segura y el uso adecuado de la red por parte del trabajador o contratista evitando errores, perdidas, modificaciones no autorizadas o uso inadecuado de la información de Internet.

La administración prohíbe los sitios de Internet que se consideren inapropiados para la ejecución del contrato. Se considera un incumplimiento a la seguridad bajo cualquier circunstancia el acceso a páginas y sitios web de contenido sexual explícito, sitios de juegos o apuestas, sitios relacionados con sustancias ilícitas, sitios de citas y redes sociales, mensajería instantánea, acceso a sistemas de almacenamiento en la nube, sitios de fraude, contenidos SPAM o en relación a delitos tipificados por la ley colombiana, contenido racista o de alguna forma ofensivo y discriminatorio, contenido violento, y todo contenido que no esté relacionado con el desarrollo de las finalidades de la empresa sin que medie previa autorización.

Por último, la administración está en potestad de monitorear todas las comunicaciones entrantes y salientes dentro de la red de la empresa. Esto incluye conocer la IP de origen, la fecha, la hora, el protocolo, el servidor o dirección de destino y los datos comunicados.

3.4 POLITICA DE USO DEL CORREO ELECTRÓNICO.

Objetivo: Definir las pautas generales para asegurar una adecuada protección de la información, en el uso del correo electrónico por parte de los usuarios autorizados.

Procedimientos

Está prohibido que el empleado o contratista utilice los correos corporativos para comunicaciones personales. En especial si para la distribución de mensajes cadena, spam o de alguna forma comercial. Su uso será exclusivo para la ejecución del contrato y con fines de la empresa.

Los empleados o contratistas no deben esperar privacidad alguna en contenido que almacenen o envíen como parte de los servicios de comunicación de la empresa. El no cumplimiento de las condiciones mencionadas anteriormente es considerado una falta a la seguridad.

3.5 BACK UP

Objetivo: salvaguardar información mediante copias de seguridad.

Procedimiento

Las copias de seguridad de la información se tomarán de forma automática cada treinta (30) días, a la información con contenido contable y administrativo de los computadores de la empresa, Las copias de respaldo se almacenarán en medios físicos como memorias extraíbles y serán custodiadas por un periodo igual a un (1) año.

Se realizará, automáticamente copias de seguridad (Back up) de acuerdo a las indicaciones del mismo con la finalidad de recuperación de la información y la infraestructura después de una falla, serán respaldadas y podrán ser restauradas en caso de una falla y/o desastre.

El administrador responsable de la gestión del almacenamiento y respaldo de la información deberán proveer los recursos necesarios para garantizar el correcto tratamiento de la misma. A su vez generar procedimientos de disposición y monitoreo del cumplimiento de las copias de seguridad al tiempo estipulado para el respaldo y protección de la información.

3.5 MANEJO DE CLAVES

Objetivo: suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados**,** con un estándar de generación de contraseñas seguras, la protección de dichas contraseñas y su frecuencia de cambio.

Procedimiento

Todas las contraseñas de nivel de sistema (root, administrador, usuarios de windows, etc., bases de datos del computador) deben ser cambiadas al menos cada 8 meses.

Todas las contraseñas de nivel de usuario (correos corporativos o software), deben ser cambiadas al menos cada ocho meses.

Las claves o contraseñas deben:

- Tener mínimo ocho (8) caracteres alfanuméricos.
- Cada vez que se cambien estas deben ser distintas por lo menos de las últimas doce anteriores.

La contraseña debe cumplir con tres de los cuatro requisitos:

- Caracteres en mayúsculas
- Caracteres en minúsculas
- Base de dígitos (0 a 9)
- Caracteres no alfabéticos (Ejemplo: ¡,$,%,&)

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 empresa 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.

En el momento que la empresa realice cambio de administrador y de su personal de contratistas debe dejar un informe con las respectivas claves y usuarios al acceso de lo computadores, correos electrónicos y software de la empresa.

3.6 POLITICAS DE SUPERVISIÓN Y MONITOREO.

Objetivo: Supervisión y monitoreo de las políticas o actividades que contienen datos personales.

Procedimiento

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 POLITICA DE SEGURIDAD FÍSICA

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

Procedimiento

Los equipos de cómputo deben estar situados y protegidos para reducir los riesgos de las amenazas ambientales y los riesgos y las oportunidades de acceso no autorizado. El equipo deberá estar protegido contra fallas de energía y otras interrupciones causadas por fallas en el soporte de los servicios públicos. El cableado que transporta datos, energía y telecomunicaciones o el soporte de los servicios de información debe estar protegido contra la intercepción, interferencia o daños. Los

equipos de cómputo deben tener un correcto mantenimiento para asegurar su continua disponibilidad e integridad como los siguientes:

- No Fumar dentro de la oficina.
- No introducir alimentos o bebidas.
- No Mover, desconectar equipo de cómputo sin autorización.
- No Modificar la configuración del equipo sin autorización.
- No Extraer información en dispositivos externos.
- Al imprimir documentos con información (semiprivada o privada), deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia
- Los trabajadores o contratistas deben bloquear la pantalla de su computador con el protector de pantalla, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo.

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 puestos de trabajo deben estar limpios de papeles, soportes de almacenamiento extraíbles

Cuando sea apropiado, papeles y medios de información deben estar asegurados en armarios especiales, especialmente en horas fuera de las normales de trabajo. A su vez, si utilizamos papel reciclaje debemos clasificar dicha información que no contenga datos (semiprivado, privado o sensible).

3.8 POLITICA PARA EL CONTROL DE ACCESO

Propósito: Limitar el acceso de la información y a las instalaciones de procesamiento de la información.

Procedimiento

Los trabajadores tienen la obligación de vigilar y garantizar que se cumplan las siguientes medidas de seguridad:

- El acceso a áreas seguras donde se procesa o almacena información confidencial y restringida, es limitado únicamente a personas autorizadas.
- El acceso a áreas seguras, requieren esquemas de control de acceso, como tarjetas, llaves o candados.
- El responsable de un área segura debe asegurar que no ingresen cámaras fotográficas, videos, teléfonos móviles con cámaras, salvo se tenga una autorización expresa.
- Se utilizan planillas para registrar la entrada y salida del personal externo del área al acceso de datos privados o sensibles.
- Se restringe el acceso físico a dispositivos como: puntos de acceso inalámbricos, puertas de enlace a redes y terminales de red que estén ubicadas en las áreas seguras.
- La conexión remota al computador o al software debe ser aprobada, registrada y auditada, por la administración de la empresa y exclusivamente en los casos establecidos en el contrato pactado.

3.9 POLITICAS DE MEDIDAS DE SEGURIDAD DE LA VIDEOVIGILANCIA:

Objetivo: Minimizar los riesgos de perdida de la información de las cámaras y suministro de la información

Procedimiento de medidas de seguridad.

- Restringir el acceso del personal a la información de las cámaras
- Cifrar la información y realizar auditorías periódicas
- Documentar los procesos de eliminación de la información
- Informar de los incidentes de seguridad a la Superintendencia de Industria y Comercio y a la administración de la empresa para el respectivo estudio y reparación si lo considera necesario.

Procedimiento de acceso a las grabaciones

- Verificar la calidad del titular, quien solicita las grabaciones mediante algún documento de identificación.
- Solicitar datos exactos de las grabaciones como fechas, horas, lugar para facilitar la ubicación de la imagen y limitar el máximo de la exposición de las imágenes con terceros.

- Solicitar autorización a los responsables y representantes de los menores de edad, si estos son visualizados en la grabación de las cámaras y con el único objetivo de salvaguardar los derechos fundamentales.

3.10 POLITICA AL ACCESO DE LA INFORMACIÓN DEL RECURSO HUMANO.

Objetivo: Garantizar que los datos sensibles relacionados con los datos de la salud, creencias religiosas, políticas, sexuales, entre otros de los trabajadores, datos de los hijos menores de edad solo puedan ser conocidos por el personal competente y pertinente en virtud de sus funciones, teniendo en cuenta el principio de Acceso Restringido.

Procedimiento:

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 de administración atendiendo las finalidades particulares autorizadas por el titular.

3.11 PROCEDIMIENTO DEL RECURSO HUMANO

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

- **PROCESOS DE SELECCIÓN:**

- La empresa 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 otorgue en las hojas de vida como referencias personales y profesionales, de igual manera los que se obtengan durante la realización del mismo.

- El tratamiento de los datos suministrados por los interesados en las vacantes de la empresa **LATAMSEC SECURITY LTDA.,** y los obtenidos del proceso de selección, será únicamente la informada en la autorización al aspirante.

- La empresa, contará con un proceso de eliminación de las hojas de vida de los aspirantes (titulares) sobre los que ya no se tenga interés en conservar contacto y los cual no reclamaran la respectiva hoja de vida, por un tiempo aproximado de un (1) mes.

- **VINCULACIÓN**:

- Una vez seleccionada un aspirante para ocupar un cargo en la empresa**,** se celebrará el respectivo contrato laboral o de prestación de servicios, acuerdo de confidencialidad y se le asignará cuando el cargo lo requiera usuarios y claves para el acceso a la información personal tratada por la empresa.

- Seleccionado el candidato para el cargo, la empresa almacenará los datos personales del trabajador o contratista en una carpeta identificada con el nombre de cada persona. A esta carpeta solo tendrá acceso el Área de recursos humanos o administración y con la finalidad de gestionar la relación entre la empresa y el trabajador o contratista.

- Para cuando la empresa 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.

- **DESVINCULACIÓN:**

- Una vez se termine el contrato de prestación de servicios, la empresa suscribirá un acuerdo de confidencialidad con el ex trabajador o contratista para salvaguardar la confidencialidad de la información personal manipulada por el ex contratista.

- Terminada la ejecución del contrato, la empresa igualmente procederá a almacenar los datos personales de sus extrabajadores o contratistas 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.

3.11 POLÍTICA DE TERCERIZACIÓN U OUTSOURCING

Objetivo: Mantener la seguridad de la información y los servicios de procesamiento de información, a los cuales tienen acceso terceras partes como contratistas, proveedores.

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 empresa. 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 empresa 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.

3.12 PROCEDIMIENTO PARA ENCARGADOS

Objetivo: 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.

Cuando la empresa 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.
- 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 empresa.
- Suscribir un contrato de transmisión de datos personales.

3.13 POLITICAS DE REVISIONES DE SEGURIDAD DE LA INFORMACIÓN

Objetivo: Garantizar el funcionamiento del sistema de gestión de seguridad de la información de acuerdo a las políticas procedimientos implementados en la empresa.

Procedimiento

Realizar auditorías con personal externo a la empresa, al sistema de gestión de seguridad de la información, para la verificación y cumplimiento de objetivos, controles, políticas y procedimientos de seguridad de la Información.

El administrador deberá realizar revisiones esporádicas no programadas con el fin verificar el cumplimiento de las políticas de seguridad de la información en las instalaciones de la empresa.

4 PROCESO PARA LA ATENCIÓN DE INCIDENTES

Objetivo: Asegurar que los eventos e incidentes de seguridad de la información, sean comunicados y atendidos oportunamente, con el fin de tomar oportunamente las acciones correctivas.

Procedimientos

Toda vez que se presente algún incidente con la seguridad de la información tratada por la empresa 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 administrador y responsable de Habeas Data en la empresa; 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 del administrador quien deberá realizarlo una vez haya sido notificados de la ocurrencia del mismo.

3). **Reunión del comité de Seguridad de la información:** El administrador encargado de la seguridad de la información, conformara de forma extraordinaria la reunión con el consejo de administración de medidas de seguridad para determinar la gravedad del incidente de seguridad en los siguientes términos:

- Hechos sucedidos para determinar las falencias, perjuicios que puede causar el incidente.
- Identificar por qué ocurrió el hecho, a quien afecto y que consecuencias traería el incidente
- Determinar qué medidas de seguridad podemos restablecer para que no vuelva a ocurrir el incidente y cómo podemos proteger los derechos a los titulares.

5 MODIFICACIÓN DE LAS POLÍTICAS

LATAMSEC SECURITY LTDA., 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 08 de mayo de 2020.