Términos y Condiciones

TÉRMINOS Y CONDICIONES

XENTRAL ALERT

Contenido

1. Acerca del sistema

XENTRAL ALERT, es una plataforma web diseñada para hacer más conscientes a las personas sobre los múltiples riesgos que pueden ser encontrados al navegar digitalmente, hacer uso de servicios en línea, recibir solicitudes por parte de terceros y al proporcionar datos sensibles e información aprovechable para actos delictivos e ingeniería social. La finalidad de XENTRAL ALERT es influenciar los hábitos de comportamiento digital, para así generar barreras de protección que disminuyan el riesgo frente al accionar de los ciber-delincuentes.

XENTRAL ALERT, cuenta con un proceso de perfilamiento, una puntuación digital, un módulo de aprendizaje, un panel de análisis de conectividad, un buscador de datos filtrados en la Deep Web, monitoreo de datos filtrados a la Dark Web y servicio de atención / soporte.

2. Datos que se solicitan al usuario para el proceso de registro

Para poder hacer uso de la plataforma, se deberá suministrar: nombre y apellido, un número de identificación, correo electrónico y número de teléfono. Hay casos en los que la asignación de la contraseña para el primer ingreso, se puede realizar por parte del prestador del servicio y, en toda ocasión, el usuario podrá configurar su clave definitiva tan pronto como haya culminado el proceso de onboarding.

Estos datos pueden ser suministrados directamente por el usuario o por la compañía que proporcione el producto como parte de una oferta de servicios adherida. Siempre se garantizará transparencia en el manejo y uso de la información, velando por el resguardo de los datos sensibles.

El único dato que no se solicita de forma mandatoria dentro del proceso de registro, es el serial de la tarjeta débito o crédito que la persona desee vincular para monitoreo en la Deep Web. El usuario podrá siempre decidir si desea asociar este ítem a su cuenta o no.

3. Conceptos clave

A. **Dark Web:** Es un término utilizado para referirnos a portales en donde tienen cabida actos ilícitos y a los que solo se puede acceder haciendo uso de navegadores especializados. Este término reúne al conjunto de portales que no están indexados y que se escapan al alcance de los navegadores comunes.
B. **Deep Web:** Si bien se suele confundir con frecuencia este concepto con el de Dark Web, se debe saber que este término es usado para referirnos a todos aquellos sitios en la internet mundial que no se encuentran indexados por los motores tradicionales de consulta y que engloba a la Dark Web. La Deep Web es mucho más grande ya que contiene portales que no necesariamente están vinculados a actos al margen de la ley. Se cree que cerca del 90% del contenido en todo internet yace en la Deep Web**.**
C. **Datos en tránsito:** Este término se usa para indicar cualquier modo de información digital que es transmitido de un sistema a otro.
D. **Datos en reposo:** Hace referencia al conjunto de datos que se encuentran almacenados en una base de datos.

4. Servicios que presta la plataforma al usuario

El sistema cuenta con los siguientes recursos:

A. Formulario de conocimiento de hábitos digitales

Es un cuestionario que permite establecer cuáles son las acciones que por parte del usuario son tenidas en cuenta, para la realización de actividades en línea. Este proceso se debe completar para conocer la calificación del perfil y poder conocer las recomendaciones que se deben atender para empezar a tener mayores controles a nivel de seguridad.

B. Calificación del perfil digital del usuario

Es un indicador que permite establecer qué tan seguro o inseguro puede ser el perfil de un usuario, tras conocer sus hábitos de cuidado digital. Esta puntuación considera las respuestas suministradas por las personas, así como variables técnicas que posibilitan establecer un rango de criticidad. La puntuación mejorará cada vez que el usuario mejore la seguridad de su ecosistema e interactúe con las opciones disponibles en el panel de aprendizaje.

C. Análisis ilimitado de conectividad

Es un servicio en el cual se determina si la conexión a internet que usa el usuario para acceder al sistema es segura o insegura. Este servicio es ilimitado, toda vez que el usuario puede someter a análisis el número de conexiones que desee, ideal si se hace uso de redes públicas de Wi-Fi en aeropuertos, cafeterías, zonas de alto tránsito y afines. En caso de presentarse un resultado de conexión insegura, se podrá hacer uso del chat de soporte para solicitar orientación y apoyo.

Al elegir la opción "Nuevo análisis", el sistema le informará al usuario el ID de la conexión evaluada y el resultado respectivo (Segura / Insegura).

D. Monitoreo de datos en la Dark Web

El sistema permite monitorear en los registros filtrados de la Dark Web si el correo electrónico, el número de identificación y el número de teléfono de un usuario han sido expuestos por parte de terceros. Este servicio de la plataforma inicia una vez el usuario se ha registrado y ha asociado sus datos.

E. Búsqueda de información filtrada a la Deep Web

XENTRAL ALERT cuenta con un buscador para identificar datos filtrados a la Deep Web. El usuario deberá leer la información del módulo de consulta y elegir la opción "Nuevo análisis" para iniciar el proceso. En toda ocasión, sin excepción alguna, el usuario deberá confirmar sus datos y aceptar los requisitos para ejecutar la búsqueda. Tras finalizar el análisis, se suministrará en el mismo módulo una tabla con los resultados de la inspección, mismos que serán notificados de forma complementaria vía correo electrónico.

En caso de que se presenten filtraciones, el usuario podrá hacer clic en la alerta respectiva para conocer las fechas de filtración y los sitios en donde fueron publicados los datos.

F. Panel de aprendizaje

La plataforma cuenta con un panel que aloja información de utilidad para conocer medidas que pueden facilitar la implementación de controles de seguridad por parte del usuario. Lo anterior, con el objetivo de ayudar a las personas en la reducción de riesgos al navegar digitalmente y hacer uso de servicios en línea.

El usuario podrá filtrar las recomendaciones de acuerdo con el nivel de criticidad.

G. Asistencia remota y soporte

XENTRAL ALERT cuenta con canales de asistencia y soporte a través de los cuales el usuario recibirá orientación en el uso del sistema, acompañamiento

en caso de detección de amenazas y resolución de inconvenientes asociados a la promesa de servicio. Estos canales, dependiendo del plan, pueden ser: ventana de chat, línea de llamada y un buzón de correo electrónico. Estos medios pueden ser encontrados al ingresar a la plataforma, en el panel lateral.

Nota: Puede haber configuraciones del producto que no cuenten con canales de atención.

H. **Sistema de información para notificaciones**

En caso de que se requiera emitir una notificación al usuario para la activación de su cuenta, informar acerca de una amenaza o comunicar algún particular asociado a la prestación del servicio, se activará el sistema de información de la plataforma, el cual hace uso del correo asociado al registro de la cuenta.

5. Alcance del servicio

A. Cada licencia de la plataforma otorga acceso a los servicios descritos en el apartado 4 de estos Términos y Condiciones. La vigencia del producto puede ser mensual o anual, según sea convenido y aceptado entre las partes. La vigencia del producto será informada al usuario con la adquisición del producto que da acceso al sistema.
B. La versión estándar de cada licencia permite alojar: 1 nombre de usuario, 1 correo electrónico, 1 número de teléfono, 1 número de identificación y 1 tarjeta débito o crédito. Puede haber ocasiones en donde el producto brinde mayor cobertura y permita asociar mayores cantidades en cada ítem, previa notificación del operador del servicio.
C. El análisis de filtraciones para tarjeta débito o crédito está disponible para la Deep Web.
D. El análisis de conectividad es un servicio ilimitado, es decir, puede operar para analizar cuantas conexiones a internet requiera el usuario.
E. Se resalta que no hay sistema que garantice protección al 100% y que XENTRAL ALERT no es un producto tipo antivirus. El servicio que se presta a través de esta plataforma es de carácter orientativo y ayuda a los usuarios a mitigar riesgos, pero sin ser infalible respecto a múltiples modalidades de amenaza digital.
F. En toda ocasión es responsabilidad del usuario acogerse a las recomendaciones de seguridad suministradas por XENTRAL ALERT. Si no se toman medidas de seguridad frente a vulnerabilidades identificadas o

manifiestas, no se podrá garantizar de forma alguna que el usuario pueda contar con un ecosistema de información digital más protegido.

G. El sistema no está sujeto a peticiones de modificación a nivel estructural o funcional por parte del usuario.
H. La URL autorizada para acceder a la plataforma XENTRAL ALERT es xentralalert.com.
I. El prestador del servicio podrá realizar modificaciones a nivel técnico y funcional, con el objetivo de brindar una mejor experiencia en el uso de los diferentes módulos del entorno de prevención. En caso dado que estas modificaciones lleguen a representar indisponibilidad en el sistema, se notificará a las personas de forma oportuna.
J. Para poder operar a cabalidad el servicio, el usuario deberá suministrar toda la información marcada como requerida en el proceso de registro, de lo contrario no se garantiza la activación de los beneficios de la oferta de valor.
K. Cada licencia es de uso personal e intransferible.

6. Sobre el operador del servicio

XENTRAL ALERT es un producto de Continental Assist LLC., una compañía global de asistencia, cuya Casa Matriz se encuentra ubicada en 20803 Biscayne Boulevard, suite 370, Aventura, Florida - Estados Unidos (código postal: 33009).

La tecnología sobre la cual opera XENTRAL ALERT es propiedad de LAZARUS TECHNOLOGY S.L., cuya sede principal se encuentra ubicada en Calle del Teide, Nº5 (Edificio Milenio), Tercera Planta, San Sebastián de los Reyes, Provincia de Madrid – España (código Postal 28703).

7. Canales de contacto

Los canales de soporte y asistencia remota se encuentran disponibles para el usuario las 24 horas del día, todo el año. A través del módulo de contacto del sistema, los usuarios podrán solicitar apoyo vía chat, llamada o correo electrónico. A continuación, se presentan las rutas oficiales para el envío de requerimientos:

- **La línea autorizada para llamadas es:** (+34) 910781923

- **Correo electrónico oficial:** support@xentralalert.com

  Nota: la opción de chat está embebida en la plataforma y solo se podrá acceder a ella si se está al interior del sistema.

En caso de que se deba contactar al usuario, se hará uso de los medios que este dejó asociados a su registro de servicio. El medio principal de notificación será el correo electrónico.

8. Terminación del servicio

El servicio se dará por terminado cuando:

A. Se culmine la vigencia establecida y no se haya solicitado renovación.
B. El usuario solicite de forma expresa la cancelación.
C. El prestador del servicio lo notifique, atendiendo a eventos que impidan la continuidad en la operación del sistema. Para estos casos, se informará de forma anticipada sobre los hechos suscitados que deriven en este evento.

9. Seguridad y resguardo de la información

Toda la información que el usuario suministra para la prestación del servicio, es almacenada de forma segura en nuestra base de datos y solo se utiliza para los efectos propios de estos Términos y Condiciones.

XENTRAL ALERT, opera sobre la infraestructura cloud de OVH, con servidores dedicados. Esta infraestructura garantiza respaldo y continuidad del negocio, además de altos estándares de seguridad.

Se usan protocolos de cifrado de última generación para garantizar el mayor nivel de resguardo.

A. **Cifrado para datos en reposo**
   Se usa el protocolo de Cifrado Simétrico AES-256-CBC. El cifrado es el proceso de transformar datos legibles (texto plano) en un formato codificado (texto cifrado) que solo puede ser descifrado por alguien que posea la clave secreta adecuada. Este

proceso es fundamental para garantizar la confidencialidad y seguridad de los datos durante su almacenamiento y transmisión.

El cifrado simétrico utiliza la misma clave tanto para cifrar como para descifrar los datos. Este método es eficiente y rápido, lo que lo convierte en una opción popular para la protección de datos. Algunos ejemplos de cifrado simétrico incluyen AES (Advanced Encryption Standard) y DES (Data Encryption Standard).

AES (Advanced Encryption Standard) es un estándar de cifrado simétrico ampliamente adoptado por el gobierno de los Estados Unidos y diversas organizaciones globales debido a su alta seguridad. AES-256 se refiere al uso de una clave de 256 bits, proporcionando un nivel robusto de seguridad.

CBC (Cipher Block Chaining) es un modo de operación de cifrado que añade un vector de inicialización (IV) a cada bloque de texto plano. Este IV garantiza que bloques idénticos de texto plano se cifren en bloques de texto cifrado diferentes, añadiendo una capa adicional de seguridad. El uso combinado de AES-256 con CBC (AES-256-CBC) asegura que los datos cifrados sean altamente seguros y resistentes a los ataques de criptoanálisis.

B. Cifrado para datos en tránsito

Siempre se hace uso del Cifrado En Tránsito: TLS 1.2 o Superior. El cifrado en tránsito es el proceso de proteger los datos mientras se transfieren a través de redes, tanto públicas comp privadas. Esto es crucial para evitar que los datos sean interceptados o manipulados durante su transmisión. Para asegurar la integridad y confidencialidad de los datos en tránsito, utilizamos Transport Layer Security (TLS) versión 1.2 o superior.

TLS es un protocolo criptográfico diseñado para proporcionar comunicaciones seguras a través de una red. TLS 1.2 y las versiones superiores ofrecen mejoras significativas en seguridad y eficiencia en comparación con las versiones anteriores. Estas mejoras incluyen algoritmos de cifrado más robustos y la eliminación de vulnerabilidades conocidas en versiones anteriores.

C. Mecanismos de Seguridad Adicionales

- **Prohibición de Downgrade de TLS:** No permitimos el downgrade a versiones anteriores de TLS. Esto significa que las conexiones deben usar TLS 1.2 o superior, asegurando que las comunicaciones se beneficien de las últimas mejoras en seguridad.
- **Certificados Firmados por Autoridades de Certificación Confiables:** Utilizamos certificados digitales firmados por autoridades de certificación (CA) de confianza. Estos certificados validan la identidad de nuestros servidores y aseguran a los usuarios que están conectándose a un servidor legítimo.

10. Sobre la aceptación de estos Términos y Condiciones

Al aceptar estos Términos y Condiciones se da por establecida la relación contractual necesaria para la prestación del servicio de acompañamiento preventivo. El usuario declara conocer, aceptar y acogerse a todos los puntos cubiertos en el presente documento.

11. Resolución de disputas jurídicas y legislación aplicable a estos Términos y Condiciones

En caso de presentarse una disputa, se debe saber por parte del usuario que estos Términos y Condiciones se rigen por la legislación de Estados Unidos, específicamente las aplicables al Estado de la Florida.


Xentral
Alert