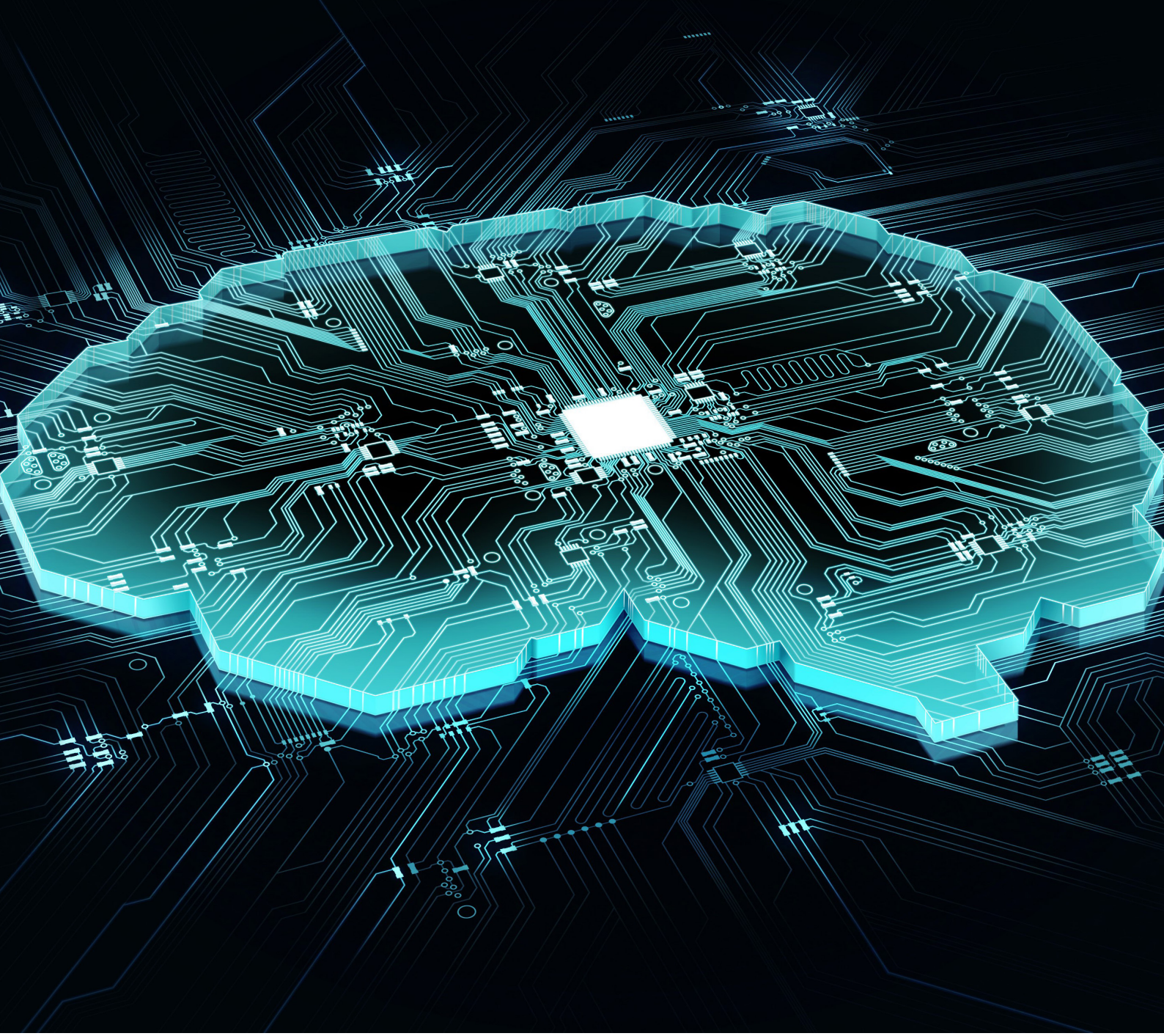

DISCLAIMER USO DE IA EN LAS ORGANIZACIONES

Una iniciativa de

isms forum

www.ismsforum.es
info@ismsforum.es
(+34) 915 63 50 62

DISCLAIMER USO DE IA EN LAS ORGANIZACIONES

AUTORES

PARTICIPANTES

Francisco Lázaro

Ángel Pérez

Virginia Rodríguez

Rubén Cabezas

GESTIÓN DE PROYECTO

Beatriz García

DISEÑO/MAQUETACIÓN

Cynthia Rica

Rim Souri

1 INTRODUCCIÓN

Frente al auge de uso de algoritmos de Inteligencia Artificial en el quehacer digital de las organizaciones y a la ausencia de regulaciones actualizadas, este documento tiene como objetivo proponer unas primeras medidas de concienciación que se pueden desplegar dentro de las organizaciones.

Estas medidas de concienciación se enfocan al colectivo de usuarios de aplicaciones que utilizan algoritmos de IA, y deberá complementarse con un marco normativo específico para desarrolladores e implementadores de algoritmos de IA en las organizaciones.

2 ASPECTOS A CONSIDERAR EN LAS MEDIDAS DE CONCIENCIACIÓN

2.1 ASPECTOS SOBRE ALGORITMOS DE IA PÚBLICOS

Si no existe un contrato de servicio entre la organización y el proveedor del algoritmo de IA se debe considerar que éste es público y, por tanto, la información que se deposite en él puede ser difundida de forma no controlada por la organización.

Por el motivo anterior no se debe compartir con algoritmos públicos información con un nivel de clasificación de la información que no sea público.

El punto anterior incluye información técnica tales como código software, fórmulas, algoritmos propios de la organización, etc.

No se debe conectar algoritmos de IA con sistemas de la organización si no se ha realizado la pertinente evaluación técnica y se han establecido cláusulas contractuales.

Deben leerse las cláusulas de uso de la plataforma IA que ofrece el algoritmo antes de plantear su uso en el contexto de la organización.

2.2 ASPECTOS GENERALES SOBRE ALGORITMOS DE IA

Los algoritmos de IA deben ofrecen resultados en base a su entrenamiento, de forma que se actuar con cautela de cara a la fiabilidad de sus resultados, existen numerosos casos conocidos de resultados erróneos frente a preguntas supuestamente sencillas.

Se debe prestar atención a los dispositivos que utilizan algoritmos, en el caso especial de los smartphones se observa una creciente aparición de APPs de uso de IA que podrían provocar compromisos de seguridad en la organización.

Si se utilizan algoritmos contratados por la organización se debe decidir si se permite que los datos que aporta nuestra organización entrenen a su vez el algoritmo, es muy probable que estos algoritmos sean a su vez utilizados por otras organizaciones, lo que podría afectar a la competitividad de nuestra organización.

3 MECANISMOS DE CONCIENCIACIÓN

Se enumeran distintas opciones de concienciación en función de las capacidades tecnológicas y la sensibilidad del mismo.

CANAL	OBJETIVOS	CONSIDERACIONES
Proxy de navegación	De forma proactiva cuando el usuario va a acceder a un Site categorizado como IA. Proxy genera un aviso con consideraciones.	▪ No válido cuando la conexión con el algoritmo no pasa por el proxy. ▪ Depende de la capacidad de categorización de la solución proxy utilizada. ▪ No siempre la protección proxy permite introducir este tipo de avisos.
Intranet	Comunicaciones en la intranet a todo el colectivo o a actores clave identificados	Será bueno incorporar ejemplos de interés sectorial para que los mensajes sean efectivos.
Correo electrónico	Similar a Intranet.	Fácil de desplegar, puede quedar obviado dentro del volumen de mensajes que se envían.
Acción reactiva tras monitorización	Cuando se detecte acceso a IA por navegación, DLP u otro mecanismo contactar con el usuario para concienciar sobre el uso.	Efectivo frente a detecciones que surjan, pueden existir usos no detectados o que lleguemos tarde. Puede generar una alta carga operativa de usuarios que no sepan cómo actuar por lo que será necesario desarrollar un buen procedimiento operativo de respuesta a los usuarios.
Incorporar formación en la formación periódica de uso adecuado de tecnología	Permite demostrar la diligencia de la empresa y la comprensión por parte del usuario mediante por ejemplo preguntas tipo test.	
Incorporar formación en la formación periódica de uso adecuado de tecnología Hacer firmar un acuerdo a las cláusulas de uso	Obligar a que los usuarios lean y acepten documento interno que regule el uso de la IA en la organización.	Puede requerir el desarrollo de una política de uso de IA y procedimientos derivados. Es útil a efectos no sólo de concienciación sino también a nivel de compliance.

4 EJEMPLO MENSAJE EN PROXY

Cuando va un usuario quiera acceder a URL que esté categorizada como de IA (ya sea esta categoría nativa del producto o introducida manualmente) al usuario, a través del proxy de navegación, se le mostraría una advertencia del tipo:

“

...**ADVERTENCIA DE SEGURIDAD Y PRIVACIDAD**

Está Ud accediendo a una web categorizada como de Inteligencia Artificial (en adelante IA). Por favor, antes de continuar sea consciente de las cuestiones de las que le estamos informando, evalúe la necesidad profesional de continuar, y conforme a su responsabilidad, continue o cancele la navegación.

- Lea atentamente los términos y Políticas del sitio al que quiere acceder. En la mayoría de las ocasiones contienen términos, políticas y condiciones CONTRARIAS al interés de nuestra empresa.
- Recuerde que si el sitio pertenece a las webs de acceso público (aunque sea con un usuario especifico) y no contratado empresarialmente por nuestra compañía, no está intercambiando información de forma confidencial.
- Verifique que es un destino confiable.
- No interconecte o autorice a conectar la IA con aplicaciones corporativas tales como el correo o [SAP/ERP/Aplicación corporativa clave]. Muchas Apps le piden permiso para sincronizar y a partir de esa sincronización le está dando acceso a mediante un token se conecten sin futuras autorizaciones.
- No instale en su equipo o dispositivo móvil aplicaciones que insertan plugin o add-on en aplicaciones ya instaladas.
- No suba (entregue) información confidencial empresarial (secretos comerciales, planes, cuentas bancarias)o regulada legalmente; por ejemplo, datos de carácter personal. Debe considerar que introducir información en esta web es análogo a difundirlo en una fuente pública.
- Como siempre: sea cuidadoso con lo que se descarga; el malware, está muy presente en apps, ficheros y documentos.
- No comparta credenciales.
- Recuerde que los accesos por defensa de los interés empresariales y para cum-plir con la regulación se trazan y en caso de incidentes se analizan.

”