

	POLITICA DE SEGURIDAD DE LA INFORMACIÓN DECLARACION DE LA DIRECCION	IT-POL-033 PÚBLICA	
SGSI		Edición 3	Página 1

POLITICA DE SEGURIDAD DE LA INFORMACIÓN DE WETRON AUTOMATIZACIÓN S.A., SU ORGANIZACIÓN, Y TODAS LAS PERSONAS Y ENTIDADES QUE CON ESTA COLABORAN.

En este documento definiremos objetivo, alcance, responsabilidades, nivel de sensibilidad o clasificación de la información y nivel de difusión que queramos brindarle.

NUESTRO PROPÓSITO

WETRON Automatización, S.A. (en adelante WESA) se compromete, de acuerdo con su misión y sus valores, **a mantener y mejorar la seguridad de la información y la continuidad de su actividad**, dentro del marco legislativo vigente.

La Política de Seguridad de la Información de WESA **está orientada a garantizar la protección de todos los activos de información y la tecnología utilizada para su tratamiento, de las amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar su integridad, disponibilidad y confidencialidad**, favoreciendo el eficiente cumplimiento de los objetivos estratégicos de la entidad.

Nuestra política de seguridad de la información **va dirigida a toda persona que tenga acceso a la información o a los sistemas de información de la empresa, ya sea interna o externa**. Más adelante detallaremos personas y empresas a las que nos dirigimos.

Para apoyar la política, WESA dispone de un Sistema de Gestión de Seguridad de la Información (SGSI) impulsado por la Dirección, que aporta un enfoque sistemático para el análisis y gestión de riesgos. Si quieres saber más nuestro **MANUAL de seguridad de la información (DOC-SGSI-001)** detalla ampliamente cada uno de los puntos y conceptos aquí mencionados.

PRINCIPIOS RECTORES

En consecuencia con lo anterior, WESA mantiene los siguientes principios rectores o directrices de aplicación a tener en cuenta en el marco del Sistema de Gestión de Seguridad de la Información (SGSI):

<ul style="list-style-type: none"> • Confidencialidad 	<ul style="list-style-type: none"> • Autenticación 	<ul style="list-style-type: none"> • Trazabilidad
<ul style="list-style-type: none"> • Disponibilidad 	<ul style="list-style-type: none"> • Autorización 	<ul style="list-style-type: none"> • Legalidad

Más información de cada “principio” en el **MANUAL de seguridad de la información (DOC-SGSI-001)**.

	POLITICA DE SEGURIDAD DE LA INFORMACIÓN DECLARACION DE LA DIRECCION	IT-POL-033 PÚBLICA	
SGSI		Edición 3	Página 2

DIRECTRICES DE SEGURIDAD DE LA INFORMACIÓN

- Promover una cultura en toda la organización orientada a la protección de los activos de información.
- Difusión, consolidación y cumplimiento de la política.
- Implementar las medidas de seguridad.
- Mantener las políticas, normativas y procedimientos actualizados, con el fin de asegurar su vigencia y nivel de eficacia.
- Promover medios y prácticas que aseguren la continuidad de la actividad.
- Establecer anualmente objetivos de seguridad de la información, KPIs, que permitan evaluar la eficacia del SGSI y promover su mejora continua.

CLASIFICACIÓN DE LA INFORMACIÓN O NIVELES DE SENSIBILIDAD :

- Pública: Información que puede compartirse sin riesgo.
- Interna: Información de uso dentro de la empresa.
- Confidencial: Datos financieros, contraseñas, datos de clientes.

(ver detalles en PG-SGSI-002 Procedimiento de CLASIFICACION y TRATAMIENTO DE LA INFORMACIÓN)

¿A QUIEN SE DIRIGE?

En general esta Política es aplicable a todo el ámbito de la empresa, a sus recursos y a la totalidad de los procesos internos. La seguridad de la información que trata WESA constituye un activo estratégico clave para asegurar la continuidad del negocio.

Va dirigida a toda persona que tenga acceso a la información o a los sistemas de información de la empresa, ya sea interna o externa. Incluye y no se limita a todos los empleados, colaboradores internos vinculados a la entidad a través de los contratos de prestación de servicios, proveedores y terceros en el marco de acuerdos pactados, clientes, otros socios comerciales, auditores y aunque no sean el público objetivo principal la política debe estar disponible a entes reguladores, para demostrar cumplimiento de normativas o estándares.

DIFUSIÓN DE LA POLÍTICA

La Política de Seguridad de la Información debe ser conocida por todos los empleados, así como aquellos que colaboren con WESA siendo el Comité de Seguridad el primer responsable de su difusión. Debe comunicarse a toda la Organización y encontrarse disponible en los medios accesibles por todos los empleados.

P.Valles Molle

Consejero Delegado

**38095907H PEDRO
JOSE EMILIANO
VALLES (R: A59623140)**

Digitally signed by 38095907H PEDRO JOSE EMILIANO VALLES (R: A59623140)
DN: cn=JES, o=WETRON AUTOMATIZACION SA, ou=2.5.4.97-VATES-A59623140,
cn=38095907H PEDRO JOSE EMILIANO VALLES (R: A59623140), sn=VALLES
MOLLE, cn=PEDRO JOSE EMILIANO, serialNumber=DCES-38095907H,
[Description=Reg. ORIS: Page 14/18] ORIS: Page 11/11/2024 /rescomp26
I am the author of this document
Date: 10/24/2024 5:08 PM
PDFgear Version 2.1.14

	<p>POLITICA DE SEGURIDAD DE LA INFORMACIÓN</p> <p>DECLARACION DE LA DIRECCION</p>	<p>IT-POL-033</p> <p><i>PÚBLICA</i></p>	
<p>SGSI</p>		<p>Edición</p> <p>3</p>	<p>Página</p> <p>3</p>

DECALOGO_PERSONAL_CIBERSEGURIDAD

Este decálogo recoge las principales consideraciones de seguridad a tener en cuenta:

1. **Gestiona tus contraseñas** – Deben ser robustas y distintas a las de uso persona, no las compartas bajo ninguna circunstancia.
2. **Usa antivirus** – Mejor si es de última generación, EDR o XDR
3. **No dejes tus dispositivos desatendidos** – Bloquea el ordenador cuando no esté en uso y establece contraseña para el salvapantallas.
4. **Haz copias de seguridad** en dispositivos externos pero que no estén siempre conectados para que nadie pueda tener acceso a ellos y borrarlos o dañarlos.
5. **Mantén actualizado** el sistema operativo y las aplicaciones.
6. **Aplicaciones seguras** – Instala las aplicaciones que provengan solo de fuentes de confianza: páginas web y tiendas oficiales.
7. **Usa cifrado de datos** para proteger la información en todos los medios extraíbles y tu ordenador.
8. **Phishing** – Cuando recibas un correo verifica el emisor, lee bien el texto, nunca des datos personales, ni contraseñas, no pinches enlaces y verifica los adjuntos antes de abrirlos.
9. **Minimiza tu huella digital** – Evita dar información personal en redes sociales. No utilices el usuario/contraseña de WETRON en servicios externos a nuestra empresa.
10. **Navega de forma segura** – Ten cuidado cuando pinchas un enlace o descargas un archivo. Verifica la reputación del sitio web al que vas a acceder.

WETRON automation technology	POLITICA DE SEGURIDAD DE LA INFORMACIÓN	IT-POL-033 <i>PÚBLICA</i>	
SGSI	DECLARACION DE LA DIRECCION	Edición 3	Página 4

La ciberseguridad también depende de ti

PERSONAS | TECNOLOGÍA | UN FUTURO MÁS SEGURO

Seguridad Hoy Mañana Siempre

Personas que hacen la diferencia

DECÁLOGO PERSONAL DE CIBERSEGURIDAD

Este decálogo recoge las principales consideraciones de seguridad a tener en cuenta en tu trabajo diario.

1

Gestiona tus contraseñas

Deben ser robustas y diferentes a las de uso personal, no las compartas bajo ninguna circunstancia.

2

Usa antivirus

Mejor si es de última generación, EDR o XDR.

3

No dejes tus dispositivos desatendidos

Bloquea el ordenador cuando no esté en uso y establece contraseña para el salvapantallas.

4

Haz copias de seguridad

Realízalas en dispositivos externos que no estén siempre conectados, para evitar accesos, borrados o daños.

5

Mantén todo actualizado

Actualiza el sistema operativo y las aplicaciones.

6

Aplicaciones seguras

Instala solo aplicaciones procedentes de fuentes de confianza: páginas web y tiendas oficiales.

7

Usa cifrado de datos

Protege la información en medios extraíbles y en tu ordenador.

8

Phishing

Verifica el emisor, lee bien el texto, no des datos personales ni contraseñas, no pulses enlaces sospechosos y revisa los adjuntos antes de abrirlos.

9

Minimiza tu huella digital

Evita compartir información personal en redes sociales. No uses el usuario ni la contraseña de WETRON en servicios externos a la empresa.

10

Navega de forma segura

Ten cuidado al pulsar enlaces o descargar archivos. Verifica la reputación del sitio web.

RECUERDA SIEMPRE

Piensa antes de hacer clic

Protege la información

Ante la duda, consulta

La seguridad de la información la construimos entre *todos*

WETRON
automation technology