POLÍTICA DE SEGURIDAD DE DATOS PERSONALES

NUESTRA POLÍTICA DE SEGURIDAD DE NUESTROS DESARROLLOS PROPIOS

- Nuestros sistemas, para crear, modificar, mantener o transmitir los registros electrónicos emplearán controles diseñados para garantizar la autenticidad, integridad y, en su caso, la confidencialidad de los registros electrónicos.

- El control de acceso accede si solo y solo si las personas se encuentran autorizadas por el administrador del sistema y las características que giran alrededor de ellas, nuestro administrador de seguridad de la plataforma contiene las opciones para administrar la seguridad de la aplicación, su creación de usuarios, cambios de contraseña, bloqueos de usuarios, asignación de roles, creación de menús, mantenimientos de los servicios.

- Es de destacar que las contraseñas (password) son encriptadas en hash mediante MD5.

- En caso de logín fallido o bloqueo de cuenta, se genera el envío de e-mail del evento ocurrido al administrador de la aplicación, además del manejo de sesiones, activas, inactivas, trazas de auditoría que se registran en la tabla s_auditlog, el manejo a la política de vencimiento de contraseñas y roles para garantizar el acceso solo a los menús autorizados.

- Se generan copias de seguridad dos veces al día, las cuales son contenidas en un espacio destinado en el propio servidor y en un disco duro externo.

NUESTRA POLÍTICA DE SEGURIDAD PARA LAS BASES DE DATOS DE MARKETING.

- Vínculo de Cancelación de Suscripción.

En nuestro sistema para el marketing por correo electrónico, estamos obligados a cumplir con las leyes contra el spam. Esto significa que debemos incluir un vínculo de cancelación de suscripción en todas las campañas. No se trata sólo de que la Ley CAN-SPAM nos obligue a tener vínculos de cancelación de suscripción. Al usar el servicio de

envíos masivos, los proveedores de servicios de Internet (ISP) nos obligan a manejar las bases de datos de una manera determinada, así que tenemos que poder:

1. Manejar y eliminar automáticamente las suscripciones canceladas de la base de datos.

2. Procesar registros de devoluciones, cuando el servidor de correo electrónico de un suscriptor rechaza un mensaje, se denomina un rebote. Hay diferentes tipos de rebotes que dependen del motivo por el cual el correo electrónico fue rebotado. Estos detalles se pueden encontrar en los informes de las campañas, por lo que se tiene un control del número de devoluciones para asegurarte de que tus campañas llegan a los suscriptores y que estás cumpliendo las leyes contra el spam.

Todo el proceso se realiza de forma automática. Ya que enviar correo electrónico a alguien que ya ha cancelado su suscripción es una infracción de CAN-SPAM, donde nos aseguramos de que el proceso de cancelación de suscripción de todos nuestros usuarios se realice automáticamente. Debido a esto, todas las campañas enviadas a las bases de datos deben contener el vínculo de cancelación de suscripción.

3. El software de correos masivos utilizado por MM Programación se llama Mailchimp, el cual es reconocido en el mercado como una plataforma confiable y segura, la cual también contiene sus propias políticas de tratamiento de datos.

NUESTRA POLÍTICA DE SEGURIDAD PARA LAS BASES DE DATOS DE LOS EMPLEADOS.

Esta información se encuentra debidamente custodiada en nuestras instalaciones, con las siguientes medidas de seguridad, que corresponden a los documentos manejados por el Área de Recursos Humanos así:

1. Se encuentran archivadas en una oficina a la cual solo entra personal autorizado y de extrema confianza.
2. Contenidas en un archivador y en su respectiva carpeta, marcada y legajada para evitar pérdidas.