



24 de abril de 2024

BOLETÍN INFORMATIVO

Abril 2024



Se actualiza el Registro de Números Excluidos: Conoce sus implicaciones

A partir del 10 de abril de 2024, los ciudadanos pueden inscribirse en el Registro de Números Excluidos (RNE) para evitar recibir mensajes comerciales o publicitarios.

El Registro de Números Excluidos fue creado por la Resolución CRC 5050 de 2016 y recientemente modificado por la Ley 2300 de 2023, mediante la Resolución 7356 de 2024. El RNE es una plataforma administrada por la Comisión de Regulación de Comunicaciones en la que los ciudadanos pueden inscribirse para evitar recibir contenido de carácter comercial o publicitario. La actualización al RNE implica los siguientes cambios: primero, adapta el

Registro a los nuevos canales de contacto establecidos por la Ley 2300 de 2023 (ley “deje de fregar”), pues se incluyó la mensajería por aplicaciones o web, correos electrónicos y llamadas telefónicas. Segundo, se modificaron los horarios en los que se pueden realizar contactos comerciales o publicitarios de acuerdo con lo dispuesto en la Ley 2300 de 2023. El horario es de lunes a viernes de 7:00 a 7:00 p.m. y los sábados de 8:00 a 3:00 p.m., excluyendo cualquier contacto con el consumidor los domingos y festivos. Tercero, los productores y proveedores de bienes y servicios en Colombia deben consultar el Registro antes de contactar a los consumidores, con el fin de evitar el envío de comunicaciones a aquellos que se hayan registrado en la plataforma.

Aunado a lo anterior, todas las empresas que proveen productos y servicios están obligadas a consultar el RNE. Además, deben revisar y actualizar regularmente sus bases de datos para evitar enviar mensajes a usuarios inscritos en el RNE y cumplir con el horario mencionado para el envío de publicidad. Finalmente, la inscripción en el RNE no se aplica a los contactos destinados a informar al consumidor sobre la confirmación oportuna de operaciones monetarias realizadas, ahorros voluntarios y cesantías, enviar información solicitada por el consumidor o generar alertas sobre transacciones fraudulentas, inusuales o sospechosas. En definitiva, es importante que las empresas cumplan con estas obligaciones y eviten posibles investigaciones y sanciones por parte de la Superintendencia de Industria y Comercio.



Fuerte sanción: Multa por recopilación indebida de datos biométricos

La Agencia Española de Protección de Datos (AEPD) impuso una multa de 365.000 euros a la empresa CTC Externalización, por solicitar la huella dactilar a sus empleados para marcar su ingreso, sin informar adecuadamente sobre la recopilación de datos biométricos ni implementar medidas de seguridad suficientes.

En este caso, la AEPD consideró que la empresa había infringido los artículos 13, 32 y 35 del Reglamento General de Protección de Datos (RGPD), debido a que no contaba con el consentimiento de los titulares, no informó correctamente sobre el tratamiento de estos datos y los almacenaba en el portal del empleado sin otorgar ninguna privacidad o seguridad frente a su consulta. Además de la multa, la sanción incluyó un plazo de seis meses para que la empresa informara adecuadamente a los trabajadores, estableciera medidas de seguridad, garantizara la eliminación de las huellas tras su captura y realizara una evaluación de impacto.

Esta noticia nos recuerda la importancia de proteger la privacidad y de tener

especial cuidado con el manejo de datos biométricos, los cuales solo pueden ser tratados con la autorización previa, expresa e informada del titular. Asimismo, ejemplifica la necesidad de que las empresas que manejan este tipo de información cumplan con las leyes de protección de datos y garanticen los derechos de los titulares. En VMC, estamos disponibles para asesorarte en el tratamiento de datos biométricos y orientarte para realizar una adecuada gestión de los mismos.



¿Cómo medio segundo marcó la diferencia en la seguridad digital?

Andrés Freund, ingeniero de software, evitó un ciberataque al notar una leve demora de medio segundo en la carga de un programa durante una rutina de mantenimiento. Este ingeniero, empleado de Microsoft y dedicado al desarrollo de software, descubrió una puerta trasera oculta en un programa del sistema operativo Linux, la cual podría haber

dado acceso remoto a millones de dispositivos en todo el mundo.

Freund detectó el problema al observar un aumento en el uso de la capacidad del procesador y una pequeña demora en el acceso al programa, los cuales fueron signos de alarma que, después de un análisis, lo llevaron a descubrir un posible ataque de cadena de suministro. Si hubiera pasado desapercibida, esta puerta trasera habría permitido a sus creadores obtener una clave maestra para acceder a los computadores que ejecutan este programa.

Es por ello esencial que las empresas cuenten con programas de datos personales y seguridad de la información que sean efectivos, que incluyan alertas tempranas, así como la vigilancia y monitoreo constante de sus plataformas, pues incluso comportamientos ligeramente diferentes pueden ser indicadores de la existencia de vulnerabilidades. También es fundamental contar con auditorías externas, que permitan evaluar la efectividad de los programas con una visión diferente a la de la misma empresa. La rapidez en la detección y respuesta puede ser clave para evitar la materialización de riesgos, que pueden conllevar graves consecuencias, e incluso sanciones. Si tienes dudas sobre el manejo preventivo o correctivo de los incidentes de seguridad de la información que puedan tener efectos sobre datos personales, en VMC estamos a tu disposición para ayudarte.



¿Está seguro de que el modo incógnito no guarda información?

Google acordó eliminar millones de registros de datos web recopilados en el modo incógnito de Chrome para evitar una demanda colectiva de 2020. Los demandantes habían acusado a la empresa de obtener información de forma ilegal en búsquedas privadas en internet. Para evitar la demanda de 5.000 millones de dólares por rastrear y recopilar datos en los modos privados de Chrome, Safari y otros navegadores, Google acordó divulgar cómo recopila información en el modo incógnito, establecer límites para futuros almacenamientos, eliminar los datos recogidos hasta diciembre de 2023 y permitir a los usuarios bloquear cookies de terceros en modo incógnito.

Esta es una lección sobre la importancia de respetar la privacidad de los usuarios y no recopilar su información sin obtener su autorización. Asimismo, nos recuerda la importancia de honrar la expectativa de privacidad de los titulares, pues las empresas deben garantizar que las promesas de valor hacia sus usuarios se cumplan en la realidad. Informar debidamente a los titulares sobre los procesamientos que se harán sobre sus datos personales es un principio esencial para cumplir debidamente con la reglamentación sobre protección de datos personales. Así, es fundamental que las empresas actúen con transparencia y

ética en la recopilación y uso de datos, asegurándose de cumplir con la ley y de respetar los derechos de los titulares.



Contáctenos

Teléfono: 3174416313

Correo electrónico: svanegas@vanegasmorales.com