Política

Política de privacidad y seguridad digital

NWP

CORP-NWP-23-0005-R01

nabla wind hub

DESCRIPCIÓN DEL DOCUMENTO

CLIENTE: NWP

PROYECTO: Política de privacidad y seguridad digital

CÓDIGO: CORP-NWP-23-0005-R01

REGISTRO DE CAMBIOS:

2023-09-19: R00 | Registro inicial

2024-02-21: R01 | Primer cambio: añadir herramienta digital KeePassXC

PREPARADO	REVISADO	APROBADO
Paola Salcedo	*Ahmed Moussa*	*Alfonso San Emeterio*
Marketing&Comms Manager	Head of BD	General Manager
Naiara Puentes	*Eder Murga*	
Bids and Proposals Manager	Head of OPS	
	Pablo Villasante	
	IT Manager	

Relevant information of the document and disclaimer

This document is for the use of the Customer, as per detailed on the first page of this document, and has been made in agreement with and according to the Customer's instructions. To the extent permitted by law, Nabla Wind Hub does not assume any responsibility whether in contract, tort including without limitation negligence, or otherwise howsoever, to third parties (being people other than the Customer).

This document has been prepared by Nabla Wind Hub with information provided by the Customer and/or third parties. This document has been produced based on information relating to dates and periods referred to in this document. Nabla Wind Hub is not responsible for the validity of such information, and the document does not imply that any information is not subject to change. Except and to the extent that checking, or verification of information or data is expressly agreed within the written scope off its services, Nabla Wind Hub shall not be responsible in any way in connection with erroneous information or data provided to it by the Customer and/or any third party, or for the effects of any such erroneous information or data whether or not contained or referred to in this document.

Any of the outputs reflected in this document are subject to factors, not all of which are within the scope of the probability and uncertainties contained or referred to in this document and nothing in this document guarantees any wind speed or energy output.

This document must be read in its entirety and is subject to any assumptions and qualifications expressed therein as well as in any other relevant communications in connection with it. This document may contain detailed technical information which is intended for the use only by people possessing the required expertise in the matter.

ÍNDICE

1. POLÍTICA DE PRIVACIDAD Y SEGURIDAD DIGITAL

El Nabla Wind Power S.L.U. tiene como objetivo crear un entorno seguro para todos sus empleados, así como para terceros implicados en nuestra actividad diaria, por ejemplo, clientes y proveedores.

Cuanto más dependemos de la tecnología para el trabajo diario, más vulnerables nos volvemos a graves fallos de seguridad (por ejemplo, errores humanos, ataques de hackers o mal funcionamiento del sistema). Por ello, Nabla Wind Power S.L.U. ha desarrollado esta política con el objetivo de establecer unas directrices globales para la seguridad y privacidad de la información y los servicios.

Esta política se aplica a todos los empleados, contratistas, voluntarios y cualquier persona que tenga acceso permanente o temporal a nuestros sistemas y hardware.

2. DATOS CONFIDENCIALES

Todos los datos confidenciales son secretos y valiosos, como:

- Información financiera,
- Datos de clientes, socios o proveedores,
- Patentes, fórmulas o nuevas tecnologías,
- Listas de clientes.

Todos los empleados están obligados a proteger estos datos. En esta política, daremos a nuestros empleados instrucciones sobre cómo evitar violaciones de la seguridad.

3. PROTEGER LOS DISPOSITIVOS PERSONALES Y DE LA EMPRESA

Cuando los empleados utilizan sus dispositivos digitales (por ejemplo: ordenador o teléfono) para acceder a correos electrónicos o cuentas de la empresa, introducen un riesgo de seguridad para nuestros datos.

Las mejores recomendaciones para los empleados son utilizar estos dispositivos sólo para intereses laborales y no para usos personales. Además, es aconsejable:

- Mantener todos los dispositivos protegidos con contraseña,
- Utilizar un software antivirus completo (por ejemplo: Microsoft 365 Defender para Azure, además de Kaspersky),
- Asegurarse de que los dispositivos están protegidos todo el tiempo y no están expuestos o desatendidos en espacios públicos,
- Inicie sesión en las cuentas y sistemas de la empresa únicamente a través de redes seguras y privadas (por ejemplo: VPN),
- Instale actualizaciones de seguridad de navegadores y sistemas mensualmente o en cuanto haya actualizaciones disponibles,
- Evitar acceder a sistemas y cuentas internas desde dispositivos ajenos o personales.

En caso de que los nuevos contratados reciban algún tipo de dispositivo digital recibirán instrucciones de: nuestro IT Manager, Pablo Villasante. Si tienen más preguntas o dudas, se pondrán en contacto con este último instructor mencionado.

Además, contamos con una nueva herramienta basada en la nube para ayudarnos a gestionar nuestros dispositivos y aplicaciones llamada Intune, desde la que podemos instalar aplicaciones y ajustar la configuración de seguridad desde un mismo lugar. Es como tener un mando a distancia, asegurándonos de que todos nuestros dispositivos están protegidos y actualizados.

4. EMAILS SEGUROS

Los correos electrónicos suelen albergar estafas y programas maliciosos (por ejemplo, gusanos o virus). Para evitar estas infecciones por virus o el robo de datos, es importante que los empleados:

- Eviten abrir archivos adjuntos y hacer clic en enlaces cuyo contenido no se explique (por ejemplo: hacer clic en imágenes sospechosas),
- No caer en títulos clickbait (por ejemplo: descuentos, consejos gratuitos),
- Comprobar si el correo electrónico y los nombres de las personas que lo envían son legítimos,
- Buscar errores misteriosos y extraños (por ejemplo: errores gramaticales, palabras sin sentido).

En caso de recibir un correo electrónico sospechoso, ponte en contacto con nuestro responsable informático, Pablo Villasante, lo antes posible.

5. GESTIONAR CORRECTAMENTE LAS CONTRASEÑAS

Las fugas de contraseñas son peligrosas ya que comprometen toda la infraestructura digital de Nabla Wind Power S.L.U. Todas las contraseñas deben ser seguras y secretas, para que no sean fácilmente pirateadas. Por esta razón, los empleados deberían:

- Elegir contraseñas con al menos ocho caracteres (incluyendo mayúsculas y minúsculas, números y caracteres especiales). Evitar en ella información personal (por ejemplo: fechas de cumpleaños, nombres) y utilizar contraseñas diferentes, no la misma para todo,
- Recuerda las contraseñas y no las escribas,
- Intercambiar esta información sólo si es absolutamente necesario,
- Se recomienda cambiar la contraseña cada 2 meses por razones de seguridad.

Si es necesario tener una serie de contraseñas comunes para varias personas, se utiliza un programa especializado para almacenar este tipo de información con la máxima seguridad, se llama KeePassXC.

6. TRANSFERIR DATOS DE FORMA SEGURA

Para transferir datos entre compañeros es muy importante seguir las siguientes recomendaciones:

- Evitar transferir datos sensibles (por ejemplo: datos de clientes, datos de empleados) a otros dispositivos o cuentas fuera del entorno de trabajo. En caso de transferencia masiva de este tipo de datos, el empleado se pondrá en contacto con el responsable de TI para solicitar ayuda,
- Comparta los datos a través de la red/sistema de la empresa y no mediante Wi-Fi público o conexiones privadas,
- Asegurarse de que los destinatarios de los datos están autorizados a tenerlos,
- Informar siempre de posibles estafas, violaciones de la privacidad e intentos de pirateo.

Es muy importante que nuestro Departamento de TI conozca las estafas, las violaciones y el malware para que pueda proteger nuestra infraestructura. Por este motivo, aconsejamos a nuestros empleados que informen siempre de cualquier duda relacionada con esto. Nuestro Departamento de TI se encarga de asesorar a los empleados sobre cómo detectar correos electrónicos fraudulentos.

7. EMPLEADOS QUE TRABAJAN EN REMOTO

Los empleados que trabajan en remoto también deben seguir las instrucciones de esta política. Dado que acceden a distancia a las cuentas y sistemas de nuestra empresa, están obligados a seguir todas las normas y configuraciones de cifrado y protección de datos, y a garantizar la seguridad de su red privada.

8. MEDIDAS ADICIONALES

He aquí algunas recomendaciones más a seguir:

- Apagar las pantallas, bloquear los dispositivos al salir y evitar tener las contraseñas escritas en el lugar de trabajo,
- Informar lo antes posible al Departamento de Informática de los equipos robados o dañados,
- Cambie la contraseña de todas las cuentas cuando le roben un dispositivo,
- No descargues cosas sospechosas o no autorizadas en los equipos de la empresa,
- Evite acceder a sitios web sospechosos.

Todos, desde nuestros clientes y socios hasta nuestros empleados y contratistas, deben sentir que sus datos están seguros. La única forma de ganarnos su confianza es proteger de forma proactiva nuestros sistemas y bases de datos. Todos podemos contribuir a ello siendo vigilantes y teniendo muy presente la ciberseguridad.

Esta política ha sido aprobada por el Director General de Nabla Wind Power S.L.U. Alfonso San Emeterio, y el Director de Informática, Pablo Villasante, y el Jefe de Operaciones Eder Murga con fecha 19/09/2023. Será revisada periódicamente con carácter anual, con el fin de incluir las modificaciones y actualizaciones que sean necesarias en cada momento, con el objetivo de mejorar su funcionamiento.

Esta política estará a disposición de todos los empleados en los medios comunes de todos los departamentos, además de en la web corporativa.

nabla
wind hub