easyCRM

Introducción

Es una plataforma que permite gestionar de forma simple, ágil y rápida todos tus clientes potenciales provenientes de distintas plataformas de prospección en tiempo real.

Con easyCRM aumenta el % de conversión gracias a una interfaz intuitiva y una gestión eficiente de tus clientes potenciales, sin perder ni un solo dato.

Es un solución a medida que se ajustará a las reglas de tu negocio.

Nuestro ADN

01 Personalización

02 Facilidad

03 Tiempo real

04 Integración

Análisis de riesgo de ciberseguridad

1) Confidencialidad y protección de datos personales.

Como proveedor de servicios de software, en Navegapp nos comprometemos a garantizar la seguridad y confidencialidad de la información de nuestros clientes y colaboradores internos y externos. En este sentido, hemos establecido una definición documentada sobre el tratamiento de la información confidencial o restringida, considerando los principios fundamentales de la seguridad de la información: confidencialidad, disponibilidad e integridad.

Política de Ciberseguridad

Definición de Información Confidencial

En Navegapp, consideramos que la información confidencial es cualquier dato que pueda comprometer la seguridad o privacidad de nuestros clientes, colaboradores internos y externos, o de nuestra propia empresa. Esto incluye, pero no se limita a, información financiera, datos personales, estrategias comerciales, y cualquier otra información sensible relacionada con nuestros servicios y operaciones.

Responsabilidades del Personal

Es responsabilidad de cada empleado de Navegapp proteger la información confidencial y restringida a la que tenga acceso en el curso de sus funciones. Esto incluye mantener la confidencialidad de la información, protegerla de accesos no autorizados, y seguir los procedimientos establecidos para su manejo seguro.

Gestión de Riesgos

Navegapp se compromete a identificar y evaluar continuamente los riesgos de seguridad de la información que puedan afectar a nuestra empresa y a nuestros clientes. Para ello, realizamos análisis periódicos

de riesgos y tomamos medidas proactivas para mitigarlos y gestionarlos de manera efectiva.

Incidentes de Seguridad

En caso de producirse un incidente de seguridad que ponga en riesgo la confidencialidad, disponibilidad o integridad de la información, Navegapp tomará medidas inmediatas para contener y remediar la situación. Esto incluye la notificación oportuna a las partes afectadas y la implementación de medidas correctivas para evitar la recurrencia.

Política de Manejo y Clasificación de la Información

Identificación y Clasificación de la Información

En Navegapp, clasificamos la información según su nivel de sensibilidad y relevancia para nuestras operaciones y servicios. Esto nos permite aplicar controles de acceso adecuados y garantizar la protección adecuada de la información en todo momento. La clasificación de la información se basa en criterios como la confidencialidad, la criticidad y la legalidad.

Acceso y Manejo Seguro de la Información

Todo el personal de Navegapp tiene la responsabilidad de acceder y manejar la información de manera segura y responsable. Esto incluye seguir los procedimientos establecidos para el acceso a la información, proteger los dispositivos y sistemas utilizados para procesar la información, y utilizar medidas de seguridad adicionales cuando sea necesario para garantizar la confidencialidad e integridad de la información.

Destrucción Segura de la Información

Navegapp tiene protocolos establecidos para la destrucción segura de la información obsoleta o no necesaria. Esto incluye la eliminación permanente de los datos de acuerdo con las mejores prácticas de seguridad y cumplimiento legal.

Política de Protección de Datos

Principios de Protección de Datos

Navegapp se compromete a cumplir con los principios de protección de datos establecidos por las leyes y regulaciones aplicables. Esto incluye el principio de consentimiento informado, minimización de datos, exactitud de la información, limitación del almacenamiento, integridad y confidencialidad de los datos personales.

Manejo de Solicitudes de Acceso y Rectificación

Navegapp reconoce el derecho de los individuos a acceder, rectificar y eliminar sus datos personales según lo establecido por las leyes de protección de datos. Por lo tanto, hemos implementado procedimientos para manejar las solicitudes de acceso y rectificación de manera oportuna y eficiente.

Medidas de Seguridad Técnicas y Organizativas

Navegapp utiliza medidas de seguridad técnicas y organizativas para proteger los datos personales contra accesos no autorizados, pérdida, alteración o divulgación. Esto incluye el uso de firewalls, cifrado de datos, controles de acceso, políticas de contraseña y capacitación del personal en seguridad de la información.

2) Notificación sobre incidentes de seguridad

El procedimiento de respuesta a incidentes tiene como objetivo establecer una guía clara y eficaz para el manejo de cualquier incidente de seguridad que pueda afectar los activos de información de nuestros clientes o los servicios que proporcionamos.

- Detección del Incidente: Identificación y notificación del incidente por parte del personal autorizado.
- Evaluación Inicial: Determinación del alcance y gravedad del incidente.

- Contención y Mitigación: Implementación de medidas para detener la propagación del incidente y minimizar su impacto.
- Investigación y Análisis: Recopilación de información relevante para comprender la naturaleza y origen del incidente.
- Notificación: Comunicación oportuna a los afectados y autoridades pertinentes según lo requieran las leyes y regulaciones aplicables.
- Recuperación: Restauración de los sistemas afectados a un estado seguro y funcional.
- Seguimiento y Mejora: Análisis post-incidente para identificar lecciones aprendidas y acciones correctivas para prevenir incidentes similares en el futuro.

Protocolo Comunicacional para la Gestión de Incidentes de Seguridad

Objetivo

El objetivo de este protocolo es establecer un proceso claro y eficiente para informar a las partes interesadas sobre las violaciones de seguridad de la información y las medidas adoptadas para abordarlas, incluso en ausencia de evidencia de impacto en los servicios o exposición de activos de información.

Procedimiento

a. Detección del Incidente:

Todo incidente de seguridad de la información será detectado y reportado inmediatamente al equipo de seguridad de la información de Navegapp por parte del personal autorizado o mediante sistemas de detección automática.

b. Evaluación Inicial:

El equipo de seguridad de la información realizará una evaluación inicial del incidente para determinar su gravedad, impacto potencial y las medidas inmediatas que deben tomarse.

c. Comunicación Interna:

Se notificará de inmediato a las partes internas relevantes, incluidos los líderes de equipo y los responsables del área afectada, sobre la naturaleza del incidente y las acciones iniciales tomadas para abordarlo.

d. Comunicación Externa:

Se designará un portavoz oficial de Navegapp para comunicarse con las partes interesadas externas, incluidos los clientes afectados, en caso de que el incidente tenga un impacto significativo en sus servicios o datos.

Se proporcionará una comunicación clara y transparente sobre la naturaleza del incidente, las medidas correctivas tomadas y las recomendaciones para mitigar cualquier riesgo asociado.

e. Registro y Documentación:

Se mantendrá un registro detallado de todos los incidentes de seguridad de la información, incluidos los informes de incidentes, acciones tomadas, comunicaciones realizadas y cualquier otra información relevante.

La documentación asociada al protocolo comunicacional estará disponible para su revisión y auditoría en cualquier momento.

3) Control y gestión de acceso lógico

Implantación de Proceso de Autorización de Cuentas

Se establecerá un proceso formal y documentado para la creación, modificación y eliminación de cuentas de usuario en los sistemas de información de Navegapp.

Todo proceso de autorización de cuentas requerirá la aprobación previa por parte de un supervisor o responsable designado, quien verificará la necesidad y los privilegios asociados a la cuenta solicitada.

Controles para el Personal que Abandona la Empresa

Todo acceso lógico utilizado por un empleado que abandona la empresa será revocado de manera inmediata y completa.

Se eliminarán todos los accesos lógicos utilizados para prestar servicios en un plazo máximo de 24 horas a partir de la fecha de cese del empleado.

Los accesos lógicos secundarios, que no estén directamente relacionados con la prestación de servicios esenciales, serán eliminados en un plazo máximo de siete días desde la fecha de cese del empleado.

Procedimiento para Implementar la Política:

a. Solicitud de Acceso:

Todo empleado que requiera acceso a los sistemas de información de Navegapp deberá completar un formulario de solicitud de acceso, especificando los privilegios necesarios para desempeñar sus funciones.

La solicitud será revisada y aprobada por el supervisor o el departamento de recursos humanos antes de proceder con la creación de la cuenta.

b. Registro de Accesos:

Se llevará un registro actualizado de todos los accesos lógicos concedidos a los empleados, incluidos los privilegios asociados y la fecha de creación.

Este registro estará disponible para su revisión periódica por parte del equipo de seguridad de la información de Navegapp.

c. Proceso de Revocación:

En caso de cese de un empleado, el departamento de recursos humanos notificará de inmediato al equipo de seguridad de la información para proceder con la revocación de los accesos lógicos correspondientes.

Se realizará una revisión exhaustiva de los accesos lógicos del empleado y se procederá con la eliminación inmediata de aquellos relacionados con la prestación de servicios.

d. Seguimiento y Auditoría:

Se llevará a cabo una auditoría regular de los accesos lógicos para garantizar el cumplimiento continuo de esta política.

Se identificarán y corregirán de manera proactiva cualquier desviación o incumplimiento de los procedimientos establecidos.

Cumplimiento y Responsabilidades:

Todos los empleados de Navegapp son responsables de cumplir con esta política y de cooperar plenamente en la implementación de los controles de acceso lógico.

El departamento de recursos humanos y el equipo de seguridad de la información colaborarán estrechamente para garantizar el cumplimiento de esta política y la protección de los activos de información de la empresa.

Implementación de Mecanismos Tecnológicos:

Hemos implementado sistemas de control de acceso basados en roles y permisos, utilizando tecnologías de última generación para garantizar la seguridad y la trazabilidad de los accesos de los usuarios.

Evidencia de la Implementación:

Proporcionamos capturas de pantalla de nuestro panel de control de acceso, donde se muestra en tiempo real la actividad de los usuarios, incluyendo inicio de sesión, cambios de permisos y acciones realizadas.

Procedimiento o Norma de Accesos Lógicos:

Hemos desarrollado un procedimiento detallado de gestión de accesos que abarca desde la solicitud inicial de acceso hasta su revocación. Este procedimiento incluye formularios estandarizados para solicitar acceso, procesos de aprobación por parte de los responsables designados y auditorías periódicas para garantizar el cumplimiento de las políticas de seguridad de la información.
Mecanismos de Control de Acceso a la Red Interna

a. Autenticación de Usuarios:

Todos los usuarios que intentan acceder a la red interna deben autenticarse mediante un nombre de usuario y una contraseña.

Se requieren credenciales válidas y autorizadas para acceder a los recursos de la red.

b. Control de Acceso Basado en Roles (RBAC):

Se asignan roles específicos a los usuarios y dispositivos basados en sus funciones y responsabilidades en la organización.

Los permisos de acceso se otorgan de acuerdo con estos roles, restringiendo el acceso a recursos sensibles según sea necesario.

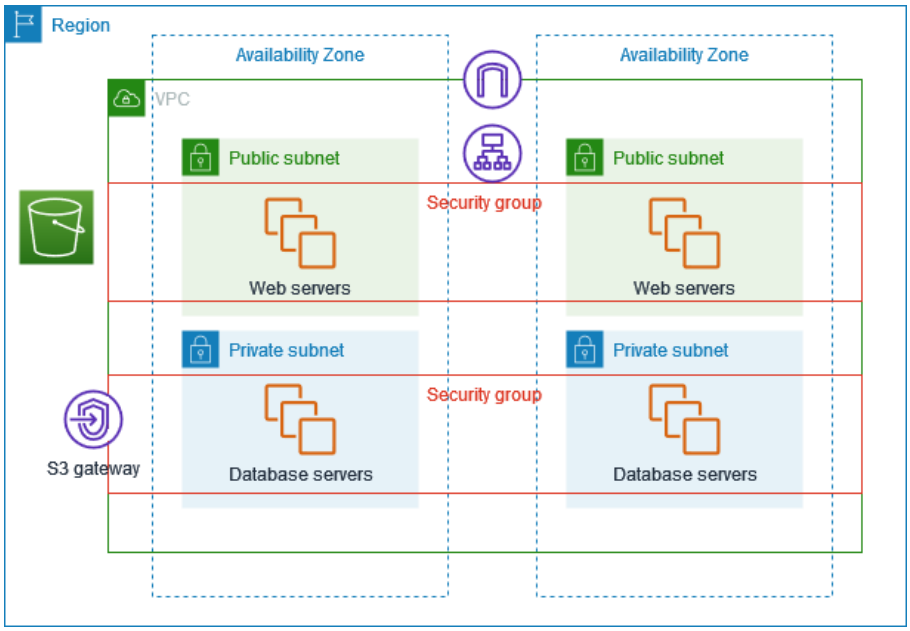
c. Firewalls y Seguridad Perimetral:

Se utilizan firewalls y otras medidas de seguridad perimetral para proteger la red interna contra accesos no autorizados desde el exterior.

Se establecen reglas de firewall para controlar el tráfico entrante y saliente, y se monitorean de forma continua para detectar y prevenir posibles amenazas.

Evidencia de Implementación

Adjunto encontrarás un print de pantalla que muestra el proceso de autenticación al ingresar a la red interna de Navegapp.



4) Instalación de actualizaciones y parches de seguridad

Proceso de Identificación y Mitigación de Vulnerabilidades:

Detección de Vulnerabilidades:

Implementamos herramientas de escaneo de vulnerabilidades en nuestros sistemas y redes para identificar posibles puntos de vulnerabilidad.

Estas herramientas realizan escaneos periódicos en busca de vulnerabilidades conocidas en el software, sistemas operativos y configuraciones de red.

Priorización de Vulnerabilidades:

Las vulnerabilidades identificadas se clasifican y priorizan según su gravedad y el impacto potencial en nuestros sistemas y datos.

Utilizamos criterios específicos para determinar qué vulnerabilidades deben abordarse primero, considerando el riesgo y la criticidad para nuestras operaciones.

Aplicación de Parches y Actualizaciones:

Se establece un proceso para aplicar parches y actualizaciones de seguridad de manera oportuna y eficiente.

Las actualizaciones críticas se implementan de inmediato para mitigar el riesgo de explotación, mientras que las actualizaciones menos críticas se programan en función de su impacto en las operaciones.

Monitoreo Continuo:

Se realiza un monitoreo continuo de nuestros sistemas y redes para detectar cualquier actividad sospechosa o intento de explotación de vulnerabilidades.

Se establecen alertas y notificaciones para informar al equipo de seguridad sobre posibles incidentes de seguridad que requieran una respuesta inmediata.

Proceso de Evaluación de Seguridad

Planificación Proactiva:

En Navegapp, nos esforzamos por mantener la seguridad y la integridad de nuestros sistemas y aplicaciones.

Implementamos un enfoque proactivo para evaluar y mitigar los posibles riesgos de seguridad.

Evaluación Cuidadosa:

Realizamos evaluaciones minuciosas de nuestras soluciones utilizando herramientas avanzadas de análisis.

Nuestro equipo interno lleva a cabo análisis exhaustivos para identificar posibles vulnerabilidades.

Acciones Correctivas Responsables:

Tomamos medidas responsables y oportunas para abordar cualquier vulnerabilidad identificada durante nuestras evaluaciones.

Implementamos soluciones efectivas para garantizar la seguridad y la protección de nuestros sistemas y datos.

Compromiso con la Seguridad:

Nos comprometemos a mantener la confianza de nuestros clientes y a salvaguardar la integridad de sus datos.

Aunque no contamos con especialistas externos en seguridad, nuestro equipo está dedicado a garantizar la seguridad de nuestras soluciones mediante un enfoque diligente y responsable.

Informes de Análisis de Vulnerabilidades

En Navegapp, nos comprometemos a garantizar la seguridad y la integridad de nuestros sistemas y servicios. Aunque no contamos con especialistas externos en seguridad, empleamos herramientas avanzadas, como los servicios de CloudWatch de AWS, para monitorear y analizar continuamente nuestra infraestructura en la nube. Estos servicios nos permiten detectar y evaluar posibles vulnerabilidades en tiempo real, ayudándonos a identificar áreas de mejora y a tomar medidas correctivas proactivas.

Evidencia de Análisis de Vulnerabilidades

Proporcionamos informes detallados generados por nuestros servicios de CloudWatch de AWS, que muestran los hallazgos de seguridad identificados durante los análisis de vulnerabilidades.

Estos informes incluyen recomendaciones claras para mitigar cualquier vulnerabilidad detectada, lo que demuestra nuestro compromiso con la seguridad y la protección de la información de nuestros clientes

Procedimientos para Reportar Problemas y Vulnerabilidades:

En Navegapp, nos esforzamos por garantizar la seguridad y protección de los datos de nuestros clientes. Para ello, hemos implementado procedimientos rigurosos para reportar cualquier problema o vulnerabilidad que pueda surgir en nuestros sistemas. A continuación, presentamos ejemplos concretos de cómo abordamos incidentes de seguridad en el pasado:

a. Vulnerabilidad en la Autenticación de Usuarios:

   - Identificación: Nuestro equipo de seguridad detectó una vulnerabilidad en el sistema de autenticación que podría permitir el acceso no autorizado a cuentas de usuario.
   - Evaluación: Se realizó una evaluación exhaustiva del impacto potencial de la vulnerabilidad en nuestros servicios y la información del cliente.
   - Comunicación: Se notificó de inmediato a los clientes afectados sobre la vulnerabilidad y se les proporcionaron recomendaciones para mitigar el riesgo.
   - Resolución: Trabajamos en estrecha colaboración con nuestro equipo de desarrollo para implementar una solución que parcheará la vulnerabilidad y fortaleciera la seguridad del sistema.

b. Exposición de Datos Sensibles:

- Identificación: Se detectó una exposición potencial de datos sensibles debido a una configuración incorrecta en uno de nuestros servidores de bases de datos.
- Evaluación: Se evaluó el alcance y la gravedad de la exposición para determinar el riesgo para nuestros clientes y sus datos.
- Comunicación: Se informó de inmediato a los clientes afectados sobre la situación y se les proporcionaron instrucciones claras sobre cómo proteger su información.
- Resolución: Implementamos medidas correctivas para asegurar adecuadamente el servidor de bases de datos y prevenir futuras exposiciones de datos sensibles.

Procedimiento de Gestión y Control de Cambios:

En Navegapp, entendemos la importancia de implementar cambios de manera controlada y estructurada para garantizar la estabilidad y seguridad de nuestros sistemas. A continuación, detallamos nuestro procedimiento de gestión y control de cambios:

a. Solicitud de Cambio:

- Cualquier cambio en nuestros sistemas debe comenzar con una solicitud formal. Esto puede ser iniciado por cualquier miembro del equipo de desarrollo, operaciones o seguridad, o como resultado de una recomendación de auditoría interna o externa.
- La solicitud de cambio debe incluir una descripción detallada del cambio propuesto, su justificación y el impacto esperado en los sistemas y servicios.

b. Evaluación y Aprobación:

- Una vez recibida la solicitud de cambio, nuestro equipo de gestión de cambios la revisará cuidadosamente para evaluar su viabilidad y riesgos potenciales.

- Se realizará una evaluación de impacto para determinar cómo afectará el cambio a nuestros sistemas existentes, la seguridad de la información y los servicios prestados a nuestros clientes.
- Si se determina que el cambio es necesario y beneficioso, se procederá a obtener la aprobación correspondiente. Esto puede implicar la revisión y aprobación por parte de múltiples partes interesadas, incluidos el equipo de seguridad, desarrollo y operaciones.

c. Implementación y Pruebas:

- Una vez aprobado, el cambio se programará y se implementará siguiendo un horario predeterminado que minimice el impacto en la disponibilidad del servicio.
- Antes de la implementación, se realizarán pruebas exhaustivas para verificar que el cambio funcione según lo previsto y que no cause interrupciones no deseadas en nuestros sistemas.

5) Responsabilidades del Personal

Programa de Concientización y Capacitación en Seguridad de la Información

En Navegapp, reconocemos la importancia de contar con un equipo capacitado y consciente en materia de ciberseguridad y protección de la información. Por ello, hemos implementado un programa integral de concientización y capacitación para nuestros colaboradores. A continuación, detallamos algunas de las acciones y evidencias relacionadas:

Cursos y Sesiones de Capacitación

Regularmente organizamos cursos y sesiones de capacitación enfocadas en seguridad de la información y ciberseguridad. Estas sesiones cubren una variedad de temas, desde buenas prácticas en el manejo de contraseñas hasta identificación de amenazas cibernéticas comunes.

La asistencia a estos cursos es obligatoria para todos los empleados y se registra para garantizar que cada miembro del equipo reciba la formación necesaria.

Material Educativo

Además de las sesiones presenciales, proporcionamos material educativo accesible en línea, como documentos informativos, videos y guías prácticas. Este material está diseñado para reforzar los conceptos clave y proporcionar a los empleados recursos de referencia fácilmente accesibles.

Simulacros y Pruebas de Conocimiento

Regularmente llevamos a cabo simulacros y pruebas de conocimiento para evaluar la comprensión y preparación de nuestros colaboradores en materia de seguridad de la información.

Estas pruebas pueden incluir escenarios simulados de ataques cibernéticos, cuestionarios de seguridad y ejercicios de resolución de problemas.

Orientación Personalizada

Nuestro equipo de seguridad de la información está disponible para brindar orientación personalizada a los empleados que lo necesiten. Esto incluye asesoramiento sobre cómo proteger y cambiar información sensible, así como cómo identificar y reportar posibles amenazas de seguridad.

Evaluación de Efectividad

Regularmente evaluamos la efectividad de nuestro programa de concientización y capacitación mediante encuestas de retroalimentación, análisis de métricas de participación y evaluación de incidentes de seguridad relacionados con el comportamiento del usuario.

6) Copias de Seguridad y Recuperación de Información

Política de Respaldos de Navegapp:

En Navegapp, entendemos la importancia crítica de garantizar la integridad y disponibilidad de los activos de información de nuestra empresa y de nuestros clientes. Por ello, hemos establecido una política integral de respaldos que define claramente las actividades y responsabilidades relacionadas con la ejecución de estos procesos.

A continuación, presentamos los aspectos clave de nuestra política de respaldos:

Frecuencia de Respaldos

Realizamos copias de seguridad diarias de todos los datos críticos, incluida la base de datos del software y otros activos de información relevantes.

Almacenamiento Seguro

Las copias de seguridad de nuestra base de datos se almacenan de forma segura en el servicio de almacenamiento en la nube de Amazon Web Services (AWS), específicamente en el servicio S3.

Esta elección de almacenamiento nos brinda garantías de seguridad, redundancia y escalabilidad para nuestros datos respaldados.

Retención de Copias

Mantenemos las copias de seguridad durante un período de 30 días después de su creación. Después de este período, las copias de seguridad se eliminan automáticamente para evitar la acumulación innecesaria de datos y garantizar la eficiencia en el uso de nuestros recursos de almacenamiento.

Protección del Código Fuente

Nuestro repositorio de código fuente está protegido en GitLab, una plataforma segura de control de versiones. Solo los desarrolladores autorizados tienen acceso para garantizar la confidencialidad e integridad del código fuente.

Responsabilidades y Monitoreo

Designamos responsables claramente definidos para la ejecución y supervisión de los procesos de respaldo.

Monitoreamos de forma regular y proactiva la ejecución de los respaldos para garantizar su éxito y detectar cualquier anomalía o problema potencial.

Recuperación de Datos:

Además de respaldar los datos de forma regular, hemos establecido procedimientos y planes de acción claros para la recuperación de datos en caso de pérdida o fallo del sistema.

Probamos periódicamente nuestros procedimientos de recuperación para garantizar su efectividad y fiabilidad en situaciones reales.