POLÍTICA DE TECNOLOGÍA DE LA INFORMACIÓN

Sección 1: Introducción – Propósito, alcance y aplicabilidad

Esta Política de Tecnología de la Información ("Política de TI") establece la gobernanza y el uso aceptable de los sistemas de Tecnología de la Información ("TI") de McWane, Inc. ("McWane").

Los siguientes términos se definen y tienen el(los) siguiente(s) significado(s), tal como se utiliza a lo largo de este documento:

- "Compañía" significará McWane, Inc., sus divisiones, subsidiarias y filiales.
- "TI corporativa" significa el departamento de TI que opera desde la sede de la empresa e incluye equipos o miembros designados que trabajan bajo la supervisión del personal de TI corporativo.
- "División" o "Divisiones" significarán todas las empresas que operan como parte de McWane, Inc., incluyendo todas las divisiones, subsidiarias y afiliadas.
- "TI de División" incluirá a todo el personal empleado por las Divisiones que participe en el soporte de los sistemas informáticos.
- "Sistema(s) de TI de la Empresa" incluirá todos los Sistemas de TI corporativos y todos los sistemas informáticos operados por una División de la Compañía; y
- "Sistema(s) de TI corporativo(s)" se definirá a continuación de la siguiente manera:

    - "Red" – todo el equipo, tecnologías, aplicaciones u otros elementos utilizados para interconectar sistemas y personal en la Compañía, incluyendo aquellos que se usan para conectar la Red interna McWane a internet, junto con cualquier otra tecnología utilizada para la comunicación entre Divisiones.

    - "Endpoints" – cualquier ordenador de sobremesa o portátil, tableta, teléfono, dispositivo móvil, pantalla de vídeo o similar.

    - "Equipo de Entrega de Servicios TI" – incluye equipos de infraestructura como servidores, routers, switches, controladores y similares, que se utilizan para proporcionar servicios tecnológicos a los usuarios a través de la Red McWane, o de cualquier segmento de la misma; y,

    - "Conectividad con Internet" – la red mundial de conectividad tecnológica que proporciona capacidades de comunicación y acceso a agencias externas, socios comerciales y otras organizaciones, a través de la Red McWane.

Las directrices y procedimientos aquí contenidos están destinados a proporcionar controles sobre el acceso, la seguridad y la propiedad de la información y datos que puedan existir o ser transmitidos a través de los sistemas informáticos de la empresa.

Esta Política de TI se aplica a todos los empleados de la Compañía (o "miembros del equipo") deben seguir sus directrices y procedimientos; también se aplica a aquellos agentes y terceros que han tenido acceso acreditado a(s) Sistema(s) TI de la empresa.

El incumplimiento de esta Política de TI puede resultar en el despido de cualquier acceso concedido y/o acción disciplinaria, que conlleve incluso la terminación del contrato laboral con la empresa. Esto también puede incluir procesos civiles y/o penales bajo las leyes federales o estatales aplicables.

El personal de TI corporativo, junto con el personal de TI de la División, comparte la responsabilidad de garantizar el cumplimiento de esta Política General de TI. El personal de TI corporativo es responsable de adquirir, desarrollar, implementar y, de otro modo, establecer y gestionar recursos de infraestructura IT de uso común en toda la Compañía. Los directivos y/o directivos de cada división son responsables del rendimiento de los recursos de TI que están bajo el control exclusivo de dicha División. El personal de TI de la División u otro tipo de personal puede solicitar la ayuda del departamento de TI corporativo con cuestiones relacionadas con sistemas y operaciones de TI independientes en cualquier momento, pero dichas divisiones asumen la responsabilidad del rendimiento y los costes de dichos sistemas.

Esta Política de TI puede complementarse con directrices y procedimientos vigentes en las Divisiones, pero dichos complementos no pueden contravenir ni debilitar los principios contenidos en esta Política de TI. Cada División debe proporcionar al departamento de TI Corporativo una copia de cualquier suplemento local de forma oportuna, y dichos suplementos podrán ser revisados para verificar la coherencia con esta política. De vez en cuando el personal de TI corporativo o sus representantes designados podrán realizar auditorías periódicas de cumplimiento de esta política, así como auditorías o revisiones de cualquier complemento local a esta política. Se distribuirán y publicarán versiones actualizadas de esta Política de TI según sea necesario.

Se espera que todos los miembros del equipo McWane, contratistas, consultores, trabajadores temporales u otros con acceso a los Sistemas TI de la empresa (colectivamente "Usuarios") sigan esta Política de TI. Es responsabilidad del miembro del equipo de la empresa que solicita acceso comunicar este requisito a cualquier usuario externo que pueda recibir acceso. Las preguntas sobre la Política de TI de McWane, su aplicación y su funcionamiento en la práctica pueden dirigirse al Departamento Legal Corporativo de McWane, o al Vicepresidente y Director de Información de McWane.

Aunque esta política aborda asuntos de TI, no es independiente; este documento se desarrolla junto con y se considera parte de las políticas generales del Código de Conducta de la Compañía, tal como puede ser publicado ocasionalmente por departamentos Jurídicos Corporativos, Recursos Humanos u otros departamentos. Se pueden incluir referencias a dichas otras políticas a lo largo de este documento, y se aconseja a los usuarios que deben seguir las Políticas Generales del Código de Conducta de McWane, además de las directrices específicas establecidas en esta Política de TI.

Sección 2: Uso autorizado y restricciones de uso

Esta sección proporciona divulgaciones y directrices y procedimientos para usuarios relacionados con el uso autorizado y las restricciones sobre el uso de los Sistemas TI de la Empresa. Estos elementos están diseñados para informar y proteger a todos los miembros del equipo, proveedores y clientes al acceder a los Sistemas de TI de la empresa.

Preámbulo:

El acceso a los sistemas informáticos de la empresa se proporciona principalmente con fines empresariales. Se permite el uso personal ocasional e incidental, siempre que dicho uso sea coherente con esta Política de TI y no interfiera con el desempeño de sus funciones laborales por parte del empleado. Ningún usuario debería realizar deliberadamente un acto que afecte negativamente al funcionamiento de los sistemas informáticos de la empresa.

2.1 Sin expectativa de privacidad

Los usuarios no deberían esperar privacidad al usar la Red McWane a través de dispositivos conectados. Los usuarios deben ser conscientes de que los datos que crean en la Red de la Compañía siguen siendo propiedad de la Compañía; por ello, los usuarios deberían evitar, siempre que sea posible, almacenar o transmitir cualquier información personal confidencial o sensible, en o a través de los sistemas informáticos de la empresa.

2.2 Internet y correo electrónico en el lugar de trabajo

La empresa proporciona acceso a Internet y capacidad de correo electrónico, como medio para aumentar la productividad, facilitar comunicaciones electrónicas y realizar transacciones comerciales. Se proporcionan servicios de Internet y correo electrónico según sea necesario para los usuarios autorizados, para ayudar en el desempeño y cumplimiento de las responsabilidades laborales.

Todos los usuarios deben saber que, al convertirse en Usuario autorizado de Sistemas TI corporativos, el uso de internet y correo electrónico puede ser monitorizado. La Compañía se reserva su derecho a supervisar, inspeccionar y/o suspender dicho uso por parte de los Usuarios autorizados, con o sin su conocimiento o presencia. Los usuarios consienten de forma inherente, mediante cualquier uso de internet y/o correo electrónico en el lugar de trabajo, que la Empresa supervise dicho uso.

Las pruebas de violaciones de las directrices de uso de Internet y correo electrónico de la Compañía, que puedan ser descubiertas durante la supervisión por parte de la Compañía, serán comunicadas a la dirección y/o al Departamento de Recursos Humanos Corporativo o de División correspondiente. La Compañía se reserva el derecho de tomar las medidas adecuadas en relación con cualquier infracción que pueda encontrarse.

- Las divisiones solo utilizarán los sistemas de correo electrónico, conexiones a Internet y proveedores de servicios de Internet aprobados por TI corporativo.

- El departamento de TI corporativo implementará protocolos de seguridad y controles técnicos alrededor de los sistemas de correo electrónico y el acceso a Internet, para mantener la seguridad de la red.

- Ninguna división puede establecer una conexión separada a Internet sin la aprobación explícita de TI corporativo; además, la TI corporativa puede aislar, desconectar o tomar otras acciones adecuadas relacionadas con cualquier conexión o conexiones que puedan haber sido o hayan sido establecidas por las divisiones.

- Los usuarios no deben realizar sus negocios de la empresa utilizando cuentas de correo electrónico distintas a las emitidas y autorizadas por McWane Corporate IT o sus divisiones.

    - Está prohibido el uso de cuentas de correo electrónico personales por parte de los miembros del equipo con fines de transmisión o recepción de información de la empresa y/o relacionada con el negocio.

    - Se prohíbe a los usuarios crear cualquier reenvío de correos electrónicos u otras acciones automatizadas, utilizando su cuenta de correo electrónico emitida por la empresa, que de otro modo enviaría información relacionada con el negocio a cualquier cuenta de correo electrónico controlada personalmente.

    - El personal de TI corporativo o local, y a discreción exclusiva de la Compañía y sin previo aviso a los usuarios, puede inspeccionar los registros de correo electrónico en los sistemas de McWane en busca de indicios de que los usuarios utilicen cuentas de correo electrónico personales para realizar negocios relacionados con la Empresa; en los casos en que se detecten violaciones, la Compañía puede tomar las medidas necesarias para bloquear dicha actividad y recuperar, eliminar o borrar información empresarial relacionada con la Compañía de esas cuentas personales y/o dispositivos.

- Además de las directrices, procedimientos y restricciones aplicables que están, o pueden estar contenidos en otras Secciones de esta Política de TI, las siguientes directrices explícitas se aplican a los usuarios autorizados cuando utilizan servicios de Internet y correo electrónico proporcionados por la empresa:

    - El uso personal excesivo de los servicios de Internet y correo electrónico proporcionados por la Empresa puede ser restringido o bloqueado, según lo consideren necesario y apropiado por los administradores de TI.
    - Los usuarios no deben utilizar servicios de internet o correo electrónico proporcionados por la empresa para realizar actividades de juego o de azar.

- Los usuarios no deben enviar correos electrónicos a sabiendas ni acceder a contenido de Internet que pueda contener materiales ilegales u ofensivos de naturaleza gráfica, como contenido pornográfico, violento o racista.
- La información confidencial relacionada con la Compañía debe transmitirse a terceros, por correo electrónico o internet, solo cuando sea necesario y, en todas las circunstancias, debe estar debidamente protegida por los usuarios. Todos los correos electrónicos que contengan información sensible, confidencial o propietaria deben estar marcados como suficientemente seguros, de manera que satisfagan las preocupaciones de confidencialidad asociadas a cualquier transmisión de dicha información. La Compañía puede proporcionar herramientas seguras de mensajería por correo electrónico, y cualquier usuario debe contactar con un administrador de TI para que le ayude a proteger la información confidencial, antes de enviar dicha información por correo electrónico o por Internet.
- Al corresponderse con los abogados de la Compañía sobre cualquier asunto legal, los usuarios siempre deben marcar los mensajes dirigidos a los abogados como "Confidencial — Privilegio Abogado-Cliente."
- Los usuarios nunca deberían intentar eludir o desactivar deliberadamente Internet ni el software de filtrado y seguimiento de correo electrónico utilizado por la Empresa.

2.3 Telecomunicaciones y dispositivos móviles inalámbricos en el lugar de trabajo

Todos los teléfonos y equipos telefónicos instalados para su uso en las instalaciones de McWane, incluidas las buzones de voz, son propiedad de la Compañía. El personal de TI corporativo y de la división es responsable de la instalación y mantenimiento de todos los teléfonos y equipos anexos, incluyendo la asignación de números de teléfono y cuentas de buzón de voz. Se recomienda a los usuarios proteger este tipo de equipos de daños en la medida de lo posible y que establezcan un acceso seguro adecuado a sus buzones de voz.

En algunos casos, McWane puede entregar dispositivos móviles inalámbricos propiedad de la empresa a los miembros del equipo. Bajo cualquier circunstancia, los dispositivos móviles inalámbricos que se utilicen para conectarse y acceder a datos, información y aplicaciones situados en los Sistemas TI corporativos deben autenticarse e inscribirse como dispositivos aprobados bajo la plataforma de gestión de dispositivos de la Compañía.

En general, el uso personal de servicios de teléfono, dispositivos móviles inalámbricos y buzón de voz propiedad de la empresa está permitido, pero no debe interferir con el desempeño oficial del negocio o del trabajo individual. Se aconseja a los usuarios que, para proteger los datos de McWane, prevenir el uso indebido y cumplir con las obligaciones legales existentes, la Compañía se reserva el derecho de monitorizar sus sistemas de mensajería y los datos creados, recibidos o transmitidos por cualquier teléfono o dispositivo móvil inalámbrico utilizado para conectarse a la infraestructura informática de la Compañía. La Compañía también puede modificar, o borrar o restablecer remotamente a los valores de fábrica, cualquier dispositivo móvil autenticado o registrado en el sistema. La Compañía avisará con antelación, cuando sea posible, si es necesario borrar un dispositivo conectado. Sin embargo, es

responsabilidad del usuario hacer copias de seguridad regulares del contenido de cualquier dispositivo de este tipo, para no perder información si un dispositivo es borrado.

- Además de las directrices, procedimientos y restricciones aplicables que están, o pueden estar contenidas en otras Secciones de esta Política de TI, las siguientes directrices explícitas se aplican a los dispositivos móviles de telecomunicaciones e inalámbricos:

    - Los usuarios deben coordinarse con el personal de TI para establecer un servicio telefónico y/o móvil móvil adecuado, coherente con las estrategias de compra de la Compañía – incluyendo, pero no limitado a, la obtención de cualquier servicio de roaming o comunicación internacional o similares características, que puedan ser necesarias para que el teléfono o dispositivo móvil inalámbrico del usuario individual funcione adecuadamente para fines comerciales de McWane.
    - Los miembros del equipo deben informar inmediatamente de cualquier dispositivo móvil de telecomunicaciones o inalámbrico utilizado para realizar negocios en McWane que se pierda, sea robado, accedido por personas no autorizadas o comprometido de otro modo. Por ello, la Compañía puede evaluar el riesgo y, si es necesario, borrar remotamente todo el contenido de McWane o todo el contenido del dispositivo, que puede incluir contenido personal del Usuario.
    - Cuando se les solicite, los usuarios deben proporcionar rápidamente a la Compañía acceso a cualquier teléfono o dispositivo móvil inalámbrico, incluso en caso de incidente o investigación de seguridad.
    - Los usuarios deberían evitar, siempre que sea posible, conectar dispositivos móviles inalámbricos a redes Wi-Fi no seguras, especialmente al realizar negocios en McWane o transmitir información de la empresa.
    - Los usuarios deben mantener la configuración de los dispositivos móviles inalámbricos (seguridad, restricciones de contenido, contraseñas o frases de contraseña, etc.) que sean coherentes con esta Política general de TI.
    - Los usuarios no deben solicitar acceso no autorizado a teléfonos, buzones de voz o dispositivos móviles inalámbricos de sus compañeros laborales, bajo ninguna circunstancia.
    - Se recomienda a los usuarios que sigan todas las leyes o normativas federales, estatales o locales aplicables sobre el uso de dispositivos móviles inalámbricos, especialmente al viajar, conducir o utilizar maquinaria o equipo.

2.4 Redes sociales en el lugar de trabajo

"Redes Sociales" se refiere a una variedad de recursos en línea como blogs, redes sociales, salas de chat, servicios de mensajería y/o otros foros de internet. Ejemplos incluyen Facebook, LinkedIn, X, Instagram, Pinterest y/o alguna de las muchas otras plataformas basadas en internet a las que pueden acceder los usuarios. No es intención de la Compañía controlar lo que los usuarios pueden publicar en sitios personales de redes sociales, pero todos los miembros del equipo son responsables de cumplir con el ***Código de Conducta Ética de la Compañía en el lugar de trabajo,*** cuando estén conectados o

trabajando desde los Sistemas de TI de la Empresa, y/o en sus instalaciones físicas, y utilizando las Redes Sociales.

Además, la Compañía ha establecido una política específica aplicable a todos los miembros del equipo, bajo su Código de Conducta general publicado por el Departamento Legal de McWane, ***titulada "Política de Redes Sociales."*** Dicha política y sus pronunciamientos se incorporan aquí, por referencia, y ninguna de las disposiciones de esta Política de TI pretende ser contraria.

2.5 Directrices generales sobre el uso de sistemas informáticos de la empresa

Las siguientes actividades están prohibidas:

- Uso de los Sistemas TI de la Empresa para cualquier propósito que viole las leyes federales, estatales o locales aplicables.
- Obtener o intentar acceder no autorizado a cualquier tipo de red, servicio, información, comunicaciones o instalación o recurso informático, por cualquier medio.
- Dañar o destruir la integridad de un sistema informático, o los datos o programas almacenados en un sistema informático.
- Descarga o instalación de software no autorizado u obtenido ilegalmente.
- Interferir en las responsabilidades laborales de otro Usuario; y/o,
- Utilizar los sistemas informáticos de la empresa para llevar a cabo actividades comerciales, personales o políticas no autorizadas.

Los usuarios no deben tomar acciones que perjudiquen a la Compañía, a su personal o a sus operaciones, ni expongan a la Compañía a posibles responsabilidades legales o daños reputacionales.

Los usuarios deben ser conscientes de que la transferencia electrónica de ciertos tipos de materiales es ilegal y se castiga con multa o pena de cárcel en Estados Unidos y en otros lugares. La Compañía entregará inmediatamente cualquier prueba de conducta ilegal en sus sistemas a las autoridades competentes.

Se espera que los usuarios que se enteren de que otro usuario está infringiendo esta Política deben notificar a su supervisor o al Departamento de Recursos Humanos Corporativo o de División correspondiente.

Esta Política no pretende restringir comunicaciones o acciones protegidas o requeridas por la ley estatal o federal.

2.6 Dispositivos de usuario final

Los usuarios solo pueden acceder a los Sistemas TI corporativos utilizando dispositivos aprobados por los usuarios finales que cumplan con los estándares mínimos de seguridad de la información de la Compañía. Los dispositivos de uso final propiedad de McWane deben configurarse para recibir

automáticamente actualizaciones y parches rápidos, siempre que sea posible. A los usuarios se les puede denegar el acceso remoto si intentan usar dispositivos no propiedad de la empresa para conectarse a sistemas informáticos corporativos.

Todo el uso de dispositivos de usuario final de almacenamiento conectado por puerto USB (memorias USB, discos duros portátiles, discos conectados, etc.) será controlado o limitado mediante software de seguridad, tal como se configure en todos los servidores y estaciones de trabajo de la empresa, por el personal de TI corporativo. En todas las circunstancias, solo serán aceptables para su uso los dispositivos conectados por puerto USB aprobados.

- Todo el uso de dispositivos conectados por puerto USB deberá ser monitorizado y podrá ser bloqueado, según se considere necesario, para evitar transferencias o compartición de datos inapropiadas o no aprobadas por parte de los usuarios, mediante el uso de dichos dispositivos; y,
- Cualquier dispositivo de almacenamiento conectado por puerto USB que haya sido conectado o utilizado por cualquier miembro del equipo estará sujeto a inspección y/o confiscación, en cualquier momento y según lo considere necesario, por un administrador de TI.

Todos los dispositivos USB identificados como conteniendo información de la Compañía deberán ser recuperados o devueltos a un administrador o supervisor local de TI, tras la finalización de la afiliación o empleo de cualquier usuario con la Compañía; la falta de identificación y/o devolución de dichos dispositivos a la Compañía puede llevar a que la Compañía busque el remedio adecuado, legal o de otro tipo, según sea necesario, para proteger su propiedad y/o su información propietaria frente a un uso indebido.

2.7 Credenciales de acceso

A cada usuario se le asigna un ID de usuario único y debe configurar una contraseña o contraseña, según sea necesario, para acceder a los Sistemas de TI corporativos ("Usuario(s) autorizado(s)"). Las contraseñas y frases de acceso se consideran confidenciales y no deben compartirse. Los usuarios deben informar inmediatamente a TI corporativo si saben o sospechan que alguna combinación de nombre de usuario/contraseña-contraseña ha sido compartida, comprometida o utilizada de forma incorrecta; y/o, si la seguridad de la información asociada a un ID de usuario ha sido violada de alguna manera.

2.8 Seguridad asociada a los dispositivos de usuario final y credenciales de acceso

En la medida en que no se indique específicamente en esta Política de TI, los administradores de TI de la empresa (corporativos, locales y de soporte técnico) deben adoptar las medidas de seguridad adecuadas al configurar nuevos y/o actualizar los endpoints o credenciales de acceso existentes en la red de la empresa, incluyendo pero no limitándose a lo siguiente:

- Asegurarse de que cada punto final desplegado para su uso en el entorno de red de la empresa esté protegido con software de seguridad autorizado por la empresa, correctamente funcionando y configurado (actualmente Microsoft Defender, CrowdStrike y/o Airlock).
- Asegúrese de que cada punto final esté correctamente inscrito en el Sistema de Gestión de Dispositivos de la Empresa adecuado, ya que tal puede ser especificado por TI corporativo de vez en cuando.
- Asegurar, en la medida de lo posible, que cada ID de usuario (miembro del equipo, consultor, contratista, proveedor o de otro tipo) se añada y se mantenga en el grupo de seguridad adecuado de Frases de Contraseña de Grano Fino o Política de Contraseña, según exista y sea aplicable para cada División.
- Asegurar que cada ID de usuario esté configurado y mantenido usando el principio de menor privilegio; y,
- Asegurar, en la medida de lo posible, que cada ID de usuario esté debidamente inscrito y haya aplicado cualquier política de Autenticación Multifactor (o "MFA") aplicable, según pueda ser especificado por TI corporativo de vez en cuando.

Los usuarios deben abstenerse de descargar, abrir, ejecutar o ejecutar aplicaciones y programas no solicitados o no autorizados en las Redes, Sistemas o Endpoints de TI de la Empresa.

- Las herramientas de escritorio remoto, acceso remoto o software de soporte remoto (también conocidas como "RAT's"), proporcionan una forma para que los usuarios de ordenadores y el personal de soporte administrativo compartan pantallas y/o accedan a las redes o puntos finales de la empresa desde ubicaciones remotas, y viceversa. Estas herramientas también pueden proporcionar una puerta de entrada trasera a la red y sistemas de McWane y/o División, que podrían usarse para el robo de accesos no autorizados y/o la destrucción de activos. Como resultado, solo se puede utilizar el escritorio remoto aprobado por la empresa, o software de soporte remoto, que es monitorizado, configurado y controlado correctamente por los administradores de TI, para acceder a la Red McWane y/o de División y a los sistemas o endpoints asociados.

Los usuarios deben tener precaución al abrir archivos adjuntos de correo electrónico contenidos en comunicaciones de remitentes desconocidos, ya que estos archivos adjuntos pueden contener malware, código malicioso u otras amenazas de seguridad de la información que puedan causar compromiso por parte del usuario. Los usuarios no deben responder a correos electrónicos u otros mensajes que constituyan solicitudes de información confidencial, ni modificar la información personal identificable de los empleados o la información bancaria/de depósito directo, ni que soliciten transferencias de fondos de la empresa o de miembros del equipo, a menos que hayan verificado por separado la identidad del remitente y estén seguros de la validez del origen y propósito del mensaje.

Además, los usuarios deben tomar la iniciativa de conocer y seguir estrictamente los procedimientos establecidos por Contabilidad, Finanzas, Recursos Humanos u otros departamentos corporativos o divisionales al manejar cualquier información que pueda considerarse Información Personalmente Identificable (o "PII") de un miembro del equipo, cliente, proveedor u otro contraparte empresarial.

2.9 Política de Inteligencia Artificial Generativa ("GenIA")

En la medida en que una herramienta particular de Inteligencia Artificial Generativa ("GenAI" o "IA") haya sido aprobada para su uso, todos los miembros del equipo de McWane deben utilizar dichas herramientas de manera ética y responsable, coherente con las prácticas declaradas de seguridad de la información de la Compañía. Los miembros del equipo deben priorizar la evaluación de cualquier riesgo de seguridad asociado al uso de herramientas GenAI y practicar una protección estricta de cualquier información confidencial de la empresa o personal cuando se utilicen dichas herramientas aprobadas.

2.9.1 Principios generales para la aprobación y uso de herramientas GenAI

a. **Utiliza ÚNICAMENTE herramientas GenAI aprobadas:** Los miembros del equipo de McWane pueden utilizar herramientas de GenAI para el negocio de la empresa que hayan sido evaluadas y aprobadas por el Comité de Gobernanza de la IA de McWane ("AIGC"). Microsoft CoPilot es la herramienta GenAI predeterminada aprobada para su uso en el entorno McWane y debería ser la única herramienta GenAI utilizada por los miembros del equipo, a menos que otras estén específicamente aprobadas bajo el proceso descrito aquí. Una lista de cualquier otra herramienta GenAI aprobada para su uso por miembros del equipo en los endpoints McWane o en la Red será mantenida, publicada y actualizada por los administradores de SharePoint corporativo en la ubicación adecuada de la intranet de la empresa.

b. **Utiliza ÚNICAMENTE herramientas GenAI suscritas a través de cuentas controladas por la empresa: Están estrictamente** prohibidas las suscripciones a herramientas GenAI destinadas al trabajo a través de cuentas controladas personalmente. Por ello, el trabajo asistido por IA debería ser realizado por los miembros del equipo mediante suscripciones de IA de nivel empresarial proporcionadas por la empresa que incluyan protecciones contractuales de privacidad de datos y cláusulas de 'no formación', como mínimo, y *todos los miembros del equipo deberían evitar el uso de herramientas de inteligencia artificial gratuitas o de nivel público para tareas relacionadas* con el trabajo.

c. **Presentar propuestas para el uso de nuevas herramientas GenAI al Comité de Gobernanza de IA de McWane:** Los miembros del equipo pueden presentar propuestas para el uso de nuevas herramientas GenAI, a medida que estén disponibles para uso empresarial. Como parte del proceso de selección, se contratará al personal adecuado para evaluar la seguridad de cualquier herramienta GenAI propuesta para su uso. Esto incluye revisar las características de seguridad de la herramienta, los términos de servicio y la política de privacidad, así como comprobar la reputación del desarrollador de la herramienta y de cualquier servicio de terceros utilizado por la herramienta antes de que pueda ser sometida al AIGC de McWane para su aprobación.

1. **Principios de Gobernanza que se Aplican a Todas las Herramientas GenAI Presentadas para Uso:** Cualquier herramienta GenAI propuesta para uso por parte de los miembros del equipo en McWane debe ser verificada para alinearse con los siguientes principios antes de su aprobación – equidad (evita sesgos), transparencia (produce resultados explicables), responsabilidad (permite una supervisión clara y controles de acceso), privacidad (protege la confidencialidad y cumple con las leyes de privacidad). seguridad (protege los sistemas de un mal uso) y supervisión humana (apoya, pero no sustituye, la toma de decisiones humanas).

2. **Herramientas GenAI "Gratuitas para Usar":** Las herramientas GenAI que no dispongan de suficientes capacidades de licencia remunerada u otras formalidades *generalmente estarán prohibidas de recibir consideración para su aprobación por parte del AIGC de McWane*. Los equipos de TI y redes corporativas de McWane tomarán medidas para asegurar que dichas herramientas sean identificadas y bloqueadas para su uso por parte de los miembros del equipo, ordenadores u otros dispositivos que se utilicen con fines empresariales en el entorno.

3. **Lista de verificación para propuestas de herramientas GenAI**: La siguiente analítica u otra información debe acompañar cualquier propuesta para el uso de una herramienta GenAI:

   - Nombre de la herramienta y proveedor (incluyendo cualquier referencia en la página web)
   - Caso de uso previsto y justificación empresarial (descripción del proyecto o de otro tipo)
   - Tipos y sensibilidad de los datos que serán procesados
   - Documentación de privacidad, cumplimiento y seguridad asociada a la herramienta
   - Plan de identificación y mitigación de riesgos, si es aplicable a la herramienta
   - Términos de servicio, dependencias de terceros, costes e información sobre licencias
   - Información de contacto del proponente y de su departamento

4. **Proceso de envío y revisión: Los miembros del** equipo que soliciten la aprobación para una herramienta GenAI que se utilice en el entorno McWane deben enviar su propuesta, incluyendo todos los elementos de la Lista de Verificación para su revisión preliminar, a TI corporativo, por correo electrónico o a través del portal Service Now (Help Desk). El departamento de TI corporativo reconocerá la recepción de dichas propuestas en un plazo de 3 días laborables, revisará las propuestas para verificar su integridad, solicitará aclaraciones según sea necesario y se comunicarán los siguientes pasos al proponente para permitir la programación de la consideración por parte del AIGC de McWane en su próxima reunión ordinaria (generalmente cada dos semanas). Si se aprueba, el/los miembro del equipo que envíen la propuesta serán informados y la herramienta se añadirá a la lista aprobada de herramientas GenAI

mantenidas por los administradores de McWane Corporate SharePoint. Si se deniega la solicitud, se proporcionarán razones y/o recomendaciones alternativas al proponente.

2.9.2 Las mejores prácticas de seguridad deben ser aplicadas por los miembros del equipo al utilizar herramientas GenAI:

a. **Proteger los datos confidenciales:** Los miembros del equipo no deben subir ni compartir datos confidenciales, propietarios o protegidos por regulación sin la aprobación previa del Departamento Legal Corporativo de McWane. Esto incluye datos relacionados con clientes, miembros del equipo y/o cualquier otro socio comercial. Los miembros del equipo nunca deben incluir contenido sensible en consultas que utilicen herramientas GenAI, tales como:
    - Información personal identificable (PII);
    - Información personal de salud (PHI);
    - Información sobre precios de empresas o clientes.
    - Identificadores de usuario, contraseñas o frases de acceso emitidas por McWane.
    - La propiedad intelectual o los secretos comerciales de la Compañía.
    - Otros miembros confidenciales del equipo, información del cliente o de terceros.
    - Información de documentos marcados como Confidencial, Sensible o Propietario.
    - Información estratégica, incluyendo preguntas que pueden no parecer especialmente problemáticas pero que podrían revelar inadvertidamente planes estratégicos organizativos (Ejemplo: pedir a la herramienta GenAI que resuma notas de una reunión durante la cual se discuten actualizaciones financieras y cambios futuros que son confidenciales).
    - Otra información no pública de la Compañía que pueda ser útil para la competencia o perjudicial para la Compañía si se revela.

b. **Confirma la exactitud de la información recibida:** Las herramientas GenAI no tienen la capacidad de recordar o citar las fuentes específicas de las que se generan sus respuestas. En lugar de citar frases específicas, sus respuestas se construyen basándose en patrones que han aprendido de una gran variedad de fuentes. Esto significa que las respuestas que un miembro del equipo podría recibir pueden no ser 100% precisas. Por lo tanto, los miembros del equipo deben confirmar la exactitud de la información cruzando las fuentes fiables que normalmente usarían para completar tareas asignadas o tomar decisiones, revisar el contenido en busca de errores y corregir cualquier error, y verificar que cualquier respuesta de una herramienta GenAI que el miembro del equipo pretenda utilizar sea apropiada, ética, no parcial, no supone una violación de la

propiedad intelectual o privacidad de ninguna otra persona o entidad, y es coherente con las políticas de la empresa y las leyes *aplicables*.

c. **Utiliza herramientas GenAI para mejorar, no para reemplazar, el trabajo de los miembros del equipo:** Los miembros del equipo no deben usar estas herramientas como sustituto de las habilidades, conocimientos y capacidades de toma de decisiones únicas que cada miembro aporta a su puesto. Las herramientas GenAI no sustituyen el juicio y la creatividad humanos. Los miembros del equipo deben evaluar la calidad y relevancia de la información proporcionada por la herramienta GenAI y utilizar su propia capacidad y juicio para tomar decisiones informadas sobre qué deben incluir en su trabajo. También deben informar a su supervisor si utilizan herramientas GenAI generativas como parte de la redacción o creación de cualquier contenido que se publique para consumo fuera de la Compañía.

d. **Sigue los estándares legales y éticos:** Se espera que los miembros del equipo sigan estándares legales y éticos al utilizar las herramientas GenAI. Los miembros del equipo deben evitar participar en actividades que puedan infringir la privacidad o los derechos de propiedad intelectual o infringir cualquier regulación o ley. Al crear contenido de cualquier tipo, los miembros del equipo deben distinguir claramente entre su propia entrada y las respuestas generadas por GenAI y atribuir adecuadamente al compartir información.

e. **Control de acceso: Los miembros del equipo** deben usar siempre un ID de usuario proporcionado por la empresa para iniciar sesión en una herramienta GenAI para uso empresarial. Los miembros del equipo no deben acceder a herramientas GenAI fuera de la empresa sin la aprobación previa del departamento o responsable correspondiente y los procesos posteriores necesarios para cumplir con los requisitos de cumplimiento de seguridad. Esto incluye compartir credenciales de acceso u otra información sensible con terceros. Los miembros del equipo también deben aplicar las mismas mejores prácticas de seguridad que se utilizan para todos los datos de la empresa y de los clientes. Esto incluye el uso de contraseñas fuertes, mantener el software actualizado y seguir la política de retención de registros de la Compañía.

f. **En caso de duda, es un error de precaución:** los miembros del equipo deben ser siempre deliberados y diligentes en los esfuerzos por proteger a la Empresa y a las personas a las que servimos al utilizar tecnología generativa GenAI.

LOS MIEMBROS DEL EQUIPO NO DEBEN:

- Utiliza herramientas GenAI para tomar o ayudar a tomar decisiones laborales sobre candidatos u otros miembros del equipo, incluyendo reclutamiento, contratación,

retención, ascensos, traslados, monitorización del rendimiento, disciplina, degradación o despidos.
- Representan el trabajo generado por una herramienta GenAI como si fuera su propio trabajo original; y/o
- Integra cualquier herramienta GenAI con software o programas internos de la empresa sin recibir antes un permiso escrito específico de su supervisor y del Departamento de TI corporativo.

2.10 Requisitos y normas de seguridad de la información de terceros

Estos estándares y requisitos de Seguridad de la Información se aplicarán a todas las terceros contratadas por McWane y/o cualquiera de sus divisiones y/o subsidiarias (colectivamente, la "Compañía"). "Terceros", tal como se menciona aquí, incluirá a cualquier proveedor, consultor, contratista u otro no empleado que busque obtener, requerir o obtener acceso a cualquiera de las redes, sistemas y equipos de tecnología de la información y operación ("TI" o "OT") propiedad de la Compañía correspondiente.

De acuerdo con la Política de TI de la Empresa, los contratos (o acuerdos de servicio) firmados con terceros para servicios relacionados con TI o OT deben especificar cualquier requisito de hardware y/o estándares de seguridad de la información que deban cumplirse durante la realización de cualquier trabajo para la Compañía. Por tanto, todas las terceras partes deberán, como mínimo:

- aceptar seguir la Política de Tecnología de la Información de McWane, o cualquier otra política de la empresa aplicable, tal como se publique y/o revise periódicamente, y que pueda ser anexada o incluida en parte de cualquier acuerdo de servicios de terceros.
- Proporcionar acuse de recibo por escrito de las políticas anexas o incluidas en cualquier acuerdo de servicios de terceros (incluyendo la verificación de la entrega de las mismas a sus empleados), junto con un acuerdo de confidencialidad debidamente firmado.
- aceptar cualquier verificación de antecedentes requerida (realizada en la entidad externa o sus empleados), según la Compañía considere oportuna.
- Acomodar, de forma oportuna, la inspección o auditoría de todo el hardware o software informático que se proponga utilizar por un tercero, antes y/o durante la realización del trabajo para la Empresa.
- se comprometen a mantener y actualizar regularmente cualquier hardware o software informático que utilice el tercero en relación con la realización del trabajo para la Compañía.
- se comprometen a seguir todos los estándares de seguridad de la información para el acceso a redes y/o sistemas, según lo que la Compañía prescriba específicamente, incluyendo pero no limitándose a:
    - especificaciones de autenticación de red y/o sistema.
    - Especificaciones de identidad de terceros o empleados.
    - Especificaciones de uso y protección de credenciales de usuario.

  - requisitos de protección de información y/o datos y privacidad; y/o,
  - Requisitos de formación o concienciación en seguridad de la información.
- A petición, completar un cuestionario de seguridad escrito firmado por un empleado autorizado de la tercera parte y aceptar conservar y proporcionar pruebas de cumplimiento de todos los estándares de seguridad de la información que la empresa pueda prescribir específicamente para la tercera parte.
- se comprometen a notificar rápidamente a la Compañía cualquier incidente o brecha de seguridad causado por el tercero y que pueda afectar a la Compañía.
- se compromete a trabajar en cooperación con la Compañía para mitigar cualquier impacto adverso (incluidos los financieros) derivado de un incidente o brecha de seguridad causado por el tercero; y,
- Aceptan seguir cualquier aviso de conservación de documentos y/o litigios, que pueda ser emitido por la Compañía, si es necesario.

Sección 3: Seguridad de la información y gestión de datos

3.1 Operaciones de Seguridad de la Información

El departamento de TI corporativo gestionará las operaciones de seguridad de la información ("InfoSec") en los sistemas informáticos de la empresa. Como tal, TI corporativa proporcionará orientación sobre prácticas de seguridad de la información, gestionará InfoSec y otras iniciativas de formación y educación en ciberseguridad, asignará roles de seguridad de sistemas, revisará los registros operativos de los sistemas de InfoSec, revisará las implementaciones de hardware y/o software de sistemas con el personal de la División, y supervisará continuamente las operaciones generales de InfoSec de la organización. La TI corporativa también puede realizar otros análisis periódicos de la postura de seguridad de los sistemas informáticos de la Compañía según lo considere oportuno.

Los altos directivos y ejecutivos de cada división son responsables de garantizar que su división siga las prácticas generales de InfoSec de la Compañía, tal y como puedan definirse de vez en cuando por TI corporativa.

Todos los miembros del equipo de McWane son responsables de estar al tanto y seguir la política, los estándares y procedimientos de InfoSec para ayudar a proteger la información frente a accesos, usos y difusión no autorizados, tanto dentro como fuera de la empresa. Los miembros del equipo de McWane que sospechen o vean alguna violación de los estándares de Seguridad Informática de la Empresa, detecten cualquier posible violación de la seguridad de la información o tengan conocimiento de partes no autorizadas que buscan acceder a los Sistemas TI, datos o información de la Empresa, deben notificar inmediatamente a su(s) supervisor(es) y/o personal de TI local o corporativo.

Bajo ninguna circunstancia se debe eludir un estándar o práctica corporativa establecida de InfoSec por parte de ningún usuario o tercero que actúe en su nombre.

3.1.1 Prácticas de seguridad de la información en sistemas informáticos, redes y/o nube

Todo el personal de TI u otro designado de la Compañía, ya sea corporativo o de división, trabajará conforme a las siguientes prácticas y directrices básicas, cuando y cuando sea posible, en conjunto con la gestión continua de las operaciones de seguridad de la información relacionadas con los entornos de endpoints, redes, conectividad a Internet y computación en la nube que conforman los sistemas informáticos corporativos:

- Los privilegios administrativos de TI, ya sean globales, regionales, locales o de otro tipo, serán monitorizados, revisados y ajustados rutinariamente para proporcionar a los usuarios acceso adecuado y seguro a los sistemas informáticos corporativos; se pueden añadir, cambiar o revocar privilegios administrativos específicos de TI para cualquier usuario, según lo determine necesario, y en cualquier momento por parte de TI corporativo.
- Los servicios, aplicaciones y/o protocolos de red innecesarios deben ser identificados y eliminados de inmediato por el personal de TI adecuado.
- Los administradores de TI siempre ejercerán sus responsabilidades laborales y mantendrán una adecuada separación de funciones, cuando sea práctico y viable.
- Se implementarán y supervisarán los controles de acceso al Sistema TI de la empresa y, cuando sea posible, se establecerán reglas de cortafuegos y segmentación de red adecuadas para proporcionar capas de seguridad de la información en todo el sistema.
- El uso de servicios de computación en la nube, obtenidos en nombre o utilizados por la Compañía, será supervisado, asegurado y controlado de cerca por personal de TI autorizado, en la medida de lo posible.
- Solo se deberán instalar herramientas y/o software antivirus, malware, escaneo, prevención de pérdida de datos u otras herramientas avanzadas de seguridad de la información y protección contra amenazas aprobadas por la Compañía en dispositivos conectados o utilizados en todo el Sistema TI Corporativo; y,
- Las herramientas de conectividad inalámbricas, remotas, de Red Privada Virtual u otras herramientas ("Wi-Fi", "VPN" y/o elementos similares del sistema serán monitorizadas y aseguradas, cuando se utilicen para proporcionar acceso al Sistema de TI Corporativo.

3.1.2 Principios de Seguridad de Tecnología Operativa ("OT")

La tecnología operativa ("OT") se refiere al software y hardware que controlan dispositivos físicos, maquinaria, eventos y/u otros procesos realizados por las Divisiones que fabrican productos en el entorno de McWane. Dado que los activos de OT pueden estar directamente conectados o depender de la Red McWane y los Endpoints asociados, proteger la tecnología central para las operaciones es un aspecto importante de las mejores prácticas de seguridad en OT.

Por ello, el personal designado de la Compañía, ya sea Corporativo o de División, operará bajo las siguientes prácticas y directrices básicas, cuando sea posible, en conjunto con la gestión continua de McWane y los activos OT de sus Divisiones:

- Se deben mapear las ubicaciones físicas y digitales de todos los dispositivos OT y verificarse las capacidades de conectividad como legítimas y controladas por personal autorizado.
- Cada persona, dispositivo, aplicación y/o red debe ser confirmada como legítima antes de poder conectarse a cualquiera de los activos de OT de McWane o de sus Divisiones. Se deben desplegar configuraciones de software de seguridad adecuadas para gestionar dichas conexiones, ya sean puntuales o de forma continua, y se debe utilizar una forma aceptable de Autenticación Multifactor ("MFA") junto con la configuración de dichas conexiones.
- Asegúrate de que los ajustes de conexión predeterminados y/o las contraseñas que estén incrustados en los activos de OT, cuando se desplieguen en una ubicación de la División McWane, se cambien para ser únicos para ese activo, en la medida de lo posible.
- Asegurarse de que cualquier miembro del equipo u otra persona que requiera acceso a cualquier activo de OT reciba acceso en base a privilegios mínimos y que las identidades, credenciales y contraseñas/frases de acceso utilizadas, junto con la aplicación de autenticación multifactor, sean revisadas rutinariamente para ajustarse o terminar rápidamente, según sea necesario; y,
- Asegúrese de que todo el software o firmware de activos OT se mantiene, actualice y/o parchee para abordar cualquier vulnerabilidad de seguridad conocida, según sea necesario y apropiado.

3.1.3 Programa de Formación y Concienciación sobre Seguridad de la Información

El departamento de TI corporativo coordinará la impartición de la formación en seguridad de la información y los boletines asociados y otros materiales de concienciación en toda la organización. Todos los directivos, directivos, miembros del equipo, contratistas, proveedores y/o otros miembros del personal que hayan recibido acceso por correo electrónico a los Sistemas TI corporativos recibirán formación y materiales de concienciación en seguridad de la información. La formación en seguridad de la información será proporcionada por TI corporativo al menos trimestralmente, y todos los usuarios deberán participar y completar cualquier tarea que pueda emitirse a través de la Plataforma de Formación en Seguridad de la Información McWane. Cualquier Usuario que no complete las tareas de formación en seguridad de la información con prontitud estará sujeto a que se suspenda o termine su correo electrónico externo o privilegios de acceso al sistema.

Se pueden contratar divisiones para ayudar a desarrollar y/o proporcionar aportaciones y materiales para su uso en la organización, con el fin de promover y aumentar la conciencia sobre la seguridad de la información en toda la Compañía. Las divisiones también pueden realizar ejercicios suplementarios de concienciación o formación en seguridad de la información, según lo consideren apropiado por el personal local de TI u otros directivos.

3.2 Gestión de información confidencial, propietaria y personal

La Compañía ha establecido una política específica aplicable a todos los miembros del equipo, bajo sus políticas generales del Código de Conducta publicadas por el Departamento Legal de McWane, ***titulada "Información confidencial y propietaria y propiedad intelectual."*** Dicha política y sus pronunciamientos se incorporan aquí, por referencia, y ninguna de las disposiciones de esta Política de TI pretende entrar en conflicto con dicha política.

Todos los datos personales tratados por los miembros del equipo estarán sujetos a los requisitos de la ***"Política de Protección de Datos Personales",*** establecida como parte del Código de Conducta general de la Compañía y publicada por el Departamento Legal de McWane. Dicha política y sus pronunciamientos se incorporan aquí, por referencia, y ninguna de las disposiciones de esta Política de TI pretende entrar en conflicto con dicha política.

Sección 4: Activos TI, Protección y Gestión

4.1 Redes, centros de datos centralizados y hardware

4.1.1 Redes

La TI corporativa implementará, gestionará y dará soporte a cualquier infraestructura de red utilizada para conectar equipos de TI corporativos y de la división. Esto incluye redes informáticas y telefónicas, así como redes y tecnologías de acceso remoto que utilizan los miembros del equipo de McWane cuando viajan o están fuera de su oficina de División.

El departamento de TI corporativo proporcionará orientación para la compra y adquisición de equipos de infraestructura conectados a la red. Las divisiones vinculadas a los Sistemas de TI corporativos son responsables de garantizar que todo el equipo conectado cumpla con estándares que pueden ser publicados, de vez en cuando, por TI corporativo. Las divisiones también son responsables de los costes asociados a la accesibilidad y las interconexiones con el Sistema TI Corporativo.

4.1.2 Centro(s) de Datos Centralizado(s)

El departamento de TI corporativo gestionará y dará soporte a los centros de datos centralizados de TI que proporcionan alojamiento de aplicaciones, almacenamiento de datos, copia de seguridad de datos, recuperación ante desastres u otros servicios y equipos relacionados con TI. Estas instalaciones están disponibles para uso de todas las divisiones. Estos centros de datos se mantendrán en una o más ubicaciones físicas. La TI corporativa puede cobrar costes a las Divisiones, relacionados con el mantenimiento y uso de instalaciones centralizadas de TI.

4.1.3 Hardware

La TI corporativa proporciona estándares y un catálogo publicado para todo el hardware y equipo que está aprobado para ser conectado a los sistemas informáticos corporativos. Cualquier excepción en tipos de hardware o estándares debe ser documentada, y el departamento de TI corporativo debe ser notificado de dichas excepciones antes de que se compre, instale y/o conecte el equipo. Todo el hardware conectado debe estar documentado siguiendo la Sección 4.2 de esta política.

Los contratos con proveedores y proveedores de servicios externos deben especificar los requisitos de hardware y los estándares de seguridad a cumplir, como parte de cualquier acuerdo o orden de compra aplicable.

Salvo que se disponga lo contrario en esta Política de TI, o en caso de excepciones, el hardware de propiedad privada no debe estar conectado a los Sistemas TI de la Empresa. Se puede proporcionar acceso a los Sistemas TI de la Empresa para los visitantes según sea necesario. Todas las conexiones de hardware para invitados serán temporales, salvo que el personal de TI corporativo o de la división debidamente autorizado haya previsto una excepción.

4.2 Protección y gestión de activos de TI

Todo el equipo informático debe estar protegido contra accesos no autorizados y daños físicos en la máxima medida posible. Los equipos de entrega de servicios de TI (servidores, routers, switches, etc.) requieren un nivel superior de protección física y, en la medida de lo posible, el acceso a dicho equipo de sistemas informáticos de la empresa debe restringirse solo a aquellas personas con responsabilidades de TI, terceros que necesiten acceso para realizar trabajo en nombre del personal de TI de la empresa y/o personal autorizado de TI corporativo o de división.

En la medida de lo posible y práctico, las salas de ordenadores, armarios de datos, racks de equipos y otros recintos que contengan equipos informáticos deben protegerse contra amenazas medioambientales como incendio, inundación, corte de energía, temperatura excesiva, humedad u otras amenazas, según lo consideren necesario para el personal de TI corporativo o de la División. El propietario de la instalación que contiene dichas habitaciones, armarios, estantes y recintos es responsable de proporcionar dicha protección y notificar al personal informático adecuado sobre las deficiencias que necesitan remediación.

Cualquier activo informático (físico o de software) que sea propiedad o se utilice para llevar a cabo el negocio de la Compañía deberá ser inventariado y rastreado por el personal de TI adecuado y autorizado, utilizando convenciones de identificación coherentes con las directrices que han sido o pueden ser proporcionadas por TI corporativo.

Al deshacerse de cualquier activo informático, todas las aplicaciones y datos, incluido cualquier material sensible, deben eliminarse antes de su eliminación y de manera que impida cualquier tipo de

recuperación. Cualquier medio que almacene información confidencial o personal identificable (PII) que no esté siendo reutilizada internamente debe ser destruido físicamente antes de su eliminación.

La divulgación de información propietaria o colateral-propietaria de McWane a partes no autorizadas, ya sea intencionada o no, debe ser comunicada a TI corporativo, de modo que se pueda tomar medidas para revisar la divulgación e identificar si son necesarios esfuerzos o acciones de remediación posteriores.

Todo el correo electrónico, documentos, datos, registros del sistema e información asociada, ya sea contenida en dispositivos físicos o asociada a servicios de computación en la nube, y independientemente de si se encuentran en Sistemas TI de la Empresa o Sistemas TI Corporativos, estarán sujetos a los requisitos establecidos en la ***"Política de Retención de Registros",*** establecida como parte del Código de Conducta general de la Compañía, y publicada por el Departamento Legal de McWane. Dicha política y sus pronunciamientos están incorporados aquí por referencia, y ninguna de las disposiciones de esta Política de TI pretende entrar en conflicto con dicha Política.

4.2.1 Gestión de parches

El departamento de TI corporativo coordinará responsabilidades con las Divisiones, asegurando que se instalen parches y actualizaciones de seguridad u otros recomendados para todo el hardware, firmware y software, según sea necesario. Los dispositivos que no estén conectados directamente al Sistema TI corporativo deben ser actualizados y mantenidos periódicamente por el personal de TI de la División, ya sea mediante controles automatizados o mediante procedimientos manuales.

Cuando sea posible, y cuando sea posible, se deben aplicar todos los parches de vulnerabilidades de hardware, firmware o software, generalmente dentro de los treinta (30) días previos al lanzamiento. Cualquier excepción debe ser documentada por las Divisiones, y cualquier hardware o software que quede sin parchear o desactualizado debe estar protegido mediante controles compensatorios.

El departamento de TI corporativo, junto con el personal de TI de la División, coordinará todos los procesos de parcheo, tanto como sea posible y necesario, y trabajará para resolver los problemas identificados y/o implementar las medidas de mitigación adecuadas, hasta que cualquier problema identificado se resuelva completamente.

Se puede solicitar a los administradores o usuarios locales de TI que reinicien estaciones de trabajo o servidores, según lo considere necesario por la TI corporativa, para facilitar la recepción de las actualizaciones y/o parches adecuados en dichas máquinas. Cualquier estación de trabajo o servidor utilizado para la conexión a la Red Corporativa puede ser restringido o deshabilitado, temporal o permanentemente, mediante controles de seguridad informática corporativa, si se determina que dicho equipo carece de software, seguridad u otras actualizaciones y/o parches adecuados, O si un usuario no ha conectado adecuadamente su estación de trabajo a la red para recibir actualizaciones oportunas.

4.2.2 Escaneo de vulnerabilidades y gestión resultante

De vez en cuando, el departamento de TI corporativo puede autorizar pruebas internas de vulnerabilidades, escaneos o pruebas de penetración externas en sistemas, por sí sola o con la ayuda de un proveedor de servicios externo. Cualquier herramienta de escaneo, prueba de vulnerabilidades y/o recurso no debe ser utilizado ni desplegado por ningún personal de TI sin el conocimiento previo y la aprobación del personal corporativo adecuado.

Todo nuevo hardware, software o activos de firmware TI debe ser escaneado, evaluado o confirmado de otro modo, con la documentación adecuada, para que no existan vulnerabilidades, antes de que dichos activos se pongan en servicio como parte de los Sistemas TI de la empresa.

Sección 5: Gestión de Identidad y Acceso

El personal de TI corporativo y/o el personal autorizado de TI de la División serán responsables de crear, asegurar y mantener las cuentas de acceso de usuario para acceder a todos los sistemas.

Solo el personal de TI corporativo puede crear o conceder acceso a nivel de administrador de TI a cualquier cuenta de inicio de sesión de usuario contenida en los directorios activos de sistemas de TI o divisionales.

Todo usuario autorizado es responsable de:

- Mantener las contraseñas y/o frases de acceso privadas.
- Informar de una brecha general de seguridad a su supervisor inmediato, al departamento de TI corporativo y/o a su administrador local de TI.
- Cambiar su contraseña o frase de acceso inmediatamente si ha sido comprometida, se sospecha que ha sido comprometida, se ha comunicado a otra persona o puede ser dirigida por TI corporativo.
- Nunca uses el ID de acceso o la contraseña/contraseña de otra persona.
- Evitar, cuando sea posible, escribir contraseñas y frases de contraseña, y/o almacenarlas o publicarlas a la vista; y,
- Asegurarse de que estén desconectados de todos los sistemas, o que su estación de trabajo y/o otros dispositivos usados para el acceso al Sistema estén bloqueados siempre que dichos dispositivos queden desatendidos.

Las siguientes directrices y/o procedimientos se aplicarán a todas las cuentas de usuario autorizadas por la Empresa:

- Se requieren identificadores de inicio de sesión únicos (en conjunto, pueden referenciarse en este documento como "Credenciales de usuario" o "Credenciales") para cada usuario autorizado.

- Se requieren contraseñas y/o frases de acceso para todos los usuarios y deben configurarse como parte de cualquier credencial de usuario. Estas contraseñas o frases de acceso deben configurarse, actualizarse, cambiarse o restablecerse, siguiendo estándares sistemáticamente aplicados, según se publiquen y/o impongan, de vez en cuando, en los sistemas informáticos de la empresa y/o corporativos.
- En general, todos los miembros del equipo, contratistas, credenciales compartidas, administradoras, de proveedores u otras cuentas utilizadas de forma interactiva para iniciar sesión en McWane o en la red, puntos finales o sistemas de su División, deben estar sujetos al nivel más restrictivo y alto disponible de protección por contraseña o contraseña prescrito por TI corporativo. Además, cuando sea posible, las cuentas de servicio utilizadas de forma interactiva también deberían estar sujetas a los mismos estándares.
- Las credenciales o cuentas de usuario genéricas o compartidas deben identificarse fácilmente como tales, limitarse solo a las necesarias y, en todos los casos, configurarse solo después de que se haya obtenido la aprobación del personal autorizado de TI.
- Para que cualquier usuario obtenga acceso remoto a sistemas informáticos corporativos, se requerirá tecnología VPN y/o autenticación multifactor ("MFA") para acceder a equipos informáticos, servidores u otros entornos de TI corporativa. En tales casos, se proporcionarán a los usuarios instrucciones específicas y credenciales VPN o MFA adecuadas, según sea necesario, para iniciar conexiones locales o remotas viables.
- Todas las contraseñas suministradas por el proveedor y cualquier otra contraseña predeterminada deben cambiarse antes de que cualquier ordenador, dispositivo u otro sistema de comunicación se conecte y utilice para fines empresariales; De manera similar, las contraseñas o frases de acceso deben cambiarse cuando un administrador o contratista de TI que tenga conocimiento de dichos elementos, se marche o sea reasignado.
- Las credenciales o cuentas de usuario deben desactivarse lo antes posible, siempre que un usuario autorizado renuncie, sea despedido o deje de trabajar en la Compañía o en alguna de sus divisiones.
- El directorio activo (o directorios) y los detalles asociados a todas las credenciales de usuario y cuentas contenidas en él, tal como se usan para acceder a cualquier sistema informático de la empresa o corporación, deben mantenerse de manera completa, consistente, ordenada y actualizada por el personal de TI de la División.
- De vez en cuando, el personal de TI corporativo puede realizar auditorías o revisiones de Active Directory (o directorios) y requerir ajustes estructurales según sea necesario, para facilitar la identificación y el reporte inmediato de Usuarios a nivel de División, grupos de usuarios y/o otros detalles relacionados con dichas credenciales de usuario contenidas en él.
- Todos los permisos de cuenta acreditados deberían estar restringidos para proporcionar la menor funcionalidad de privilegios necesaria.
- Todas las cuentas acreditadas deben revisarse rutinariamente para garantizar su validez continuada, y las cuentas inactivas durante más de 90 días deben ser deshabilitadas y programadas para su eliminación, salvo que un administrador de TI determine lo contrario.

- Cualquier Credencial de Usuario que permanezca en Active Directory (o directorios), y que se identifique como no utilizada por un periodo superior a 120 días, será confirmada por las Divisiones por necesidad continua o puede ser eliminada por el personal de TI corporativo.
- Cuando sea posible, las cuentas deberían tener una fecha de caducidad específica establecida.
- Para todas las cuentas, el campo "employeetype" en Active Directory debe rellenarse, lo más posible, usando uno de los siguientes valores aceptables:
    - "CompañeroEquipo": para cuentas creadas y asignadas a un empleado individual.
    - "Compartida": para cuentas creadas solo cuando sea necesario, y para soportar múltiples usuarios que compartan la misma identidad; Todos los usuarios que comparten deben estar documentados, especificados y actualizados para cualquier cuenta de este tipo.
    - "Servicio" – para cuentas creadas cuando es necesario y utilizadas para sistemas o aplicaciones que se autentican sin ninguna asociación con una persona específica.
    - "Contratista" – para cuentas creadas y asignadas a una persona que trabaja en nombre de McWane o sus divisiones durante un periodo definido y necesita acceso a los sistemas para desempeñar sus funciones asignadas.
    - "Proveedor" – para cuentas creadas y asignadas a un proveedor que trabaja con McWane o sus divisiones. Estas cuentas pueden compartirse, con la documentación adecuada, por empleados designados de ese Proveedor; o,
    - "Admin" – para cuentas creadas y asignadas únicamente al personal autorizado, según sea necesario para desempeñar sus funciones y responsabilidades.
    -

5.1 Creación de cuentas de terceros y controles de acceso

Las siguientes directrices se aplicarán a todas las credenciales o cuentas de acceso de sistemas de terceros autorizadas por la empresa que se creen para su uso:

DIRECTRICES GENERALES RELACIONADAS CON CUENTAS DE TERCEROS

- Los terceros ("Parte" o "Partes"), tal como se menciona aquí, incluirán a cualquier proveedor, consultor u otro no empleado que busque obtener una credencial para acceder a las redes de las Empresas y/o a equipos tecnológicos de propiedad de la Compañía correspondientes.
- Antes de solicitar el acceso al sistema para cualquier tercero, un miembro autorizado del equipo de la empresa (patrocinador o supervisor) debe realizar un control visual de cumplimiento sobre el tercero y cualquiera de sus delegados Y obtener un Acuerdo de No Divulgación firmado ("NDA") y/o un Acuse de Reciba y Aplicabilidad firmado de esta Política de TI, de un agente autorizado de la tercera parte que especifique, como mínimo:

    - el nombre legal y la dirección del tercero (nombre de la empresa).

- el nombre, cargo, dirección de correo electrónico, trabajo y números de teléfono móvil de la persona designada para recibir notificaciones en nombre del tercero; y,
- la identidad de cualquier persona o personas asociadas con ese tercero para el cual se proporcionará acceso específico a los sistemas de la Compañía; y,

- Al menos 15 días antes del inicio de cualquier trabajo que vaya a realizar cualquier tercero a través de sistemas de acceso, un miembro autorizado del equipo de la empresa debe presentar un ticket de soporte completo especificando a la persona o individuos terceros para los cuales se crearán las cuentas de acceso de usuario. Los miembros autorizados del equipo (patrocinador o supervisor) autorizados por la empresa que aprueben la solicitud de tickets de soporte para el acceso de cualquier tercero, deben registrarse y mostrarse en Active Directory en un campo adecuado, como parte de los datos de cuenta de ese tercero.

DIRECTRICES PARA ADMINISTRADORES DE TI RELACIONADAS CON CUENTAS DE TERCEROS

- Las credenciales o cuentas de acceso a sistemas de terceros emitidas por McWane también están sujetas a las siguientes limitaciones:

  - dichas cuentas creadas para su uso en sistemas McWane no serán válidas más allá de los 120 días desde la fecha de creación y, por defecto, expirarán y quedarán deshabilitadas, salvo que el supervisor solicite una prórroga más allá de los 120 días; Las solicitudes de prórroga de dichas cuentas por parte de los supervisores no serán concedidas por más de 120 días seguidos.
  - dichas cuentas no pueden ser compartidas por múltiples individuos o terceros.
  - dichas cuentas deben usar el VEN. NOMBRE. APELLIDO @divisionname.com convención de nombres.
  - dichas cuentas solo estarán permitidas hasta la licencia F3 de Microsoft Office 365, salvo que el miembro supervisor del equipo de dicho tercero justifique lo contrario.
  - dichas cuentas se verán obligadas a cumplir los requisitos corporativos de contraseña, contraseña, acceso remoto, VPN y/o autenticación multifactor (MFA) de McWane, al crearse; y,
  - dichas cuentas solo pueden utilizarse mediante conexiones remotas seguras, cuando sea necesario, utilizando software aprobado por McWane que haya sido instalado y configurado en el ordenador de terceros.

- Cuando cualquier tercero con acceso a sistemas McWane sea terminado y/o complete su trabajo antes del plazo originalmente previsto, el miembro autorizado del equipo de la empresa (patrocinador o supervisor) deberá notificar al personal de TI adecuado para desactivar y/o eliminar la credencial o cuenta asignada a ese tercero, de manera oportuna.

- Todos los ordenadores, portátiles, tabletas u otros dispositivos de terceros utilizados para acceder a los sistemas de McWane pueden estar sujetos a inspección y aprobación por parte del personal de TI de McWane o de sus Divisiones, antes de poder conectarse a los sistemas de McWane o de sus Divisiones.

Sección 6: Copia de seguridad de datos

Todas las aplicaciones, datos e información contenidos en los Sistemas TI de la Empresa deben ser respaldados y/o archivados para garantizar que existan capacidades fundamentales de datos y/o recuperación ante desastres. Siempre que sea posible, las Divisiones deberían utilizar sistemas informáticos corporativos centralizados para copias de seguridad, para garantizar un acceso consistente y rápido en caso de necesidad de recuperación. Todas las medidas de respaldo de datos y recuperación ante desastres informáticos llevadas a cabo en la Compañía y por sus Divisiones deben proporcionar un soporte satisfactorio a necesidades internas o externas, incluyendo el cumplimiento de cualquier ley y regulación federal, estatal o local aplicable. Las divisiones también deben mantener registros adecuados que documenten copias de seguridad rutinarias exitosas de todos los datos, estaciones de trabajo y servidores mantenidos localmente, y como tal, proporcionar los registros que puedan ser necesarios de vez en cuando para cumplir con cualquier auditoría interna o externa u otros requisitos de cumplimiento. El departamento de TI corporativo trabajará con las Divisiones para garantizar la coherencia en sus prácticas de respaldo de datos y/o hardware, según sea necesario.

Sección 7: Respuesta a incidentes y preparación ante desastres

McWane ha desarrollado y mantiene un Plan de **Respuesta a Incidentes de TI ("IRP") separado**, que puede actualizarse periódicamente, y que se establece para proporcionar a la dirección y al personal de TI principios, directrices y procedimientos para identificar y gestionar adecuadamente incidentes de TI que puedan afectar la seguridad y/o la seguridad de la información de los recursos de TI de McWane y/o de sus Divisiones.

En general, los objetivos para gestionar incidentes informáticos en el entorno McWane incluyen:

- Determinar qué pasó.
- Determinar cómo ocurrió.
- Evaluar cualquier impacto y/o daño derivado de un incidente informático.
- Evitar escalada, propagación o un impacto adicional que pueda derivar de un incidente informático.
- Recuperándose de un incidente informático.
- Perseguir una remediación prudente y permanente de las amenazas para permitir la oportunidad de evitar más incidentes informáticos que de otro modo podrían repetirse por las mismas o similares vulnerabilidades del sistema.
- Determinar la identidad del(los) actor(es) amenazante(s) implicados en cualquier incidente informático y buscar cualquier recurso legal disponible para la Compañía, si es apropiado y posible; y,

- Determinar cualquier acción (conforme a la legislación federal, estatal o local vigente) necesaria para que McWane o sus Divisiones tomen, que mitiguen y resuelvan adecuadamente cualquier brecha de información o datos, o brecha de privacidad, que pueda haber resultado de un incidente informático.

El Plan de Respuesta a Incidentes de TI de McWane ofrece orientación y aborda los siguientes principios:

- Estableció directrices para ayudar a priorizar, caracterizar y/o clasificar incidentes.
- Definiciones específicas de los roles y responsabilidades de los respondedores, procedimientos de gestión de incidentes y planes de comunicación.
- Directrices establecidas que conducirán a la adecuada conservación de cualquier documentación relevante relacionada con incidentes que puedan reportar, según lo requiera la ley aplicable o según lo ordenado por el Departamento Jurídico de McWane.
- Procesos establecidos que permiten revisar y modificar periódicamente el plan; y,
- Procesos establecidos que permiten que el IRP sea evaluado, según la dirección de McWane lo considere necesario, para asegurar que McWane y/o sus Divisiones estén preparadas para llevar a cabo una respuesta exhaustiva ante cualquier incidente informático real.

Sección 8: Elementos generales

Cuestiones y retroalimentación: Para informar y mejorar las prácticas de la empresa en materia de gestión de las tecnologías de la información, se anima a los miembros del equipo a proporcionar su opinión sobre la eficacia, limitaciones o cualquier aspecto problemático que encuentren al aplicar los principios incluidos en esta Política.

Las tecnologías modernas están evolucionando rápidamente. Por ello, McWane se reserva el derecho de cambiar, modificar, complementar o reemplazar esta Política en cualquier momento, con o sin previo aviso, y todos los miembros del equipo deben mantenerse informados sobre la última versión de esta Política.

Aviso legal: Nada en esta política está diseñado ni destinado a interferir, restringir o impedir la comunicación de los miembros del equipo sobre salarios, horarios u otros términos y condiciones de empleo o cualquier otro derecho protegido por las leyes laborales aplicables.

Cumplimiento de las políticas y acuerdos relacionados: Esta política pretende añadir, no contradecir, limitar o reemplazar cualquier otra política y requisito legal aplicable, todos los cuales siguen vigentes y en pleno vigor.

Reconocimiento y cumplimiento: EL CUMPLIMIENTO *DE ESTA POLÍTICA ES UNA CONDICIÓN PARA EL EMPLEO EN LA EMPRESA*. Se anima a todos los miembros activos del equipo a leer y firmar esta política, ya sea como parte de su proceso de incorporación o mediante la realización de interacciones rutinarias con personal de TI de la División, Corporativo u otro directivo. Las copias de las páginas de firma devueltas serán mantenidas por la Compañía, ya sea localmente o en una carpeta de almacenamiento designada situada en la red McWane.

Al firmar a continuación, reconozco que he leído y comprendido los requisitos que se describen en esta política. Acepto utilizar las redes, sistemas y/o equipos informáticos de McWane de manera coherente con las mejores prácticas de seguridad descritas anteriormente y a informar de cualquier incidente o preocupación de seguridad a mi supervisor o responsable de RRHH.

Firma de un miembro del equipo: _____

Fecha: _____