Recomendaciones de infraestructura para distribuidores STAR

2025

MEJORES PRÁCTICAS Y RECOMENDACIONES DE LA INDUSTRIA PARA LA TECNOLOGÍA DE LA INFORMACIÓN EN EL CO`MERCIO MINORISTA AUTOMOTRIZ

Índice

1. Recomendaciones de infraestructura para distribuidores STAR

1.1 Visión general

En este documento exhaustivo, Recomendaciones de infraestructura para distribuidores STAR (*Dealer Infrastructure Guidelines*, DIG), se describen las mejores prácticas del sector y los distribuidores deben consultarlo para verificar las necesidades de infraestructura y redes. Los distribuidores grandes y pequeños deben contar con administradores de red internos, o gerentes TI, que se encarguen de revisar estas recomendaciones, listas de verificación y consejos junto con su Guía de consulta rápida para garantizar que su distribuidora ha implementado una solución segura y sólida que satisfaga las necesidades tanto del cliente como las de los equipos del distribuidor.

1.2 El Grupo de trabajo de las Recomendaciones de infraestructura para distribuidores DIG (GT)

Las Recomendaciones de infraestructura para distribuidores (*Dealer Infrastructure Guidelines*, DIG) cuentan con el apoyo de uno de los varios grupos de trabajo (GT) de la organización STAR. A diferencia de muchos de los grupos de trabajo que se centran en estructuras de datos y transportes, las DIG se crearon para ayudar a los distribuidores, vendedores y fabricantes de equipos originales (*Original Equipment Manufacturers*, OEM) con una guía común para la infraestructura de TI necesaria para respaldar una distribuidora de automóviles segura, eficiente y sólida.

1.3 Ventajas de las DIG: Distribuidores, vendedor y fabricantes de equipos originales (OEM)

Al igual que otros minoristas, las distribuidoras de automóviles necesitan disponer de la tecnología adecuada para respaldar procesos sólidos destinados a la venta y el mantenimiento de vehículos. Con la llegada de Internet, una distribuidora hace uso de muchos sistemas diferentes para satisfacer las demandas crecientes de los clientes. Los proveedores de sistemas para distribuidores (*Dealer System Providers*, DSP) suministran y brindan asistencia a estos sistemas de distribuidores e incluyen desde el núcleo del sistema de gestión de distribuidores *(Dealership Management*, DMS) hasta numerosas soluciones de apoyo como marketing relacional con el cliente (*Customer Relationship Marketing*, CRM), gestión de clientes posibles (*Lead Management*), minería de participación de capital (*Equity Mining*), gestión de la reputación (*Reputation Management*), sitios web, marketing digital, gestión de inventario en línea (*Online Inventory Management*), herramientas de vía de servicio (*Service Lane Tools*) y muchas otras. Con la creciente necesidad de DSP, también es necesario que los datos se compartan de con eficacia y seguridad entre estos sistemas de distribuidores y los OEM. Esta DIG se diseñó para ser una guía para respaldar la integración eficaz de los datos, la protección de los datos, la confiabilidad del sistema y la eficiencia de los procesos empresariales.

1.4 Exención de responsabilidad

Cualquier nombre de empresa, aplicación, vínculo a sitio web o referencia tecnológica que se menciona en este documento no debe considerarse un aval de los fabricantes de equipos originales o de STAR, a menos que dicho aval se indique expresamente.

En este documento se proporciona una especificación o directriz básica para que los distribuidores establezcan una comunicación por Internet. Es importante señalar que la infraestructura de red, los datos del distribuidor y la seguridad del sistema son responsabilidad de la distribuidora. Las organizaciones de terceros, como proveedores de servicios y socios, pueden brindar orientación y recomendaciones. Algunas organizaciones pueden proveer software, hardware o elementos de red patentados para ayudar a optimizar las operaciones de red. Sin embargo, estas aplicaciones, recomendaciones o herramientas no sustituyen a la gestión de la red.

2. Infraestructura de la red de distribuidores

2.1 Visión general

La infraestructura de red de un distribuidor está compuesta por los recursos de hardware y software utilizados para permitir la conectividad de red, la comunicación, las operaciones y la gestión de la red de área local (LAN) del distribuidor. La infraestructura de red proporciona la vía de comunicación y servicios entre los usuarios, los proveedores de servicios, los fabricantes de equipos originales y los clientes finales. La selección y la implementación adecuadas de la infraestructura de red son esenciales para garantizar la eficiencia de la red y la compatibilidad con las aplicaciones y los datos de los fabricantes de equipos originales, los DSP y los distribuidores.

2.2 Hardware

El hardware del concesionario es un dispositivo físico que sirve para capturar datos del concesionario (p. ej., PC, portátiles, dispositivos de mano), enrutar esos datos (p. ej., enrutadores, conmutadores, firewalls) y proporcionar esos datos a petición (p. ej., servidores, monitores y periféricos).

La selección del hardware de red es un componente esencial de la gestión de red de un distribución. Aunque el hardware nuevo puede suponer un gasto de capital muy caro, el hardware antiguo puede entorpecer las operaciones comerciales por problemas de velocidad o compatibilidad, por ejemplo.

En la sección siguiente se detalla cuándo adquirir hardware nuevo, directrices para la compra y recomendaciones para la adquisición de computadoras de sobremesa, portátiles y equipos de red.

2.2.a ¿Cuándo adquirir hardware nuevo?

Un hardware informático con buen mantenimiento puede durar de tres a cinco años o incluso más, en algunos casos. Sin embargo, en algún momento, un distribuidor tendrá que sopesar las opciones de actualizar -o sustituir- el hardware actual.

STAR recomienda que los distribuidores consideren reemplazar el hardware en las siguientes situaciones:

- Cuando el hardware actual no cumple las especificaciones mínimas necesarias para operar una tecnología específica.
- El hardware actual cayó por debajo de los estándares mínimos que establece un OEM, un DSP u otros socios tecnológicos del distribuidor.
- El hardware actual no dispone del hardware, los accesorios o el soporte que los periféricos necesitan para una función específica.
- El dispositivo funciona con tanta lentitud que afecta a las operaciones comerciales. *Tenga en cuenta lo siguiente*: *Esto puede no deberse necesariamente a un problema de hardware. La lentitud puede deberse a la configuración, el almacenamiento, la seguridad o un error del usuario.*
- El software nuevo (como sistemas operativos, navegadores o aplicaciones para distribuidores) no es compatible con el hardware actual.
- El nuevo hardware podría brindar un ahorro en los costos suficiente gracias al ahorro de tiempo, las funciones añadidas o la facilidad de uso.
- Los costos de actualización son iguales o casi iguales a los de un reemplazo, o el producto está llegando al final de su vida útil o ya no cuenta con asistencia técnica.
- El fabricante ya no ofrece asistencia técnica para el hardware. Esto significa que los parches, las actualizaciones de seguridad y las mejoras de software no se instalarán en el dispositivo de hardware.

Cuando el hardware deja de recibir asistencia, el distribuidor se expone a riesgos de seguridad y confiabilidad.

2.2.b Qué comprar: Comparación entre hardware diseñado para el consumidor frente a Hardware de calidad empresarial

La mayoría de los fabricantes ofrecen dos tipos de computadoras: las de hardware diseñado para el consumidor destinadas al uso doméstico y personal, y las de hardware de calidad empresarial, destinadas a los negocios. Aunque el precio del hardware diseñado para el consumidor puede parecer atractivo para los distribuidores, a menudo el costo total de propiedad termina siendo mayor debido a la funcionalidad limitada, los índices de fallos y un soporte más complejo.

STAR recomienda a los distribuidores adquirir hardware de calidad empresarial por las siguientes razones:

- Los sistemas de consumo suelen fabricarse con piezas más genéricas o menos costosas de suministrar en grandes cantidades. Además, los fabricantes son conocidos por cambiar piezas, proveedores y componentes sin cambiar los modelos. Debido a estos factores, estas piezas pueden tener un índice de fallos mayor. Esto puede dar lugar a más tiempo de inactividad, más tiempo de asistencia y una tasa de rotación del sistema más lenta.
- Los sistemas de nivel empresarial suelen estar fabricados con piezas estandarizadas de marcas conocidas, lo que facilita a muchas empresas la estandarización y el soporte de la red.
- Las computadoras diseñadas para el consumidor suelen venir con sistemas operativos pensados para el uso doméstico. Esto puede provocar problemas en las redes empresariales, como la conexión a servidores u otras computadoras.
- El hardware de red diseñado para el consumidor suele estar pensado para admitir solo un número pequeño de conexiones. El hardware de calidad empresarial está diseñado para admitir el gran número de conexiones que necesitan las redes de los distribuidores.
- El hardware diseñado para le consumidor puede tener garantías limitadas. Algunas garantías para consumidores no se extienden a las empresas.
- El ahorro inicial se podría neutralizar con el costo mayor de los recambios y la asistencia técnica, así como por los plazos de rotación más largos para obtener un recambio.

2.2.c Recomendaciones dehardware

Hardware de punto final (computadoras de escritorio, portátiles y tabletas)

Las recomendaciones STAR para computadoras de escritorio, portátiles y tabletas de los distribuidores se han alejado de las especificaciones generales de hardware. Esto se debe, en principio, a los avances en la potencia de procesamiento del hardware, el paso a la computación en nube y la ubicuidad de la movilidad. STAR recomienda que las necesidades de hardware se determinen en relación con una hipótesis de caso de uso según la función del trabajo.
A la hora de adquirir dispositivos nuevos, tenga en cuenta los factores a continuación:

1. **Movilidad:** Algunas funciones dentro de un concesionario exigen movilidad. Otras funciones del puesto se efectúan, en principio, en un lugar físico. Tenga en cuenta las necesidades de movilidad a la hora de adquirir un dispositivo nuevo. Recuerde también que muchos dispositivos móviles, como las tabletas, funcionan con un software específico que puede no ser compatible con todo el hardware y el software necesarios. Considere los requisitos de hardware y software antes de decidir si una tableta, una portátil o una computadora de escritorio es la mejor opción para esa función laboral.
2. **Requisitos de software:** Las funciones en la distribuidora necesitarán la interacción con softwares diferentes. El software suele estar escrito para sistemas operativos y navegadores de Internet específicos. Las aplicaciones de software también pueden necesitar una especificación mínima de hardware. Cuando adquiera un dispositivo nuevo, familiarícese con el software que ejecutará y los requisitos necesarios para ejecutarlo.

3. **Requisitos de los accesorios de hardware.** A menudo, los distribuidores necesitan accesorios específicos para desempeñar una función laboral. Se necesitan ayudas de venta, diagnósticos de servicio y otros adaptadores físicos para casos de uso específicos. Estos accesorios suelen fabricarse teniendo en cuenta especificaciones concretas de software y hardware. Si la función de robo exige un accesorio específico, consulte los requisitos con el proveedor antes de adquirir un equipo nuevo.

4. **Requisitos de OEM, DSP y terceros:** Los fabricantes de equipos originales, los proveedores de servicios para distribuidores y otros proveedores externos suelen implantar tecnologías específicas para distribuidoras. Estas tecnologías (hardware o software) pueden demandar especificaciones concretas para funcionar con eficiencia. Si un dispositivo del distribuidor utiliza tecnologías específicas, consulte al proveedor de la tecnología.

5. **Confiabilidad:** Se debe tener en cuenta la confiabilidad de los dispositivos a la hora de comprar hardware. Algunas áreas de la distribuidora, como el entorno de servicio, son más propensas a fallos de dispositivos. Algunas funciones laborales están más limitadas por el tiempo de inactividad de los dispositivos. Al considerar cuándo y qué comprar, tenga en cuenta la probabilidad de fallos del dispositivo y el impacto que un fallo puede tener en esa función laboral y en las operaciones comerciales de la distribuidora.

Más allá de las recomendaciones sobre casos de uso, STAR puede orientar sobre cuándo adquirir nuevo hardware y qué comprar cuando llegue ese momento. STAR brinda orientación sobre "cuándo comprar hardware nuevo" en las Recomendaciones de infraestructura para distribuidores STAR en la sección 2.2.a. A la hora de determinar qué comprar, STAR ofrece orientación sobre las compras de hardware diseñado para el consumidor frente al hardware de calidad empresarial en la sección 2.2.b., y una guía para tabletas y dispositivos móviles en la sección 2.2.d.

Para obtener más información sobre las recomendaciones de hardware para distribuidoras, incluso tabletas, la movilidad y el retiro de servicio y reciclaje de hardware, consulte la sección 2.2.e.

Hardware de red (enrutadores y conmutadores)

Enrutadores y conmutadores	
Componente	**Especificaciones**
Especificación estándar Ethernet	IEEE 802.3 100baseT o 1000baseT
Redundancia	La conexión de varios conmutadores entre sí debe utilizar enlaces redundantes de la mayor velocidad disponible, como STP o rSTP para garantizar una topología sin bucles.
Fuente de alimentación	Se recomienda utilizar fuentes de alimentación redundantes para reducir el tiempo de inactividad.
Velocidad	100 o 1000 Mbps
VLAN	Los conmutadores con tecnología VLAN y troncal 802.1Q deben utilizarse para redes enrutadas con varias subredes o VLAN.
Protocolos de gestión	Los dispositivos gestionados deben ser compatibles con los estándares de gestión remota del sector, como el protocolo simple de gestión de red (SNMP) y la monitorización remota de red (RMON).
Conmutadores inalámbricos	Los dispositivos inalámbricos deben ser de doble banda y compatibles con IEEE 802.11ac/ax.

2.2.d Tabletas y dispositivos móviles

Las tabletas son dispositivos portátiles diseñados para brindar movilidad y accesibilidad. Las tabletas no suelen tener la misma funcionalidad que una computadora de escritorio o una portátil. Por ello, es muy recomendable que las distribuidoras no sustituyan las computadoras de escritorio o las portátiles por tabletas, sino que las amplíen cuando las aplicaciones y funciones necesiten mayor movilidad y accesibilidad.

Algunas aplicaciones se desarrollaron específicamente para funcionar en determinados dispositivos de tableta, como las iPad. Cuando se instalan estas aplicaciones, el OEM o el DSP se comunicará con los dispositivos cuyas aplicaciones están diseñadas para su uso. En función de la evolución de la tecnología en el espacio móvil, la compatibilidad de ciertos programas puede estar limitada a tabletas específicas o versiones del sistema operativo de dispositivos móviles.

2.2.e Retiro del servicio y reciclaje de hardware

El propietario original del dispositivo tiene la responsabilidad de asegurarse de que todos los aparatos electrónicos usados se desechen correctamente. Hay miles de empresas de reciclaje electrónico en Estados Unidos, pero es importante elegir la correcta. A continuación se ofrecen algunas sugerencias a la hora de elegir una empresa de reciclaje.

Averigüe las políticas o prácticas del reciclador para destruir los datos personales de los equipos usados.

- Los datos pueden borrarse de los soportes de almacenamiento utilizando un método de borrado magnético o un programa para sobrescribir todos los sectores de un disco duro. Cualquier método que se use para borrar datos debe ejecutarse más de una vez (varias pasadas).
- Los medios de almacenamiento pueden destruirse por trituración, corte, incineración, perforaciones múltiples o aplastamiento.
- El reciclador debe poder certificar por escrito que los datos se borraron -o los medios de almacenamiento se destruyeron, así como proporcionar un registro de los métodos utilizados.

Averigüe cuál es la certificación de la empresa de reciclaje.

- El reciclador debe estar certificado. Si le dicen que no tienen certificación, que es un "secreto comercial" o que su método es "confidencial", evite utilizarlos.
- Las principales certificaciones del sector son las siguientes:
    - E-Stewards - www.e-stewards.org
    - Red de Acción de Basilea - www.ban.org
    - R2 - www.sustainableectronics.org
- Los recicladores y consolidadores deben poder demostrar que cuentan con las instalaciones, la formación y los equipos adecuados para ejecutar las operaciones que declaran con solo presentar un sistema de gestión u operaciones auditado con pruebas de auditorías recientes.
- Pregunte si la empresa de reciclaje dispone de un sistema o certificación de gestión medioambiental, ya sea una certificación de gestión medioambiental ISO 14001 o certificaciones de organizaciones como la Asociación Internacional de Recicladores de Electrónica (IAER) o el Instituto de Industrias de Reciclaje de Chatarra (ISRI).
- Se recomienda precaución con quienes no estén certificados. La distribuidora, como propietario original del dispositivo, tiene la responsabilidad de garantizar un reciclaje adecuado.

Averigüe si el reciclador ha tenido alguna infracción medioambiental o de seguridad (citaciones, multas, avisos de

infracción, órdenes de consentimiento, etc.) o si ha presentado alguna reclamación al seguro por daños medioambientales en los últimos 5 años.

- Se prefieren las empresas con un buen historial de cumplimiento de los requisitos medioambientales y de seguridad.
- Una empresa que lleva varios años en el mercado y sólo ha cometido algunas infracciones menores que se resolvieron con rapidez puede ser tan responsable como una empresa que sólo lleva uno o dos años en el mercado y no ha cometido ninguna infracción.
- Comprobar si se han producido infracciones importantes, como vertidos de residuos en grandes cantidades o quejas vecinales significativas.

Averigüe si el reciclador envía equipos usados o residuos a otros socios comerciales o proveedores de servicios; éstos se denominan "socios intermedio".

- Llevar un buen registro es una de las mejores prácticas de gestión del sector. Busque empresas que lleven registros detallados que incluyan dónde envían los materiales, cuánto envían y los números de serie de los artículos que se van a reutilizar.
- Aunque existen varios recicladores de "servicio completo" en EE. UU., es probable que el reciclador no se encargue del procesamiento completo del dispositivo.
- La empresa de reciclaje debe disponer de registros escritos sobre el procesamiento que se realiza *in situ* (como la clasificación o trituración) y sobre quién recibe los materiales o los productos tras el procesamiento inicial.
- Pregunte si los socios comerciales del reciclador (socios intermedios) tienen un vínculo contractual con las mismas normas o mejores prácticas de gestión que el reciclador elegido. La empresa de reciclado elegida debería disponer de un listado completo de todos los socios intermedios.
- Desconfíe de los recicladores que afirman que sus procesos y socios comerciales son "confidenciales", "patentados" o que "no los conocen".
- Toda exportación debe realizarse de conformidad con la legislación aplicable tanto en el país exportador como en el importador.

Un reciclador debe contar con un seguro de responsabilidad civil general y medioambiental.

- Los requisitos en materia de seguros varían de un estado a otro, y el monto y el tipo de cobertura necesarios variarán en función del tamaño y las operaciones de la instalación.
- El monto y la cobertura dependerán del alcance y la magnitud de las operaciones.

2.3 Software

El software es el programa o la información operativa que utiliza el hardware de la distribuidora para capturar, almacenar, manipular y mostrar datos en el hardware de la red. Las distribuidoras utilizan software para capturar datos de clientes, automatizar procesos comerciales de venta y mantenimiento de vehículos y comunicarse con otros sistemas o redes.

En el caso de las distribuidoras, estos programas o procesos suelen residir en el sistema operativo de una computadora o en el navegador de Internet. El software se suele diseñar para sistemas operativos o navegadores de Internet específicos. Dado que el software es esencial para las comunicaciones y los procesos empresariales de la distribuidora, es importante que las distribuidoras utilicen sistemas operativos y navegadores compatibles con el software de la distribuidora.

En la siguiente sección se detallan los sistemas operativos y navegadores más comunes. El objetivo de esta sección es brindar orientación para comprender y seleccionar sistemas operativos y aplicaciones de navegación. Se recomienda encarecidamente al distribuidor que consulte a su OEM y a los proveedores de servicios de la distribuidora para garantizar la compatibilidad del software con las aplicaciones de la distribuidora.

2.3.a Sistemas operativos

A continuación encontrará una lista de los sistemas operativos más comunes en el mercado actual. Algunas aplicaciones no son compatibles con sistemas operativos específicos. Se recomienda a los distribuidores que consulten con sus OEM, DSP y otros proveedores para determinar

qué sistemas operativos utilizar. Tenga en cuenta que Microsoft ha finalizado la asistencia técnica para los sistemas operativos Windows XP, Vista y Windows 7. Esto incluye actualizaciones de seguridad críticas. STAR recomienda a los concesionarios no utilizar Windows XP, Vista ni Windows 7.

Sistemas operativos comunes actuales de clientes	Última actualización o Service Pack*	Fin de la asistencia estándar	Fin de la asistencia ampliada
Windows XP	Service Pack 3	14 abril 09	8 abril 14
Windows Vista	Service Pack 2	10 abril 12	11 abril 17
Windows 7	Service Pack 1	13 enero 15	14 enero 20
Windows 8	Windows 8.1	9 enero 18	10 enero 23
Windows 10	22H2	13 octubre 20	14 octubre 25
Windows 11	24H2		
MAC OS X	15.1.1	Las versiones 14 e inferiores ya no tienen asistencia.	Las versiones 14 e inferiores ya no tienen asistencia.
IOS (para iPad y iPhone)	18.2		
Android	15		

Últimas actualizaciones/service pack a partir de enero de 2025

2.3.b Navegadores de Internet

A continuación se muestra una lista de los navegadores de Internet más comunes en el mercado actual. Algunas aplicaciones no son compatibles con determinados navegadores. Otras aplicaciones demandan una configuración específica del navegador, como el modo de compatibilidad. Se recomienda a los distribuidores que consulten a sus OEM, DSP y otros proveedores para determinar qué sistemas operativos deben utilizar.

Navegador	Última actualización o Service Pack*	Notas
Safari de Apple	17	No se recomienda su uso en sistemas operativos de Microsoft
Google Chrome	131	
Internet Explorer	11	Internet Explorer se retiró en junio de 2022. Microsoft Edge es el navegador que recomienda Microsoft.
Microsoft Edge	1131	
Mozilla Firefox	133	

Últimas actualizaciones/service pack a partir de enero de 2024

2.3.c Licencias de software

El cumplimiento de las licencias de software es algo que la mayoría de los distribuidores pueden no preocuparse. Sin embargo, si no se tiene en cuenta, puede costar miles de dólares a la distribuidora. Estos son los errores más comunes en la concesión de licencias de software para una distribuidora.

- Compartir una licencia común en lugar de tener una por dispositivo
- Compartir inicios de sesión para software basado en la nube
- Tener copias de software con licencia legal instaladas pero sin utilizar
- Comprar versiones "domésticas" de software en lugar de versiones comerciales o para empresas
- Uso de software pirata, descargado gratuitamente

Para solucionar este problema, las empresas necesitan crear un programa de Gestión de Activos de Software (SAM). SAM es la práctica de gestionar y optimizar la compra, la instalación, el mantenimiento y el ciclo de vida de los activos de software dentro de una organización. Las dos ventajas mayores de un programa SAM son el control de costos y la reducción de riesgos.

2.4 Red de área local (LAN)

Una red de área local (LAN) es un grupo de computadoras y dispositivos asociados conectados entre sí mediante comunicaciones comunes compartidas, como una línea de cable o un enlace inalámbrico. Las distribuidoras deben gestionar una red para que los dispositivos de la distribuidora puedan comunicarse y compartir recursos de forma eficaz y segura.

La gestión de redes puede ser una tarea difícil para los concesionarios de automóviles. Los distribuidores necesitan que la red esté disponible para compartir datos, así como limitar el acceso por motivos de seguridad. Además de los empleados de la distribuidora, a menudo un proveedor de servicios, el OEM e incluso los clientes también pueden necesitar compartir los recursos de red. Proporcionar un acceso seguro a la red de la distribuidora puede ser todo un desafío.

En la sección siguiente se ofrecen recomendaciones para la configuración y gestión de la red de área local. También se provee asesoramiento sobre redes inalámbricas, movilidad de la distribuidora y acceso de los clientes.

Recomendación	Especificación
Firewall	Dispositivo de seguridad totalmente gestionado que ejecuta una supervisión continua de las amenazas mediante el sistema de detección de intrusiones "IDS" y el sistema de prevención de intrusiones "IPS" y otros mecanismos como el filtrado de paquetes, el antivirus y la inspección de paquetes con estado. - Los firewalls deben ser compatibles con la traducción de direcciones de red/tecnología analítica de procesos (NAT/PAT). Los firewalls también deben admitir el enrutamiento dinámico mediante RIPv2, OSPF y BGP. - Cambie la contraseña del dispositivo en el momento de la instalación y de forma continua y periódica. - Guarde una copia de seguridad de la configuración en caso de fallo del software o de sustitución del hardware. - Se puede lograr una redundancia de hardware adicional mediante un firewall secundario de alta disponibilidad. - Para obtener más información sobre firewalls y seguridad de la red, consulte el apartado 2.6.
Servicios de nombres de dominio (DNS)	Utilice DNS público excepto cuando utilice Windows Active Directory. (En cuyo caso, es necesario disponer de un servidor DNS interno)

2.4.a Configuración y gestión de la red

Recomendación	Especificación
Red de área local	Gigabit Ethernet
Cableado de datos	El cableado de red de datos existente debe ser, como mínimo, de categoría 5e según las normas TIA-568-A. La categoría 6a debe utilizarse para el cableado nuevo. Los tramos horizontales de cable no deben superar los 90 metros (295 pies). El cable de fibra óptica es muy recomendable en lugar de los tendidos de cable de datos cuando la longitud supera los 90 metros (295 pies).
Ubicación del equipo	Los equipos LAN (conmutadores) deben alojarse en un armario de cableado o sala de comunicaciones. Todos los equipos deben montarse en un bastidor o estante o fijarse a un bastidor o estante. Algunos modelos de conmutadores pueden alojar una fuente de alimentación adicional para una mayor tolerancia a fallos.
Direccionamiento IP	El ISP de la distribuidora debe proporcionar un direccionamiento IP enrutable. En el caso de la LAN del distribuidor, debe utilizarse el direccionamiento dinámico (DHCP) para facilitar la asistencia.
Adaptador de red	Gigabit Ethernet
Conmutación Ethernet	Conmutador Gigabit gestionado. Etiquete cada interfaz y cable. Esto ahorrará tiempo a la hora de localizar cables de red para asistencia o instalaciones nuevas.
Enrutadores	Enrutador para empresas. Los enrutadores deben ser compatibles con la Traducción de Direcciones de Red/Tecnología Analítica de Procesos (NAT/PAT). Los enrutadores también deben admitir el enrutamiento dinámico mediante RIPv2, OSPF y BGP. - Cambie la contraseña del dispositivo en el momento de la instalación y de forma continua y periódica. - Guarde una copia de seguridad de la configuración en caso de fallo del software o de sustitución del hardware. - La implementación de SDWAN es una solución preferida que proporciona conmutación por error, funciones de tráfico optimizadas y mantiene las configuraciones almacenadas en la nube mientras conecta la distribuidora a Internet, centros de datos y otras ubicaciones del distribuidor.

2.4.b Infraestructura de los distribuidores y continuidad comercial

La infraestructura de los distribuidores desempeña una función esencial en la recuperación en caso de catástrofe y en la capacidad de volver al funcionamiento normal de la red.

Las áreas críticas de la red de una distribuidora deben estar en alta disponibilidad, contar con infraestructura redundante o con soluciones de copia de seguridad críticas. Star recomienda las siguientes consideraciones de infraestructura:

Infraestructura de distribuidores	Recomendación	Referencia
Transporte de datos/ ancho de banda	Varias tecnologías y operadores proporcionan una conectividad confiable a Internet	Sección 2.5.c
Red de área extensa	Las tecnologías como SDWAN proporcionan conmutación por error, funciones de tráfico optimizado y mantienen las configuraciones almacenadas en la nube mientras conectan la distribuidora a Internet, centros de datos y otras ubicaciones del concesionario.	Sección 2.4.a
Red de área local	El hardware de alta disponibilidad, las fuentes de alimentación redundantes y las copias de seguridad de la configuración garantizan que los fallos de los equipos no afecten a las operaciones de la empresa.	Sección 2.4.a

Copia de seguridad de datos	Debe hacerse una copia de seguridad de los datos de servidores, terminales y equipos de red y guardarla en otro lugar.	Secciones 2.2.c y 2.4.a

2.4.c Redes inalámbricas

Las LAN inalámbricas permiten la comunicación en red sin las limitaciones físicas del cableado. La tecnología inalámbrica puede ser especialmente conveniente, ya que puede proporcionar movilidad a los empleados, permitir a los clientes traer y utilizar sus propios dispositivos y ampliar la red del distribuidor más allá de las paredes físicas del mismo. Los distribuidores también deben comprender que la omnipresencia de las redes inalámbricas conlleva problemas de diseño, asistencia y seguridad.

Utilice las siguientes directrices a la hora de diseñar, soportar y proteger una red inalámbrica de concesionario.

Diseño de redes inalámbricas	
Recomendación	**Especificación**
Hardware inalámbrico	Sólo deben utilizarse puntos de acceso de nivel empresarial. Los puntos de acceso de nivel empresarial están diseñados para proporcionar itinerancia y otras funciones de clase empresarial (como VLAN o múltiples SSID) necesarias para admitir los dispositivos inalámbricos para aplicaciones. Los puntos de acceso inalámbricos para empresas también están diseñados para alojar un mayor número de conexiones que el hardware diseñado para el consumidor.
Segmentación de la red	Las distribuidoras deben asegurarse de que el tráfico de invitados está segmentado de la red de la distribuidora mediante VLAN o una conexión a Internet independiente.
SSIDs	Se recomienda a las distribuidoras que utilicen SSID distintos para las diferentes funciones empresariales (es decir, ventas, servicio y administración). Sin embargo, las distribuidoras no deben confundir los SSID con la segmentación de la red. Por lo general, los SSID no separan el tráfico de red, sino que sólo proporcionan una forma diferente de unirse a la red.
Cobertura	Despliegue puntos de acceso inalámbricos para garantizar una cobertura adecuada. Las herramientas inalámbricas pueden proporcionar intensidad de señal en todo el edificio. Tenga cuidado con las estructuras u objetos que puedan interferir en la cobertura inalámbrica (interferencias eléctricas, interferencias de radiofrecuencia o materiales físicos como metales u hormigón).
Autenticación y cifrado	WPA2 con autenticación RADIUS y cifrado AES. Nota: Consulte las recomendaciones del OEM para obtener orientación sobre la compatibilidad de las tecnologías específicas del OEM.
Norma de red	802.11ax o 802.11ac
Detección de redes inalámbricas no autorizadas	Escanee, identifique y elimine cualquier punto de acceso inalámbrico no autorizado que pueda haber en la red de la distribuidora. - Un punto de acceso inalámbrico no autorizado se define como un punto de entrada inalámbrico a la red de la distribuidora que no ha sido autorizado o protegido por el distribuidor, la dirección de TI y el propietario. - Todas las redes inalámbricas no autorizadas deben detectarse, encontrarse y eliminarse de inmediato. - STAR recomienda el uso de un servicio gestionado de detección inalámbrica que ejecute un escaneo continuo de la red en busca de amenazas inalámbricas.

Movilidad de las distribuidoras	
Recomendaciones	**Especificación**
Movilidad dentro de la distribuidora	Utilice una red de malla inalámbrica para garantizar que los usuarios finales puedan desplazarse por el lugar sin perder la conexión ni tener que autenticarse de nuevo.
Controladores inalámbricos	Un controlador de LAN inalámbrica puede utilizarse en combinación con el protocolo de punto de acceso ligero (LWAPP) para gestionar puntos de acceso ligeros en toda la red de la distribuidora. Esto ayudará a garantizar una cobertura adecuada, confiabilidad y eficiencia de la red.

Acceso de clientes	
Recomendaciones	**Especificación**
Priorización del tráfico	Los concesionarios deberían utilizar un firewall u otro mecanismo para limitar el consumo de ancho de banda de los invitados. Esto evitará que el acceso de invitados interfiera en las operaciones de la empresa al consumir demasiado ancho de banda.
Autenticación de invitados/Términos y condiciones de servicio	STAR recomienda a las distribuidoras que utilicen un portal cautivo que obligue a los clientes a aceptar los términos y condiciones de uso en el concesionario. Esto puede incluir restricciones de contenido, limitaciones de ancho de banda y acuerdos de uso.
Ancho de banda de Internet	Para asegurarse de que la distribuidoras disponga de suficiente ancho de banda, debe elegir la tecnología y la velocidad adecuadas. (Para obtener más información sobre tecnologías y ancho de banda de Internet, véanse las secciones 2.5a y 2.5b del STAR DIG). - STAR también recomienda que cada distribuidora tenga una conexión ISP de reserva de un proveedor diferente, que utilice una tecnología distinta. - Consulte la sección 2.5c para obtener recomendaciones sobre las conexiones de reserva a Internet.

2.5 Ancho de banda de Internet

El ancho de banda de Internet es la cantidad de datos que pueden enviarse hacia y desde la distribuidora, y suele medirse en bits por segundo. La mayor parte del software de la distribuidora depende de Internet para la comunicación de datos. La información de inventario, las órdenes de trabajo, los manuales de servicio y los datos de los vehículos suelen ser accesibles a través de Internet. Además, muchos empleados y clientes utilizan el acceso a Internet de la distribuidora por motivos personales, como consultar el correo electrónico o navegar por la red. Dado que tantos usuarios dependen de Internet para obtener información, es fundamental que la distribuidora obtenga suficiente ancho de banda para proporcionar a cada recurso el ancho de banda necesario para acceder a los datos con rapidez. Para asegurarse de que la distribuidoras disponga de suficiente ancho de banda, debe elegir la tecnología y la velocidad adecuadas.

En la siguiente sección se detallan las tecnologías disponibles para el acceso a Internet y cómo planificar un ancho de banda suficiente para cada recurso de la red de área local (LAN).

2.5.a Tecnologías de Internet

Tecnología	Descripción	Velocidad	Medio físico	Comentarios
Cable	Se necesita un módem de cable especial y una línea de cable.	La velocidad puede variar, pero suele oscilar entre 10 Mbps y 100 Mbps	Cable coaxial	El servicio de Internet por cable utiliza una infraestructura compartida y puede degradarse con el uso intensivo. Las distribuidoras deberían comprobar qué proveedores de cable tienen ya servicio en la zona. El costo de llevar el servicio a una zona y zanjar el cable puede ser prohibitivo. Ford recomienda que las distribuidoras adquieran cable de calidad empresarial y soliciten al proveedor un acuerdo de nivel de servicio (SLA) u objetivo de nivel de servicio (SLO) por escrito.
DSL	Esta tecnología aprovecha la parte digital no utilizada de una línea telefónica de cobre normal para transmitir y recibir información. La ADSL es asimétrica, lo que significa que la velocidad de subida del servicio es más lenta que la de bajada. La SDSL es simétrica, es decir, tiene la misma velocidad de subida que de bajada. VDSL es otra tecnología asimétrica que puede ofrecer velocidades de hasta 52 Mbps.	De 128 Kbps a 52 Mbps	Par trenzado (utilizado como medio digital de banda ancha)	Ford recomienda a las distribuidoras que adquieran líneas DSL de nivel empresarial con velocidad de carga y descarga suficiente para ejecutar las aplicaciones del distribuidor Ford. VDSL es la única tecnología de grado DSL recomendada ya que puede ser el único servicio con ancho de banda suficiente para satisfacer los requisitos de ancho de banda recomendados.

T1	Se necesitan líneas y equipos especiales (DSU/CSU y enrutador).	1,544 Mbps	Par trenzado, cable coaxial o fibra óptica	Se pueden unir varias líneas T1 para conseguir velocidades mayores.
Tecnología	**Descripción**	**Velocidad**	**Medio físico**	**Comentarios**
Satélite		6 Mbps o más	Ondas Puede utilizar la conexión telefónica para el tráfico ascendente	El ancho de banda no se comparte. Además, la latencia suele ser alta. Esta alta latencia interfiere a menudo con las aplicaciones de los distribuidores. El satélite no es una tecnología recomendada para los distribuidores.
Fibra	Los tipos de conexión a Internet de los servicios de fibra óptica funcionan a través de una red óptica.	Hasta 300 Mbps	Red óptica	La fibra ofrece velocidades altas, costos más bajos y buenos acuerdos de nivel de servicio. Sin embargo, la disponibilidad es limitada en algunas zonas del país.

2.5.b Planificación del ancho de banda

Empiece por conocer el servicio de Internet actual de la distribuidora

Muchas distribuidoras desconocen su tecnología actual de Internet, su velocidad y su uso. Comprender la tecnología puede ayudar a identificar limitaciones posibles y ahorros de costos. Utilice el gráfico anterior para comprender mejor las distintas tecnologías disponibles en el mercado. Averigüe las velocidades de carga y descarga del ancho de banda del servicio actual (normalmente identificadas en Mbps o Kbps) consultando al ISP distribuidor. Por último, inicie sesión en el dispositivo de puerta de enlace de la distribuidora, pregunte al ISP del distribuidor o busque pruebas en línea para conocer el uso real del ancho de banda.

Planifique los picos de uso

El uso del ancho de banda no siempre es constante. Los distribuidores verán picos de uso en función de los procesos empresariales (como las "horas pico"), los procesos tecnológicos (como la ejecución de copias de seguridad o la descarga de actualizaciones) y el uso por parte de los clientes (como la transmisión de vídeo desde la sala de espera de clientes). Se recomienda que los distribuidores tengan una media de uso en torno al 60 para tener en cuenta picos posibles.

Planificar los avances tecnológicos

La mayoría de los OEM, los DSP y los proveedores de las distribuidoras están desarrollando soluciones que aprovechan aún más las comunicaciones por Internet. Las distribuidoras deben comprender que sus necesidades de ancho de banda no son estáticas, sino que seguirán creciendo a medida que la distribuidora, los proveedores y los socios implementen nuevas tecnologías.

Plan de crecimiento

El IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) afirma que las redes tendrán que ser capaces de soportar tasas de crecimiento anual compuesto del 58 % en ancho de banda. El crecimiento está impulsado por el aumento simultáneo de

usuarios, metodologías de acceso, tarifas de acceso y servicios como el vídeo a la carta y las redes sociales.

Manténgase alerta

Dado que el uso del ancho de banda no es estático, la planificación debe ser una actividad continua. Al obtener visibilidad de los patrones de uso de la distribuidora, un administrador de TI puede anticiparse mejor a una posible limitación del ancho de banda antes de que afecte al rendimiento del negocio de la distribuidora. Se recomienda a las distribuidoras configurar alertas para los picos de uso, el consumo medio o los momentos en los que el ancho de banda no está disponible. Esto mitigará los riesgos, limitará el tiempo de inactividad y permitirá a la distribuidora actualizar antes de que se produzca un impacto significativo en el negocio.

2.5.c Conexión de reserva

La disponibilidad del servicio de Internet es fundamental para los negocios de las distribuidoras. Dado que los distribuidores dependen de Internet para vender y dar servicio a los vehículos, se recomienda disponer de una conexión de reserva.

A la hora de elegir una conexión de reserva, siga las recomendaciones siguientes:

- Utilice un proveedor y una tecnología de Internet diferentes para la conexión de reserva.
- Como mínimo, disponer de un servicio de banda ancha 5G de copia de seguridad o de conmutación por error. Pruebe la señal inalámbrica con antelación para garantizar una intensidad de señal adecuada. Los proveedores de servicios de Internet, la ubicación física y el diseño del edificio son variables que influyen en la intensidad de la señal en cualquier distribuidora.
- STAR recomienda un circuito dedicado para una alta disponibilidad.
- STAR recomienda a las distribuidoras que usen un dispositivo de puerta de enlace que admita la conmutación por error automática para garantizar un tiempo de inactividad mínimo.
- No es necesario que el servicio de respaldo tenga la misma velocidad que la conexión principal, pero debe tener suficiente ancho de banda para soportar las funciones críticas del negocio de la distribuidora.

2.6 Seguridad

La finalidad de la infraestructura de red de una distribuidora es compartir datos y recursos con empleados, clientes y terceros proveedores o socios. Las distribuidoras también deben tomar medidas para garantizar que estos datos se comparten de forma segura. Las distribuidoras deben vigilar tanto las conexiones conocidas como las desconocidas para detectar indicios de pérdida de datos. Una distribuidora debe tomar medidas para proteger los datos en la puerta de enlace y en cada punto final de la red. Deben utilizarse tecnologías, procesos y procedimientos para garantizar que los datos de los distribuidores no acaben en las manos equivocadas.

En la sección siguiente se revisa la protección de la red desde el punto de vista de la puerta de enlace, el escritorio, la gestión de eventos de información de seguridad y la seguridad de los datos, así como desde el punto de vista del cliente, la administración pública y los riesgos y el cumplimiento. Además, encontrará información sobre los procesos y procedimientos de seguridad en la sección 6 titulada "Prácticas de formación, procesos y documentación".

2.6.a Políticas de seguridad

El marco de Políticas de Seguridad de la distribuidora debe ser completo, coherente y estar aprobado por el órgano de gestión de la distribuidora. Es importante garantizar que todas las partes interesadas se comprometan con las políticas y acuerden aplicarlas en todos los aspectos relevantes de la distribuidora.

Las políticas deben reflejar la estrategia de protección de la información -y no al revés-, y para ello es fundamental comprender los requisitos de seguridad. El objetivo básico debe ser la confidencialidad, la integridad y la disponibilidad de los datos y los recursos sensibles, incluidos el entorno físico, la infraestructura de red, las aplicaciones y los datos (tanto físicos como digitales). Sin embargo, esta no es una lista completa, ya que hay muchas otras consideraciones. Por ejemplo, a menudo hay que tener en cuenta el no rechazo, la trazabilidad o la autenticidad.

Además, cada industria tiene sus propias áreas sensibles. Por ejemplo, nos importa mucho más la integridad -que la confidencialidad- de un avión en el aire o de un coche en la autopista que la confidencialidad del historial médico de un paciente (que también puede depender del contexto). Las políticas de seguridad deben reflejar estas consideraciones.

Existen muchas políticas o directivas marco de seguridad listas para usar que pueden seleccionarse y aplicarse en una empresa. Sin embargo, aunque este tipo de marco puede proporcionar una base general, una empresa tendrá que ajustar y desarrollar las políticas para aplicarlas en su contexto empresarial.

2.6.b Gestión de identidades y accesos

La Gestión de Identidades y Accesos (IAM) es un marco fundamental para garantizar que las personas adecuadas tengan un acceso apropiado a la información y a los recursos tecnológicos. La gestión de identidades implica crear, mantener y gestionar las identidades de los usuarios y sus permisos de acceso asociados. La autenticación es el proceso de verificar que un usuario es quien dice ser, normalmente mediante contraseñas, biometría o autenticación multifactor (MFA). La autorización, por su parte, determina lo que un usuario autenticado puede hacer, garantizando que sólo tenga acceso a los recursos necesarios para su función. Las mejores prácticas en IAM incluyen la adopción de un enfoque de confianza cero, la aplicación del principio de mínimo privilegio y la auditoría periódica de los controles de acceso. Estas prácticas son esenciales para proteger los datos sensibles, impedir el acceso no autorizado y garantizar el cumplimiento de las normas reglamentarias.

- Confianza cero.
    - Verificación explícita: Cada solicitud de acceso se verifica minuciosamente. Esto incluye verificar la identidad del usuario, la salud del dispositivo y el contexto de la solicitud (por ejemplo, ubicación, hora del día) antes de conceder el acceso1.
    - Acceso de mínimo privilegio: A los usuarios se les concede el nivel mínimo de acceso necesario para efectuar sus tareas. Esto reduce el riesgo de acceso no autorizado a información sensible.
    - Asumir incumplimiento: El marco funciona bajo el supuesto de que ya se ha producido una infracción o de que podría producirse en cualquier momento. Esta mentalidad impulsa la supervisión y validación continuas de todas las solicitudes de acceso.
    - Autenticación fuerte: La autenticación multifactor (AMF) se utiliza a menudo para garantizar que los usuarios son quienes dicen ser. Esto añade una capa adicional de seguridad más allá de un simple nombre de usuario y contraseña.
    - Supervisión continua: Las actividades de los usuarios se supervisan continuamente para detectar cualquier indicio de comportamiento sospechoso. Esto ayuda a detectar y responder a posibles amenazas en tiempo real.
- Gestión de identidades.
    - Establezca inicios de sesión únicos: A cada miembro de la organización se le proporciona un nombre de usuario único para el sistema y se le asigna acceso a las aplicaciones y funciones necesarias para sus tareas asignadas.
    - Mantener listas de usuarios precisas: Los administradores de red mantienen las listas de usuarios finales y eliminan activamente a los usuarios cuando son dados de baja.
    - Métodos de autenticación fuerte: Autentique a los usuarios exigiendo contraseñas únicas para cada aplicación y sistema al que acceda el usuario. Las contraseñas no deben reproducirse ni repetirse para diferentes aplicaciones, funciones o accesos al sistema. Implantar la autorización multifactor (MFA), la biometría o la tokenización o cualquier combinación para validar la identidad del usuario en el momento de la solicitud de acceso.
    - Gestione activamente los usuarios de terceros: Exija a los usuarios de terceros los mismos criterios que a los usuarios internos y disponga de un proceso dinámico para la eliminación de usuarios de terceros a medida que cambie su necesidad de acceder a sistemas y aplicaciones.
    - Codificar por escrito las políticas y procedimientos de gestión de identidades .
- Gestión del acceso.
    - Definir una política clara de gestión de accesos: Establezca y documente políticas que describan cómo se concede, revisa y revoca el acceso. Esto debería incluir directrices sobre las funciones, permisos y responsabilidades de los usuarios1.
    - Control de acceso basado en roles (RBAC): Asigne derechos de acceso en función de las funciones de los usuarios dentro de la organización. Esto garantiza que los usuarios sólo tengan acceso a la

información necesaria para sus funciones laborales.

- Métodos de autenticación fuerte: Implemente la autenticación multifactor (MFA) para añadir una capa adicional de seguridad. Esto ayuda a verificar las identidades de los usuarios de forma más sólida que el simple uso de contraseñas.
- Revisiones periódicas de acceso: Realice revisiones periódicas de los derechos de acceso de los usuarios para asegurarse de que siguen siendo adecuados. Esto ayuda a identificar y eliminar permisos innecesarios u obsoletos.

- Procesos de incorporación seguros: Asegúrese de que los derechos de acceso se revocan rápidamente cuando un empleado abandona la organización o cambia de función. Así se evita el acceso no autorizado de antiguos empleados.
- Supervisión y auditoría continuas: Supervise continuamente las actividades de los usuarios y los patrones de acceso. Utilice herramientas de auditoría para rastrear y registrar los eventos de acceso, lo que puede ayudar a detectar y responder a actividades sospechosas.
- Federación de identidades e inicio de sesión único (SSO): Implantar la federación de identidades y el SSO para agilizar la gestión de accesos en múltiples sistemas y aplicaciones. Esto reduce la complejidad de gestionar múltiples credenciales.
- Endurecimiento medioambiental: Reforzar la seguridad del entorno en el que operan los sistemas de gestión de acceso. Esto incluye la protección de servidores, redes y puntos finales. También implica prohibir el acceso a espacios donde se guardan datos y sistemas a personas sin una necesidad válida de acceder al espacio físico. No mantenga los datos en espacios sin acceso controlado.

La integración de prácticas sólidas de gestión de identidades y accesos (IAM) es esencial para avanzar por los tres niveles de madurez de la seguridad de la información. En el nivel **inicial (Ad Hoc**), las organizaciones a menudo luchan con procesos IAM incoherentes y reactivos, dejándolas vulnerables a las amenazas de seguridad. A medida que avanzan hacia el nivel **Gestionado (Definido)**, la IAM se vuelve más estructurada y proactiva, con políticas y procedimientos claramente definidos que mejoran la capacidad de la organización para gestionar y mitigar los riesgos. Por último, en el nivel **Optimizado (Avanzado)**, la IAM se integra perfectamente en las operaciones de la organización, fomentando una cultura de seguridad madura que evoluciona continuamente para hacer frente a las amenazas emergentes. Al alinear las prácticas de IAM con estos niveles de madurez, las organizaciones pueden reforzar significativamente su postura general de seguridad y su resistencia.

2.6.c Gestión de parches

Los sistemas operativos de los servidores o computadoras locales necesitan actualizaciones periódicas, muchas de ellas debidas a riesgos de seguridad. Los parches que envía el fabricante suelen ofrecer protección frente a vulnerabilidades nuevas o desconocidas hasta ahora. Es fundamental que estos parches se gestionen, apliquen y verifiquen para garantizar una aplicación confiable y segura. Además, los concesionarios deben prestar especial atención a lo siguiente:

- Sistemas para el final de la vida útil
  - Mantenerse al día con el fin de la vida útil de los sistemas operativos (EOL) ayudará a asegurarse de que la ubicación no está utilizando sistemas operativos que ya no reciben actualizaciones de seguridad u otro tipo de actualizaciones porque el proveedor suspendió el soporte.
  - Por lo general, los proveedores avisan la fecha de caducidad, lo que siempre puede comprobarse en sus respectivos sitios web.
- Dispositivos móviles
  - A menudo, los dispositivos móviles abandonan la protección de la red de un concesionario y se conectan a otra red, a menudo menos segura. Por ello, estos dispositivos pueden considerarse más vulnerables. Es importante que los dispositivos móviles se parcheen con rapidez para limitar el riesgo y la exposición a amenazas y vulnerabilidades.

2.6.d Formación sobre sensibilización en materia de seguridad

La inmensa mayoría de los incidentes de seguridad, incluidas las violaciones de datos, son el resultado de un error humano, como hacer clic en un correo electrónico de phishing, por ejemplo. Del mismo modo que los técnicos reciben formación sobre los últimos avances en vehículos y los vendedores sobre las nuevas características de los vehículos y las técnicas de venta, todos sus empleados deben recibir formación sobre cómo proteger su empresa de robos, filtraciones de datos y otros problemas de seguridad.

El objetivo del programa de formación no es sólo educar a sus empleados, sino influir en su comportamiento. Usted querrá que se conviertan en un cortafuegos humano para la empresa.

La seguridad no debe ser aburrida -si la gente no presta atención, el mensaje no se expandirá-, así que no tema ser creativo con el programa de formación y concientización. El humor, los ejemplos de la vida real y los concursos y juegos son algunas formas de mantener el interés y conseguir el compromiso de los empleados.

Para mantener el compromiso de los empleados, considere la posibilidad de utilizar con más frecuencia módulos de formación en seguridad en línea más breves, en lugar de una sola sesión de formación larga. Este enfoque ayuda a mantener la formación al día sobre los últimos avances en malware y ataques.

- La formación debe ser anual, como mínimo, y abarcar temas como:
  - Concientización sobre ingeniería social: phishing, Business Email Compromise (BEC), vishing, ransomware, navegación web segura
  - Contraseñas
  - Datos sensibles - PII, PCI, PHI, etc. - y tratamiento de datos
  - Intercambio de datos y políticas de uso aceptable
  - Protección y destrucción de datos
  - Seguridad de los dispositivos móviles
  - Redes sociales seguras
  - Violencia laboral
  - Políticas de empresa relacionadas con la seguridad

- Puede ser necesaria una formación complementaria según la función del empleado en la empresa. Por ejemplo, los empleados que manejan las finanzas de la empresa pueden beneficiarse de la comprensión de las formas únicas en que son blanco de la ciberdelincuencia

por el acceso que tienen a las cuentas bancarias. Considere la formación basada en funciones para ayudar a los empleados a comprender la función que desempeñan en la protección de la empresa en sus actividades diarias.
    - Utilice material de concientización sobre seguridad en las salas de descanso y otros espacios exclusivos para empleados, como carteles o folletos que recuerden a los empleados el manejo seguro de los datos de los clientes, la concientización sobre ingeniería social, recordatorios de formación, etc.
    - Utilice los boletines de la empresa, los correos electrónicos, las sesiones de formación en directo y otras funciones de la empresa para reforzar continuamente el mensaje de seguridad.
- Revisar periódicamente los programas de formación y adaptarlos a las nuevas tecnologías, los cambios en la actividad de los concesionarios y las opiniones de los empleados.
- Recursos. Pueden ser gratuitos o de pago, pero algunos de sus socios comerciales pueden ofrecer formación en seguridad en línea para sus empleados.
    - Proveedor de DMS
    - Proveedor de seguros
    - Empresa de contabilidad
    - Estudio jurídico
- Otros recursos:
    - Cómo hacer accesible la formación en ciberseguridad
        - https://www.staysafeonline.org/articles/how-to-make-cybersecurity-training-accesible?utm_source=chatgpt.com
    - SANS Ouch: boletín mensual gratuito de seguridad para empleados
        - https://securingthehuman.sans.org/resources/newsletters/ouch/2016

2.6.e Cumplimiento de la legislación federal

Garantizar que el distribuidor cumple todas las normativas federales, estatales, locales y del sector para instituciones financieras y minoristas, como la Ley Gramm-Leach-Bliley, la Norma de Salvaguardias, el PCI DDS, etc.

- Ley Gramm-Leach-Bliley(GLB) y norma de salvaguardias
    - La Ley de Modernización Financiera de 1999, también conocida como "Ley Gramm-Leach-Bliley" o Ley GLB, incluye disposiciones para proteger la información financiera personal de los consumidores en poder de las instituciones financieras. La Ley Gramm-Leach-Bliley (GLB) exige a las empresas definidas como "instituciones financieras" que garanticen la seguridad y confidencialidad de la información sensible. Dado que los distribuidores alquilan y prestan (aunque sea a través de un tercero), deben cumplir la Ley GLBA.
    - La Norma de Salvaguardias fue promulgada por la Comisión Federal de Comercio (FTC), como parte de la Ley GLB. La Norma de Salvaguardias exige a las entidades financieras que adopten medidas para mantener segura la información de sus clientes.
    - Para más información sobre estas legislaciones y los requisitos, visite:
      http://www.ftc.gov/privacy/privacyinitiatives/glbact.html
      https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying
- Norma de seguridad de datos del sector de las tarjetas de pago (PCI DSS)
    - PCI DSS es una norma mundial de seguridad de la información elaborada por el Payment Card Industry Security Standards Council (PCI SSC). La norma se creó para ayudar a las organizaciones que procesan pagos con tarjeta a prevenir el fraude con tarjetas de crédito mediante un mayor control de los datos y su exposición a riesgos.

- Todos los comerciantes que almacenen, acepten, procesen o transmitan datos de titulares de tarjetas deben cumplir los requisitos técnicos y operativos establecidos por PCI DSS. Todos los concesionarios deben cumplir la norma PCI DSS. Sin embargo, existen diferentes requisitos de información y auditoría para las distribuidoras en función del nivel de comerciante. El nivel de comerciante viene determinado por el número de transacciones con tarjeta de crédito realizadas en la distribuidora. Para más información sobre PCI DSS y estos requisitos, visite: https://www.pcisecuritystandards.org

- Recursos adicionales
  - Las siguientes organizaciones disponen de información para ayudar a implantar salvaguardias adecuadas para los datos:
    - Centro de Recursos de Seguridad Informática Instituto Nacional de Normas y Tecnología (NIST) - http://csrc.nist.gov
    - Estrategia Nacional para la Seguridad del Ciberespacio, Departamento de Seguridad Nacional - http://www.dhs.gov/files/publications/editorial_0329.shtm
    - The SysAdmin, Audit, Network, Security (SANS) Institute las Veinte Vulnerabilidades de Seguridad en Internet más Críticas - www.sans.org/top20
    - Recursos y herramientas CISA
      - https://www.cisa.gov/resources-tools
    - Centro de Coordinación CERT del Instituto de Ingeniería de Software Carnegie Mellon - www.cert.org
    - Cuestionario Estrella de Evaluación de Riesgos - https://www.starstandard.org/index.php/risk-assessment- cuestionario-2/

2.6.f Seguridad de la red

Las distribuidoras deben centrarse en la seguridad y la integridad de los datos de su red de área local (LAN). Esto empieza con políticas sobre el uso de la red para empleados e invitados. Estas políticas deben incluir a qué datos tiene acceso cada usuario, a qué recursos de la red puede acceder cada usuario y dónde se almacenan los datos en la red. Las políticas también deben indicar deliberadamente en qué dispositivos se almacenan los datos de la empresa. Consulte la sección 2.6.a para obtener más orientación sobre políticas y prácticas de seguridad.

Más allá de las políticas, la red debe configurarse y segmentarse de la forma más segura posible para evitar accesos no deseados. Siga las siguientes recomendaciones a la hora de configurar y proteger la red de la distribuidora.

Recomendación	Especificación
Firewall/UTM	Dispositivo de seguridad totalmente gestionado que ejecuta supervisión continua de las amenazas mediante el sistema de detección de intrusiones "IDS", el sistema de prevención de intrusiones "IPS" y otros mecanismos. El dispositivo también debe tener las siguientes características: • Mecanismos como el filtrado de paquetes, el antivirus y la inspección de paquetes con estado • Filtrar paquetes y protocolos (por ejemplo, IP, ICMP) • Escaneo con antivirus • Inspección de estado de las conexiones • Realizar operaciones proxy en las aplicaciones seleccionadas • Informar del tráfico permitido y denegado por el dispositivo de seguridad de forma periódica (por ejemplo, mensualmente) Debido a la importancia del firewall y al hecho de que a menudo se encuentra en la ruta de datos de la mayor parte del tráfico de las distribuidoras, STAR recomienda un dispositivo de reserva en caso de fallo. Para limitar el tiempo de inactividad, los distribuidores deberían considerar una solución de conmutación automática al dispositivo de reserva en caso de fallo del hardware.
Segmentación de la red	La información de las tarjetas de pago, la información de los clientes, el tráfico de la distribuidora y el tráfico de los clientes deben segmentarse mediante una segmentación de red (como VLAN) o una red diferente (como un circuito dedicado para invitados) para garantizar la seguridad de los datos.
Filtrado de contenidos	La pérdida de datos puede deberse a que los empleados naveguen por Internet para actividades no relacionadas con la empresa. STAR recomienda a las distribuidoras filtrar el contenido de la red para eliminar el tráfico potencialmente dañino, inapropiado o no relacionado con el negocio.

Gestión de eventos de información de seguridad (SIEM)	Una solución SIEM proporciona visibilidad más allá de la protección antivirus o de firewall. El objetivo último de una solución SIEM es recopilar e inspeccionar el tráfico de seguridad de la red para encontrar indicios de peligro. Esta indicación debe enviarse, en forma de alerta, a un recurso cualificado para que lleve a cabo una investigación y posibles actividades correctoras de inmediato. Es importante señalar que la adopción de software SIEM por sí sola no es suficiente para proteger la red del distribuidor. Las distribuidoras deben disponer de procesos y recursos para responder a la información generada por la tecnología SIEM. Las directrices generales para la gestión de la información de seguridad de las distribuidoras son las siguientes. Las distribuidoras deben tener lo siguiente: • Supervisión proactiva de eventos en tiempo real que utiliza un servicio SIEM.
Recomendación	**Especificación**
	• SIEM debe ser capaz de recopilar datos con capacidad para agregar y correlacionar datos de seguridad variables de la red en tiempo real. • El proveedor de servicios SIEM debe ser capaz de notificar al administrador de la red en caso de que se produzca un incidente de seguridad, así como de proporcionar la documentación adecuada a efectos de cumplimiento de la normativa. • El objetivo último de un servicio SIEM es ayudar a identificar o prevenir una intrusión en su red. La respuesta inmediata a una violación puede reducir en gran medida o evitar la pérdida de datos. **Nota**: No hay que confundir un software de gestión reactiva (por ejemplo, firewall o antivirus de escritorio) con un servicio SIEM proactivo.
Pruebas de penetración y exploración de vulnerabilidades	Se recomienda encarecidamente realizar pruebas anuales de penetración internas y externas de la red de distribuidores. Una prueba de penetración ("pen test") es un método de evaluación de la seguridad de un sistema informático o de una red mediante la simulación de un ataque procedente de una fuente maliciosa. Debe realizarse una prueba de penetración en cualquier sistema informático que vaya a desplegarse en un entorno de red, en particular, en aquellos que tengan algún sistema expuesto o con acceso a Internet. Los compromisos de pruebas de penetración se pueden realizar externamente (simulación de un ataque desde fuera de su red y exactamente igual que si se lanzara un intento de pirateo desde un país extranjero), o se pueden realizar internamente (desde dentro de su red para ver qué accesos y vulnerabilidades existen).
Socios integradores certificados	Asegúrese de que los integradores de datos del distribuidor están certificados con aplicaciones DMS y OEM. Los puntos de integración no autorizados u hostiles suelen ser menos seguros y, a veces, exigen que la distribuidora comparta información de usuario y contraseña.
Sistema de detección inalámbrico	Escanee, identifique y elimine cualquier punto de acceso inalámbrico fraudulento que pueda haber en la red del minorista. Un punto de acceso inalámbrico no autorizado se define como un punto de entrada inalámbrico a la red de la distribuidora que no está autorizado, protegido o conocido por el departamento de TI, la dirección y los propietarios de la distribuidora. Todas las redes inalámbricas fraudulentas deben detectarse, encontrarse y eliminarse de inmediato. STAR recomienda el uso de un servicio gestionado de detección inalámbrica que ejecute un escaneo continuo de la red en busca de amenazas inalámbricas.
Control continuo	La supervisión continua proporciona visibilidad en tiempo real y pruebas de que los controles de seguridad y las medidas de protección de datos funcionan para detectar y prevenir las amenazas. Utilizar tecnologías, procesos y procedimientos de supervisión continua para garantizar que la distribuidora tenga la capacidad de alertar y responder a ataques y vulnerabilidades.

Autenticación multifactor	Implemente la autenticación multifactor (MFA) para todas las cuentas privilegiadas y los usuarios que necesiten acceso remoto. Utilice la AMF para cualquier persona (empleado, proveedor o cliente) que necesite acceder a sistemas que contengan información de clientes.

2.6.g Seguridad del escritorio

Recomendación	Especificación
Supervisión de virus de PC	Los productos antivirus de nivel empresarial deben instalarse en todos los PC y configurarse para que realicen automáticamente las siguientes acciones: • Descargue e instale las actualizaciones de firmas de virus más recientes • Control activo de virus • Ponga en cuarentena y erradique los archivos infectados
Recomendación	**Especificación**
	• La solución antivirus debe incluir antivirus, antispyware, prevención de intrusiones, control de aplicaciones, control de spam y detección de rootkits
Gestión de parches	STAR recomienda que la gestión de parches se realice en cada PC para asegurar que cada estación de trabajo tiene los parches de Microsoft actualizados. La gestión de estaciones de trabajo debe incluir la supervisión remota de fallos de hardware o software, servidores inactivos, poco espacio en disco, uso excesivo de CPU y uso excesivo de memoria.
Protección por contraseña	Las contraseñas deben caducar cada 60 días o menos. Como mínimo, las distribuidoras deben utilizar "contraseñas seguras" que contengan un mínimo de 8 caracteres compuestos por 3 de los 4 requisitos siguientes: 1) Mayúsculas 2) Minúsculas 3) Numérico 4) Caracteres especiales
Plataforma de detección y respuesta a puntos finales	• Una plataforma de protección de puntos finales (EPP) y una solución de detección y respuesta de puntos finales (EDR) singulares deben desplegarse en los dispositivos de puntos finales para prevenir los ataques de malware basados en archivos, detectar la actividad maliciosa y proporcionar las capacidades de investigación y reparación necesarias para responder a incidentes y alertas de seguridad dinámicos. Se debe responder de inmediato a las alertas de este servicio para mitigar el riesgo y la posible pérdida de datos. La oferta de servicios debe proporcionar visibilidad multiplataforma de las actividades del punto final/servidor, así como: Detección de amenazas mediante motores de IA estáticos y de comportamiento y HIDS dentro del agente de punto final • Orientación para la contención y corrección de amenazas • Informes de actividad y caza de amenazas • Visibilidad multiplataforma de la ejecución de procesos, las comunicaciones de red, el acceso a archivos, las aplicaciones, las solicitudes DNS y el tráfico web cifrado

2.6.h Seguridad del correo electrónico

Visión general: La seguridad del correo electrónico es un riesgo crítico para muchas de las mayores organizaciones del mundo. Hoy en día, el 91 % de todos los ataques con éxito a redes empresariales implican el uso del correo electrónico. Una solución de seguridad del correo electrónico proporcionará inspección de contenidos entrantes y salientes, cifrado y alertas de seguridad para mitigar muchos de estos riesgos.

Seguridad del correo electrónico saliente: Identifique y responda al malware, los correos electrónicos inapropiados, los contenidos no autorizados y la información privada de la empresa antes de que salga de la red.

Seguridad del correo electrónico entrante: Aplique filtros para detener el malware, el phishing o los correos electrónicos maliciosos antes de que entren en la red.

Cifrado: Se recomienda el cifrado de correo electrónico TLS para dificultar que terceros lean el correo electrónico en tránsito.

2.6.i Seguridad de las aplicaciones

A continuación, supongamos que todas las aplicaciones se adquieren a proveedores externos y se implantan sin ninguna modificación, o que sólo se aplica una pequeña personalización. Además, por aplicación se entienden las aplicaciones empresariales, y la seguridad de las aplicaciones consiste en garantizar que todos los datos procesados -y todas las funciones empresariales que ofrece la aplicación- estén debidamente protegidos.

- Ámbitos y actividades clave
    - Realizar un inventario de las aplicaciones. Documente qué aplicaciones hay en la red de la distribuidora, cuál es su finalidad, quién es el responsable y cómo obtener asistencia. Realizar análisis de impacto en el negocio (BIA), incluida la clasificación de la información para comprender la criticidad del negocio y aplicar la priorización correcta. Este catálogo también ayudará a encontrar y eliminar aplicaciones no autorizadas que pueden convertirse en una amenaza para la red del distribuidor y la seguridad de los datos.
    - Proteger la información procesada en tránsito y en almacenamiento. Asegúrese de que los datos sensibles y críticos están bien protegidos, tanto desde el punto de vista de la confidencialidad como de la integridad. Revise tanto las integraciones de aplicación a aplicación como las aplicaciones de comunicación interna, especialmente las conexiones a bases de datos, que muy a menudo se olvidan. Si es necesario, asegúrese de que se utiliza la criptografía correcta para la protección en el almacenamiento. Por último, asegúrese de que los flujos de información están protegidos de extremo a extremo.
    - Tenga en cuenta requisitos empresariales adicionales como la autenticidad, el no rechazo o la trazabilidad; a menudo necesarios para cumplir la normativa sobre privacidad (por ejemplo, el GDPR).
    - Aplique el principio de defensa en profundidad introduciendo una configuración precisa de las zonas de seguridad y la ubicación de los componentes de las aplicaciones, servicios de infraestructura adicionales como proxies inversos o firewalls de aplicaciones web, y capas de control de acceso como la autenticación multifactor, etc.
    - Introducir la estrategia adecuada de gestión de identidades y accesos (más información en la sección IAM). Aplicar los principios de mínimo privilegio y necesidad de conocer.
    - Espere de un proveedor el resultado de un escaneo de vulnerabilidad de aplicaciones realizado por una empresa tercera independiente. Asegúrese de que se abordan todos los riesgos altos y medios identificados.
    - Parte de una estrategia de seguridad consiste también en asegurarse de que las transacciones comerciales se gestionan sin errores y con el nivel de calidad esperado. Por ello, cabe esperar que una empresa proveedora facilite resultados de pruebas o informes de auditorías.
    - Introducir procesos para gestionar incidentes, solicitudes de acceso, etc. Considere la posibilidad de introducir la supervisión de las aplicaciones empresariales para rastrear o incluso prevenir eventos no deseados. Suele formar parte de la implantación de la gestión de servicios informáticos.
    - Realice actividades periódicas de modelado de amenazas para asegurarse de que los riesgos del entorno de las aplicaciones se documentan, mitigan y mantienen bajo control.
    - Aplique las actualizaciones y los parches de las aplicaciones lo antes posible para limitar la exposición a posibles vulnerabilidades.

2.6.j Movilidad

Este ámbito está estrechamente relacionado con otros, como la seguridad de las aplicaciones o del correo electrónico. Sin embargo, se considera por separado debido a los riesgos adicionales que introduce por un control mucho menor de los tipos de dispositivos definidos. Los dispositivos móviles se definen aquí como teléfonos inteligentes, tabletas, ordenadores portátiles y cualquier otro dispositivo especializado que procese o almacene datos de la empresa.

- Áreas y actividades clave
  - Crear políticas y procedimientos sobre quién, cuándo y cómo acceder a distancia al entorno de la empresa y a qué partes (red, servidores, aplicaciones, etc.) Por ejemplo, una política puede permitir que los teléfonos inteligentes y las tabletas accedan a una red externa de la empresa y restringir el acceso a la red interna de la empresa; y permitir el acceso a la red interna de la empresa a los portátiles gestionados a través de VPN. Implantar una solución técnica adecuada para apoyar el enfoque establecido.
  - Defina qué información se puede procesar y almacenar en los dispositivos móviles; asegúrese de incluir consideraciones relacionadas con los dispositivos gestionados y no gestionados.
  - Introducir políticas, procedimientos y capacidades técnicas para definir qué software puede instalarse y ejecutarse en todo tipo de dispositivos móviles. En el caso de dispositivos no gestionados, introduzca condiciones en las que los datos de la empresa no estén expuestos a riesgos inaceptables (por ejemplo, instalando soluciones como MobileIron o Microsoft iTunes para smartphones).
  - El acceso a los dispositivos debe estar restringido y exigir la autenticación del usuario. La mayoría de los dispositivos pueden bloquearse con un bloqueo de pantalla, una contraseña o un PIN.
  - Aplicar la estrategia adecuada de gestión de identidades y accesos.
  - Asegúrese de la correcta configuración y endurecimiento del dispositivo y del sistema operativo (por ejemplo, contraseña de la BIOS, cifrado a nivel de dispositivo, disponibilidad de puertos USB y SD). Asegúrese de que (especialmente en el caso de dispositivos Android e iOS) el dispositivo no está enrutado ni liberado.
  - Mantenga un software antimalware actualizado y, preferiblemente, gestionado de forma centralizada, tanto en portátiles como en teléfonos inteligentes.
  - Actualice el sistema operativo móvil con parches de seguridad. Encontrará más información sobre la gestión de parches en la sección 2.6.c.
  - Aplique un cifrado adecuado de los datos tanto en los ordenadores portátiles como en los dispositivos móviles, prestando especial atención a la gestión de claves para el descifrado.
  - Revise todos los métodos de conectividad, teniendo cuidado con la conectividad inalámbrica automatizada, ya que las contraseñas pueden quedar expuestas y pueden ejecutarse ataques de intermediario.
  - Active la opción de borrado remoto de datos si está disponible.
  - Haga copias de seguridad periódicas del dispositivo móvil.
- Consideraciones sobre la política de "traiga su propio dispositivo" (BYOD)
  - Cuando el distribuidor no provee los dispositivos móviles que usan los empleados o los contratistas para fines empresariales, sino que son propiedad personal del empleado o contratista, es necesaria una política BYOD detallada, que debe abordar los siguientes aspectos clave, además de las áreas y actividades clave ya mencionadas:

- Designe qué teléfonos móviles, tabletas, etc. están permitidos; es posible que los dispositivos antiguos no tengan el nivel de seguridad necesario para proteger adecuadamente los datos privados de la empresa.

- Asegúrese de que queda claro que TODOS los datos recopilados en el transcurso de la actividad empresarial son propiedad de la empresa.
- Identifique qué aplicaciones no están permitidas en el dispositivo.
- Utilice casilleros de contraseñas cifradas en lugar de gestores de contraseñas sin cifrar basados en navegadores, especialmente para el acceso a aplicaciones empresariales.
- Exigir la autenticación multifactor (AMF) para el acceso a las redes empresariales.
- Implemente software o aplicaciones que separen el uso personal del empresarial, como una aplicación de navegador controlada por el equipo de Tecnología de la Información de la empresa.
- Definir limitaciones en el uso de datos empresariales y su eliminación cuando ya no sean necesarios para el uso empresarial.
- Dejar clara la política de borrado de dispositivos en caso de incidente de seguridad de la información, el borrado puede provocar la pérdida de datos personales como fotos e información de contacto personal.
- Definir los requisitos para la notificación de dispositivos perdidos y la capacidad de borrado remoto en caso de pérdida o robo de un dispositivo.
- Deje claro que los BYOD están sujetos a supervisión y que los usuarios no deben tener ninguna expectativa de privacidad con respecto al uso o los datos empresariales.
- Todos los datos empresariales son propiedad de la empresa y serán accesibles a petición de ésta.
- En caso de cese de la relación laboral, la limpieza de los datos de los dispositivos personales debe formar parte del proceso de desvinculación. Las empresas deben tener capacidad de acceso remoto para borrar los datos privados de un dispositivo en caso de que un empleado se marche sin previo aviso.
- Exigir el cifrado de dispositivos y el uso de VPN para uso empresarial.
- Impartir capacitación sobre el uso adecuado de los dispositivos personales para la empresa y las políticas para definir el uso adecuado de las aplicaciones empresariales y los datos empresariales con los dispositivos personales.

2.7 Proveedores de servicios gestionados

Los distribuidores suelen recurrir a proveedores o socios para que les ayuden a gestionar, mantener y proteger la infraestructura de la distribuidora. Un proveedor de servicios puede disponer de la tecnología o los conocimientos necesarios para ofrecer a la distribuidora una solución que le permita gestionar con mayor eficacia distintos aspectos de la red de distribuidores. Los distribuidores no suelen disponer del tiempo, los recursos o los conocimientos necesarios para gestionar una red empresarial por sí solos. Por lo tanto, recurrir a un proveedor de servicios podría ser una opción lógica.

Un acuerdo de nivel de servicio (SLA) es muy importante a la hora de seleccionar a un tercero que preste asistencia en infraestructuras de red. El proveedor se comprometerá a informar sobre el nivel de servicio que se puede esperar, el alcance de los servicios y las posibles devoluciones o compensaciones por el incumplimiento de los compromisos.

En la siguiente sección se ofrecen algunas orientaciones para seleccionar y comprender los acuerdos de nivel de servicio.

2.7.a Acuerdos de nivel de servicio (SLA)

Las distribuidoras que reciben servicios de TI confían mucho en el Acuerdo de Nivel de Servicio (SLA) que eligen. El SLA detallará la Calidad de Servicio (QoS) que el proveedor ofrece con su servicio - en otras palabras, su garantía de que el servicio cumplirá lo prometido.

Los acuerdos de nivel de servicio se utilizan en una amplia variedad de servicios de TI para distribuidores, entre los que se incluyen (entre otros):

- Servicio de Internet
- Servicios de integración de redes
- Servicios de asistencia de hardware y software
- Asistencia in situ
- Servicio de asistencia y centro de llamadas

Cuando elija un proveedor de servicios, asegúrese de hacer las siguientes preguntas sobre los acuerdos de nivel de servicio.

- ¿Existe un acuerdo de nivel de servicio por escrito?
- ¿Cuáles son los contratiempos, reembolsos u otras consecuencias si el proveedor no cumple su SLA?
- ¿Hay informes disponibles en relación con el SLA?
- ¿Se puede cancelar el servicio si no se cumple el SLA?

Los acuerdos de nivel de servicio más habituales son (entre otros):

- Disponibilidad de la red
- Velocidad de la red
- Latencia de la red
- Tiempo de sustitución del hardware
- Horas de asistencia disponibles
- Compromisos de servicio in situ
- Contratos de mantenimiento de hardware o software

2.8 Gestión de datos

2.8.a Copia de seguridad de datos

Tener una copia de seguridad de los datos de la distribuidora es fundamental para la continuidad del negocio. Es habitual que la disponibilidad de los datos se convierta en un problema grave debido a incidentes de ciberseguridad, incidentes físicos o errores humanos. Cuando se producen estos incidentes, es importante que las distribuidoras dispongan de una copia de seguridad y un plan de restauración. STAR recomienda a las distribuidoras realizar una copia de seguridad completa e incremental a intervalos regulares para garantizar la disponibilidad y redundancia de los datos.

Copia de seguridad de datos	Debe hacerse una copia de seguridad de los datos de servidores, terminales y equipos de red y guardarla en otro lugar.	Más referencias: Secciones 2.2.c y 2.4.a

2.8.b Seguridad de los datos (cifrado)

El cifrado en las redes informáticas es el proceso de convertir los datos en un formato seguro al que sólo pueden acceder o descodificar las partes autorizadas. El cifrado de datos garantiza que la información solo sea accesible cuando sea necesario y a los destinatarios designados. STAR aconseja a las distribuidoras que implanten el cifrado en las redes inalámbricas, las comunicaciones por correo electrónico, los terminales y las conexiones remotas (VPN).

Siga las siguientes directrices a la hora de utilizar el cifrado en la arquitectura de su distribuidora.

Cifrado inalámbrico	WPA2 con autenticación RADIUS y cifrado AES. Nota: Consulte las recomendaciones del OEM para obtener orientación sobre la compatibilidad de las tecnologías específicas del OEM.
Cifrado de correo electrónico	Se recomienda el cifrado de correo electrónico TLS para dificultar que terceros lean el correo electrónico en tránsito.
Cifrado de extremos	Aplique un cifrado adecuado de los datos tanto en las computadoras portátiles como en los dispositivos móviles, prestando especial atención a la gestión de claves para el descifrado.
Cifrado VPN	Exigir el cifrado de dispositivos y el uso de VPN para uso empresarial.

2.8.c Gobernanza de la Inteligencia Artificial (IA)

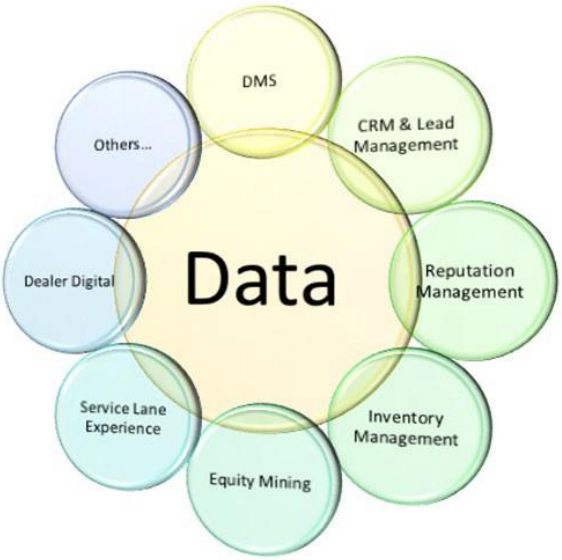
La IA es una gran herramienta para mejorar la eficiencia de las distribuidoras, obtener inteligencia adicional y realizar análisis de datos avanzados. Sin embargo, el uso de la IA en las distribuidoras plantea problemas de seguridad de los datos de distribuidores, clientes y fabricantes. Cuando utilice herramientas de IA, tenga en cuenta las siguientes consideraciones:

- Anonimización y minimización de datos: Anonimizar los datos personales, recopilar sólo la información necesaria y aplicar políticas de conservación de datos para reducir el riesgo.
- Gestión segura de modelos de IA: Mantenga los modelos separados de los sistemas de producción, aplique el control de versiones y realice pruebas periódicas para detectar vulnerabilidades.
- Evaluación de la seguridad de los proveedores: Investigar a fondo a los proveedores de IA, garantizar el cumplimiento de la normativa y auditar periódicamente sus medidas de seguridad. + Asegúrese de que los requisitos de gobernanza y seguridad de datos de todos los proveedores son coherentes con sus propias políticas y requisitos normativos.
- Capacitación y concientización de los empleados: Imparta capacitación periódica sobre seguridad, eduque al personal sobre las amenazas y fomente una cultura de concientización sobre la seguridad.
- Consideraciones sobre el intercambio, la propiedad y el uso de los datos. Asegúrese de que los datos proporcionados o compartidos con un modelo de IA no se comparten, venden o utilizan para fines distintos de los previstos para la distribuidora.

3. Proveedores de sistemas de distribución

3.1 Visión general

La complejidad de una distribuidora y su tecnología asociada ha evolucionado mucho desde la creación de STAR. Esta tecnología en constante evolución ha seguido mejorando el valor empresarial global de STAR y las normas de integración utilizadas para alinear los datos entre sistemas y procesos.



Aunque un sistema de gestión de distribuidores (DMS) ha sido tradicionalmente el núcleo del ecosistema tecnológico de los distribuidores, ahora hay muchos sistemas diferentes que necesitan compartir datos para garantizar que los clientes, los vehículos y las piezas se puedan gestionar de forma eficaz a lo largo de todo el proceso en línea y sin conexión. Este ecosistema de proveedores de servicios para distribuidores (DSP) está en constante cambio, y es absolutamente fundamental garantizar la implantación de procesos para una integración de datos segura y eficaz.

Las opciones de DSP cambian día a día, y es fundamental que los distribuidores comprendan la importancia de una integración de datos segura y eficaz.
Hay soluciones DSP que se centran en el lado cliente de la distribuidora y otras que se centran en el lado interno. Otras soluciones están orientadas a gestionar a los clientes desde la red a fuera de ella y algunas buscan específicamente ayudar a las distribuidoras con la comercialización del inventario de vehículos nuevos/usados, la gestión y distribución de contenidos o a mantener una imagen positiva en las redes sociales y en el mundo online.

Tanto si se trabaja con un proveedor que ofrece numerosos productos como con uno especializado en una función específica, es importante asegurarse de comprender cómo se integrarán y gestionarán los datos en todo el ecosistema.

No existe un enfoque único para implantar una solución DSP en una distribuidora, pero es de vital importancia alinear las tecnologías con las prioridades empresariales e implantar procesos de gobernanza de datos que respalden la experiencia deseada del cliente. Los clientes esperan cada vez más una experiencia en línea y sin conexión sin fisuras, que sólo puede lograrse mediante la integración de datos.

La distribuidora dispone de un gran número de opciones a la hora de decidir qué DSP utilizará en su red. Los DSP suelen servir de "centro neurálgico" de los datos, las comunicaciones y las operaciones comerciales de los distribuidores. Al revisar varias ofertas de DSP, la sección STAR DIG Dealer Network Infrastructure puede proporcionar orientación sobre las diferentes funciones que un proveedor de servicios de sistema puede ofrecer a las distribuidoras.

3.2 Integración de datos y normas: La prestación STAR

La organización STAR y las normas de integración que contiene se crearon para optimizar las actividades de integración de datos de los distribuidores entre el OEM y el DSP (principalmente DMS al principio) utilizando Internet como medio principal.

Como toda tecnología, Internet no ha dejado de evolucionar, y la infraestructura utilizada para que las empresas que la utilizan funcionen ha experimentado una enorme cantidad de innovaciones. Estas mejoras han dado lugar a un método extremadamente confiable para integrar los procesos empresariales y los sistemas asociados.

En el núcleo de todos estos sistemas se encuentran los datos necesarios para apoyar el proceso empresarial deseado. Los

datos de vehículos, recambios, clientes, servicios, finanzas y muchos otros grupos de datos deben pasar de un sistema a otro -y entre el distribuidor (junto con el DSP) y el OEM- de forma fluida y segura. Las normas de integración de datos STAR son

normas abiertas que permiten a vendedores y fabricantes de equipos originales reducir el tiempo total de desarrollo y simplificar las implantaciones mediante un conjunto de documentos que describen los elementos de datos necesarios para apoyar los objetivos empresariales (BOD - Business Object Documents).

Con el tiempo, estas BOD pueden mejorarse con definiciones/reglas empresariales y alinearse con diversas metodologías de transporte de datos para proporcionar integraciones de datos eficientes y repetibles. Cuando STAR comenzó este viaje tan importante, el ecosistema era mucho más sencillo. Dado que el panorama tecnológico de los distribuidores se complica cada año que pasa, las normas empezarán a mostrar realmente las ventajas de STAR

3.3 Panorama tecnológico de los distribuidores (opciones de DSP)

Parece que el panorama tecnológico de los distribuidores estará en constante cambio en el futuro inmediato. Dedicar cualquier cantidad de tiempo a intentar definir este panorama sólo daría como resultado un documento que quedaría obsoleto poco después de su publicación.

En los últimos años, varias categorías de productos DSP nuevas y significativas se han unido al DMS tradicional y han dejado una huella permanente en el ecosistema minorista del automóvil, por lo que merece la pena ofrecer un poco de información sobre sus antecedentes. Al igual que con todas las opciones de DSP, uno debe tomar tiempo para comparar las capacidades y asegurarse de que la solución se alinea con las Directrices de Infraestructura STAR.

Además de comparar las capacidades y comprender la integración general, es extremadamente importante entender la gestión de datos y los elementos de inclusión/exclusión asociados a la solución. La gobernanza completa de los datos y la transparencia de uso son cruciales para cualquier solución DSP/OEM.

3.3.a DMS

El Dealer Management System (DMS) es un sistema de gestión de la información creado específicamente para las distribuidoras del sector automotriz. También se ha adaptado (normalmente como producto DMS especializado) para distribuidores de maquinaria pesada, embarcaciones, bicicletas, vehículos recreativos y equipos para deportes de motor. El DMS contiene funcionalidades para dar soporte a los componentes de finanzas, ventas, inventario, recambios, servicio y contabilidad/oficina comercial para el funcionamiento de la distribuidora.

Algunas soluciones DMS se ofrecen con servidores centrales in situ, y otras se ofrecen aprovechando "la nube" mediante un modelo de software como servicio (SaaS); una solución in situ o basada en SaaS podría ser adecuada, en función de las necesidades de la distribuidora. Una consideración importante es el mantenimiento del hardware que se utiliza para dar servicio a las necesidades de las aplicaciones. Los servicios SaaS se generan en la nube y no necesitan mucho mantenimiento, mientras que las soluciones in situ suelen demandar gestión de parches, actualizaciones y mantenimiento general del servidor.

Aunque la funcionalidad general de ambas soluciones es similar de un DMS a otro, las capacidades específicas pueden variar. En todos los casos, es fundamental garantizar que la solución sea compatible con las normativas estatales/locales/de mercado/regionales y con las marcas OEM para el grupo de distribuidoras específico.

3.3.b CRM y gestión de clientes potenciales

Los sistemas de gestión de relaciones con los clientes (CRM) y de gestión de clientes potenciales se utilizan para capturar, seguir y gestionar con eficacia la correspondencia en línea y sin conexión con clientes potenciales y clientes.

Las soluciones CRM y Lead Management requieren la integración con los datos DMS (clientes) y todas las fuentes de leads (prospectos).

El sistema CRM ofrece funcionalidades que ayudan al personal de la distribuidora a gestionar la relación con el cliente a lo largo de todo su ciclo de vida. Se pueden gestionar las fechas clave del cliente y del vehículo, las citas de servicio y muchos otros aspectos.

El sistema de gestión de clientes potenciales ofrece funciones para asignar clientes potenciales al personal de ventas y servicios (o a través de un centro de desarrollo empresarial definido) para su seguimiento. Todas estas actividades de seguimiento de clientes potenciales tienen como objetivo aumentar las ventas y los ingresos.

Los leads (consultas) se recopilan y almacenan a partir de muchas fuentes diferentes, entre las que se incluyen:

- Sin cita previa
- Contactos en línea adquiridos
- Contactos OEM
- Contactos telefónicos
- Captación de clientes potenciales

Las soluciones CRM y Lead Management también se aprovechan para generar nuevos negocios. Al alinear las soluciones de los distribuidores con los manifiestos de los OEM, otras soluciones DSP (por ejemplo, Equity Mining) y las necesidades de los vehículos usados, es posible llegar de forma eficaz a los clientes existentes y crear negocio adicional.

Las distribuidoras necesitan disponer de la infraestructura necesaria para atender a los clientes potenciales de las empresas de nivel 3. Una solución eficaz de gestión de clientes potenciales también debe tener en cuenta a las organizaciones de nivel 3 (como cars.com y truecar.com).

3.3.c Gestión de la reputación

Una solución de gestión de la reputación ofrece funciones que le ayudan a supervisar, comprender, identificar y abordar lo que la gente escribe en línea sobre su distribuidora.

Una solución de gestión de la reputación requiere la integración con fuentes de datos DMS y OEM.

La reputación online de una distribuidora viene definida por los comentarios encontrados en sitios de opiniones de clientes, blogs, sitios web y redes sociales. Internet facilita la búsqueda de información sobre una distribuidora con poco esfuerzo. En unos pocos clics, un cliente tiene una instantánea de lo que es una distribuidora, dónde está situada y qué opinan los clientes sobre la distribuidora en general. En la mayoría de los casos, los resultados de la búsqueda incluyen valoraciones con estrellas y reseñas. Estas valoraciones y reseñas influyen en la decisión de un cliente de comprar un vehículo a una distribuidora.

3.3.d Gestión de inventario en línea

Una solución de gestión de inventario de distribuidores ofrece funciones que permiten la comercialización, la gestión de contenidos y la distribución del inventario de vehículos. Esto incluye la distribución dirigida por el distribuidor del inventario de vehículos nuevos o usados en stock a publicaciones web o impresas, junto con fotos de los vehículos, vídeos, precios, incentivos, etc.

Una solución de gestión de inventario de distribuidores necesita integraciones con el DMS, herramientas de fijación de precios de terceros, proveedores de servicios de lotes, proveedores de servicios de descripción de vehículos (validación de VIN y datos de fabricación) y OEM.

3.3.e Minería de participación de capital

Una solución de Equity Mining proporciona funcionalidad para identificar a los consumidores que tienen participación de capital en su vehículo y luego proporcionarlos como clientes potenciales de ventas a través de un Centro de Desarrollo de Negocios (BDC), gestor de Internet, equipo de ventas u otros representantes del distribuidor apropiados.

Una solución de Equity Mining demanda la integración con datos DMS (clientes), CRM/LM (clientes potenciales), fuentes de

intercambio, datos bancarios (financiación y leasing) e incentivos.

3.3.f Herramientas de vía de servicio

Service Lane Tools es una solución basada en procesos o flujos de trabajo que engloba funcionalidades que tradicionalmente se han encontrado en soluciones independientes relacionadas con el servicio (es decir, DMS, programación de servicios en línea, menús de servicio, comprobaciones del estado del vehículo, etc.). Permite una experiencia del cliente coherente y sin fisuras a través de las etapas de 1) programación de la cita, 2) redacción del servicio, 3) vehículo en servicio y 4) nueva entrega del servicio.

Service Lane Tools necesita integración con fuentes de datos DMS y OEM.

3.3.g Distribuidor digital

Un paquete de marketing digital para distribuidores es un conjunto de servicios de marketing minorista que permite a los distribuidores enviar mensajes coherentes y sincronizados a los consumidores a través de canales digitales y emergentes. Proporciona una plataforma inteligente de marketing en red con alineación de marketing de marcas y distribuidores. También proporciona análisis que respaldan la optimización del gasto en marketing de varios niveles y la mejora del rendimiento de la red de distribuidores en los procesos de marketing y ventas.

Las soluciones Dealer Digital necesitan integración con fuentes de datos DMS, CRM y

OEM. Los componentes principales de una solución Dealer Digital pueden incluir lo

siguiente:

- Sitio web del distribuidor (web y móvil)
- Optimización de motores de búsqueda (SEO)
- Gestión de audiencias
- Información y análisis
- Gestión de activos (imágenes, vídeos , etc.)
- Chat
- Citas

4. Recuperación en caso de catástrofe y continuidad comercial

4.1 Visión general

La recuperación en caso de catástrofe y la continuidad de la actividad es la capacidad de una organización para recuperarse de una catástrofe y reanudar el funcionamiento normal de la red. Las distribuidoras deben contar con un plan en el que se detallen la tecnología, los procesos y los pasos procedimentales a seguir en caso de avería. La clave del éxito de la recuperación en caso de catástrofe es contar con un plan mucho antes de que se produzca la interrupción.

Los planes de recuperación y continuidad de las actividades en caso de catástrofe son procesos que ayudan a las organizaciones a prepararse para situaciones de emergencia, ya sea un tornado devastador o simplemente una línea de Internet averiada por las repetidas heladas y descongelaciones.

Para saber qué podría ocurrir en caso de fallo de la red, se recomienda a la distribuidora que comprenda primero qué datos están en peligro. ¿Durante cuánto tiempo pueden no estar disponibles esos datos? ¿Qué ocurre cuando no está disponible? ¿Qué medidas pueden adoptarse para mitigar el riesgo? En esta sección se detallan algunas respuestas básicas a esas preguntas, así como algunas recomendaciones para planificar con antelación a los fallos, así como para restablecer el funcionamiento de la red.

4.2 Análisis y mitigación de riesgos

El objetivo principal del análisis de riesgos es ayudar a la distribuidora a identificar todas las áreas en las que puede haber

riesgo de pérdida. Puede tratarse de hardware, software, edificios, personal, etc. Una vez identificados los distintos elementos, la distribuidora puede clasificar el nivel de cada riesgo y determinar cómo le afecta.

A continuación se enumeran algunas de las distintas categorías de riesgo a las que puede enfrentarse una distribuidora .

- Personal clave
- Edificio
- Interrupción o fallo de Internet
- Fallo del sistema de llaves
- Fallo total del sistema
- Pérdida de datos

Una organización puede mitigar los riesgos de varias maneras. Estos planes o soluciones pueden ser in situ o externos. A continuación, algunos ejemplos de cada uno de ellos.

Opciones de mitigación de riesgos in situ	Opciones de mitigación de riesgos externos
Hardware redundante	Software de copia de seguridad remota
Software y servidores de copia de seguridad de datos in situ	Almacenamiento en la nube
Sistema de alimentación ininterrumpida (SAI)	Contratos de servicio de hardware RMA
Generadores	

5. Computación en nube y virtualización

5.1 Visión general

Las importantes tendencias emergentes en Tecnologías de la Información pueden resumirse en un paradigma basado en los servicios y la virtualización. Con un "paradigma basado en servicios", condensamos diferentes acrónimos como Arquitectura Orientada a Servicios (SOA) y el popular concepto de Cloud Computing (que tiene implicaciones empresariales relevantes). *"La principal tecnología habilitadora de la computación en nube es la virtualización. La virtualización proporciona la agilidad necesaria para acelerar las operaciones de TI y reduce los costes al aumentar la utilización de la infraestructura."* (Wikipedia)

5.2 Virtualización cliente/servidor

Virtualización, en informática, significa crear una versión virtual de un dispositivo o recurso, como un servidor, un dispositivo de almacenamiento, una red, etc., donde el "marco" divide el recurso en uno o más entornos de ejecución. Las aplicaciones y los usuarios humanos pueden interactuar con el recurso virtual como si fuera un único recurso físico real. En un entorno de distribuidor, las áreas más relevantes para la virtualización son la Virtualización de Servidores y la Virtualización de Clientes; ambas son interesantes y aseguran ahorros constantes.

5.3 Computación en nube

"La computación en nube es un modelo que permite el acceso ubicuo, cómodo y bajo demanda a un conjunto compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente aprovisionados y liberados con un mínimo esfuerzo de gestión o interacción con el proveedor de servicios". (Definición del NIST - Instituto Nacional de Normas y Tecnología)

La computación en la nube se basa en compartir recursos para lograr economías de escala, de forma similar a una empresa de servicios públicos (como la red eléctrica), a través de una red. En la base de la computación en la nube está el concepto más amplio de servicios compartidos y estandarizados, explotados con un modelo de consumo.

Según el NIST, el modelo de nube se compone de tres modelos básicos de servicio.

- Software como servicio (SaaS): capacidad ofrecida al consumidor para utilizar las aplicaciones del proveedor que se ejecutan en una infraestructura de nube.
- Plataforma como servicio (PaaS): capacidad ofrecida al consumidor para desplegar en la infraestructura de la nube aplicaciones creadas por el consumidor o adquiridas mediante lenguajes de programación, bibliotecas, servicios y herramientas compatibles con el proveedor.
- Infraestructura como servicio (IaaS): capacidad proporcionada al consumidor para suministrar procesamiento, almacenamiento, redes y otros recursos informáticos fundamentales en los que el consumidor puede desplegar y ejecutar software arbitrario, que puede incluir sistemas operativos y aplicaciones.

El correo electrónico y el CRM ya son utilizados por muchos distribuidores con un modelo SaaS. Muchos proveedores de DMS ya ofrecen algo parecido a un modelo SaaS para su DMS. Los otros 2 modelos rara vez son adoptados por los distribuidores, con algunas excepciones (por ejemplo, IaaS para desastres/recuperación es una opción interesante).

6. Prácticas de formación, procesos y documentación

Muchos expertos argumentarán que la mayoría de las violaciones de datos se deben a errores humanos. En años anteriores, estudios realizados por Nuspire Networks, IBM, Verizon y The Ponemon Institute han llegado a la conclusión de que la mayor amenaza para los datos de los distribuidores podrían ser los empleados. Más allá de la seguridad, los empleados suelen ser la causa de las caídas de la red, los fallos de los dispositivos y la lentitud de las operaciones empresariales. La mayoría de las veces, la causa no son unos empleados deficientes, sino una capacitación y una documentación deficientes. A menudo, los empleados provocan un incidente de seguridad, no saben utilizar los sistemas y/o provocan un fallo de la red porque no han recibido capacitación sobre lo que deben o no deben hacer. Esta falta de capacitación de los empleados puede conducir a menudo a una falta de documentación.

La siguiente sección cubre consejos y directrices de formación desde una perspectiva tanto tecnológica como de seguridad de los datos. Se anima a las distribuidoras a adoptar políticas y procedimientos de capacitación. Estas políticas deben estar bien documentadas y utilizarse con la capacitación de los empleados. La documentación, los procesos y los procedimientos por sí solos pueden tener un impacto positivo en las operaciones de la red y en la seguridad de los datos de los distribuidores.

6.1 Capacitación para los empleados

Recomendación	Especificación
Capacitación en seguridad	Disponga de un programa formal y escrito de capacitación en seguridad para cada empleado. La capacitación debe abarcar aspectos como la concientización sobre la ingeniería social, la gestión de contraseñas, las políticas de intercambio de datos y los procedimientos de tratamiento de datos sensibles. Revisar periódicamente los programas de capacitación y adaptarlos a las nuevas tecnologías, los cambios en la actividad de los distribuidores y las opiniones de los empleados.
Responsabilidad de seguridad diseñada	Designe a un empleado como coordinador del programa de seguridad de la información.
Capacitación en sistemas informáticos para distribuidores	Proporcionar capacitación formal para aplicaciones críticas, hardware y otros sistemas informáticos del distribuidor. Un empleado bien informado puede aumentar la productividad, reducir los costos de asistencia y mejorar la satisfacción del cliente.

6.2 Proceso

Recomendación	Especificación
Acceso para nuevos empleados	Disponga de un proceso formal por escrito para conceder a los nuevos empleados acceso al sistema. Esto debe incluir nombres de usuario y contraseñas únicos.

Acceso de empleados dados de baja	Disponga de un proceso formal por escrito para retirar a los empleados de la red de TI del distribuidor, recuperar el hardware de la distribuidora y desactivar todas las cuentas de los empleados antes de que se marchen.
Capacitación en sistemas informáticos	Disponer de un programa formal para abordar la capacitación de las tecnologías, aplicaciones y hardware de la distribuidora. Un empleado bien informado puede aumentar la productividad, reducir los costos de asistencia y mejorar la satisfacción del cliente.
Evaluación de riesgos	Identificar los riesgos internos y externos razonablemente previsibles para la seguridad, confidencialidad e integridad de la información de los clientes. Diseñar y aplicar salvaguardias para el cliente a fin de controlar los riesgos identificados mediante la evaluación de riesgos.
Controles de seguridad de terceros (proveedores)	La selección de proveedores de servicios de confianza es muy importante. Seleccione proveedores de servicios con experiencia en la protección de la información de los clientes de un distribuidor.
Gestión y respuesta a incidentes de seguridad	Disponer de un proceso formal para responder a los incidentes de seguridad en la red. Cubrir aspectos relacionados con la identificación de fallos de seguridad, la respuesta, la comunicación y la documentación.

6.3 Documentación

Recomendación	Especificación
Documentación de seguridad	Crear una política de seguridad escrita que aborde las normas técnicas, de proceso y administrativas para tratar la seguridad de los datos de los clientes. La documentación debe incluir lo siguiente: • Capacitación para los empleados • Respuesta y gestión de incidentes e infracciones • Acuerdos sobre el uso de Internet por los empleados • Políticas y procedimientos de supervisión y gestión de redes
Documentación para empleados nuevos	Disponga de un programa escrito para las nuevas contrataciones. Esto debe incluir capacitación sobre seguridad, capacitación sobre sistemas y un proceso documentado para solicitar asistencia técnica informática.
Documentación de sistemas	Ofrezca formación sobre aplicaciones críticas, hardware y otros sistemas informáticos del distribuidor. Un empleado bien informado puede aumentar la productividad, reducir los costos de asistencia y mejorar la satisfacción del cliente.

7. Apéndices

7.1 Guía de la política de seguridad de los distribuidores

El marco de Políticas de Seguridad de la distribuidora debe ser completo, coherente y estar aprobado por el órgano de gestión de la distribuidora. Es importante garantizar que todas las partes interesadas se comprometan con las políticas y acuerden aplicarlas en todos los aspectos relevantes de la distribuidora.

Las políticas deben reflejar la estrategia de protección de la información -y no al revés-, y para ello es fundamental comprender los requisitos de seguridad. El objetivo básico debe ser la confidencialidad, la integridad y la disponibilidad de los datos y los recursos sensibles, incluidos el entorno físico, la infraestructura de red, las aplicaciones y los datos (tanto físicos como digitales). Sin embargo, esta no es una lista completa, ya que hay muchas otras consideraciones. Por ejemplo, muy a menudo hay que tener en cuenta el no rechazo, la trazabilidad o la autenticidad.

Además, cada industria tiene sus propias áreas sensibles. Por ejemplo, nos importa mucho más la integridad -que la confidencialidad- de un avión en el aire o de un coche en la autopista que la confidencialidad del historial médico de un paciente (que también puede depender del contexto). Las políticas de seguridad deben reflejar estas consideraciones.

Existen muchas políticas o directivas marco de seguridad listas para usar que pueden seleccionarse y aplicarse en una

empresa. Sin embargo, aunque este tipo de marco puede proporcionar una base general, una empresa tendrá que ajustar y desarrollar las políticas para aplicarlas en su contexto empresarial.

Directrices generales

- Asegúrese de que existe un entendimiento compartido con la Dirección sobre lo que debe protegerse, así como sobre el nivel de ambición en materia de protección de datos. Por un lado, es importante que las políticas garanticen un nivel de protección esperado. Sin embargo, también es especialmente importante que las políticas no sean tan restrictivas que impidan a la empresa realizar las actividades necesarias.
- Asegúrese de que las políticas están en consonancia con las leyes y normativas (por ejemplo, en el ámbito de la privacidad o las normativas específicas del sector).
- Desarrollar políticas que reflejen las prácticas de seguridad reales y realizables. Es mejor tener un pequeño conjunto de normas que un documento exhaustivo imposible de seguir. Por si acaso el estado real dista mucho del nivel de ambición, elabore un plan de transición acordado por todas las partes interesadas clave para llevar a una organización del nivel actual al nivel esperado. Es especialmente importante desarrollar un plan de comunicación eficaz como parte del programa general de seguridad.
- Las políticas no deben modificarse con demasiada frecuencia (incluidos el modo y el lenguaje en que se expresan). No obstante, si es necesario, deben aplicarse los cambios oportunos, ya que siempre deben reflejar los requisitos de seguridad y las estrategias de seguridad de la información actuales.
- Las políticas deben expresarse de forma que no haya lugar para excepciones. Esto está relacionado tanto con el compromiso de todas las partes interesadas de seguir las políticas como con el lenguaje. De lo contrario, especialmente cuando se permiten muchas excepciones, la cuestión puede llegar a ser si la Dirección está realmente comprometida con la política o si la política refleja realmente la estrategia de la empresa para la protección de la información.
- Las políticas deben expresarse de forma que no haya lugar a interpretaciones. Además, las políticas deben apoyarse en directrices, procesos, procedimientos, funciones con responsabilidades e interpretaciones para que quede claro qué hacer en casos concretos. También debe quedar claro a quién dirigirse en caso de necesitar una interpretación o una decisión. También es una buena práctica mantener los artículos de la base de conocimientos.
- Asegúrese de que se dispone de las soluciones y tecnologías adecuadas para respaldar las expectativas políticas. Por ejemplo, cuando una política exige la autenticación de dos factores en circunstancias específicas, es importante que el entorno informático existente permita implementar este nivel adicional de protección.
- Introducir un cuadro de mandos para hacer un seguimiento del nivel de aplicación de las políticas, que permita una gestión confiable de los riesgos, así como la priorización de los esfuerzos.

Las directrices con ejemplos de políticas consideradas especialmente válidas desde la perspectiva de una distribuidora son las siguientes.

7.1.1 Política de uso aceptable

Describe el uso aceptable de los recursos físicos y digitales de una empresa. Abarca también la propiedad y el control. Haga hincapié en los ejemplos de actividades prohibidas.

7.1.2 Política de gestión de activos

Los activos representan todo lo que tiene valor para la organización. Los activos de la empresa se consideran tanto en su dimensión física como lógica.

Físico. Servidores, discos duros, enrutadores, teléfonos móviles, medios extraíbles como DVD o memorias USB, por ejemplo. Es importante hacer un seguimiento del ciclo de vida de los activos, prestando especial atención a su eliminación y reutilización.

Lógico. Es importante que una empresa desarrolle normas que regulen la recogida, conservación y uso adecuados de los datos. Estas normas deben considerar qué información se recoge, cuánto tiempo se guarda, cómo se almacena, quién puede acceder a ella y cómo se consigue el acceso. Esto está muy relacionado con la función creciente de la regulación de la privacidad en los distintos países.

Además, debe desarrollarse una política de clasificación de la información con requisitos claros de propiedad y protección de la información a distintos niveles. Es tan importante que a veces se considera en una política independiente e identificable.

7.1.3 Política de aplicaciones empresariales

Introducir una política de clasificación de aplicaciones empresariales. Describir los requisitos de protección a nivel de aplicación para los distintos niveles de criticidad (por ejemplo, colocación de zonas de seguridad, métodos de conectividad, control de identidad y acceso, aplicación de la defensa en profundidad, fallar de manera segura, privilegio mínimo y principios similares). Incluya las expectativas relativas a la arquitectura de la aplicación, la comunicación con otros sistemas y la separación de datos entre clientes. Definir las expectativas hacia las soluciones basadas en la nube (cada vez más populares).

Otros aspectos que hay que especificar es la forma en que la empresa adquiere una aplicación, cuáles son los pasos obligatorios, cuáles son los requisitos comunes hacia los proveedores tanto funcionales como no funcionales (por ejemplo, SLA, seguridad, gestión de identidades, integraciones). Definir las auditorías esperadas de la aplicación adquirida (por ejemplo, informes Pentest o Vulnerability Scan). Políticas de apoyo con plantillas y directrices para compartir con los proveedores.

7.1.4 Política de comunicación electrónica

En la era tecnológica actual, las empresas tienen muchas opciones de comunicación e intercambio de información. Sin embargo, estas opciones conllevan riesgos. Por ejemplo, uno puede utilizar un servicio en la nube para comunicarse, pero también está recopilando datos con intenciones maliciosas. Es importante regular la comunicación electrónica, como los correos electrónicos y la mensajería instantánea, utilizando tableros como Trello, el intercambio de archivos a través de Dropbox y soluciones y plataformas similares.

7.1.5 Política de gestión de identidades y accesos

Una de las áreas más críticas. Encontrará más detalles en la sección correspondiente de esta directriz. La política de contraseñas debe incluirse en esta sección.

7.1.6 Política de gestión de incidentes de seguridad

No existe ningún entorno informático que pueda asegurarse al 100 %. Una empresa debe estar preparada para cuando se produzca un incidente de seguridad. La política de gestión de incidentes de seguridad debe formar parte de la gestión global de incidentes, o contribuir con ella. Proporcionar la definición de incidente de seguridad, introducir procesos y procedimientos (es decir, plan de respuesta) para saber qué hacer en caso de incidente de seguridad (dependiendo de la categoría del incidente, por ejemplo, piratería informática, comportamiento incorrecto, fallo del equipo), y la criticidad. Definir los procedimientos exactos de respuesta y actuación. Por ejemplo:

- Si un ordenador está en peligro, desconéctelo inmediatamente de la red.
- Si alguien entra sin tarjeta de acceso, pregunte por su identidad.
- Considera una investigación forense adicional.
- Considerar las correcciones de emergencia para apoyar los Planes de Continuidad de Servicio y de Negocio.

- Considere a quién notificar en caso de incidente, tanto dentro como fuera de la organización. Puede ser necesario informar a las siguientes partes: consumidores, fuerzas de seguridad, clientes y agencias de crédito y otras empresas que puedan verse afectadas por la violación.

- A menudo también existen leyes y normativas que exigen un comportamiento específico en caso de que se produzca una violación de datos y que dependerán del país, el estado y el sector.

La política también puede esperar introducir soluciones técnicas apropiadas para apoyar su aplicación.

Encontrará información más específica sobre la respuesta a incidentes en: https://www.sans.org/reading-room/whitepapers/incident.

Puede encontrar modelos de formularios y documentación para la gestión de incidentes en https://www.sans.org/score/incident-formularios.

7.1.7 Política de red

La política de red es otro aspecto muy importante de la seguridad general. A la hora de desarrollar una política de red, se recomienda tener en cuenta los siguientes aspectos:

- Definir clases de zonas de red con organización de apoyo (propietario de zona, operador de zona, etc.), asignar nivel de confianza a cada clase, definir conexiones permitidas entre diferentes niveles de confianza. Introducir segmentos de red más restringidos para aplicaciones y datos más sensibles.
- Una lista de los dispositivos de red y las configuraciones asociadas, así como qué se debe permitir conectar y a dónde.
- Conexiones de red externas, VPN (tanto para empleados como para socios externos)
- DNS, incluida la estructura de nombres, así como la infraestructura de apoyo y el ámbito de aplicación
- Firewalls, proxy inverso y configuraciones de proxy (por ejemplo, que todo el tráfico saliente pase por un proxy, que todo el tráfico entrante sensible pase por el proxy inverso)
- Clases y normas inalámbricas sobre autenticación y protección en tránsito. Segmentos de clientes separados, específicos y muy limitados.
- Mantenimiento a distancia
- VoIP, telefonía y conferencias

7.1.8 Política de gestión de riesgos y auditoría

Definir el marco de riesgos y las consideraciones de auditoría de apoyo. Describir los requisitos para la evaluación de riesgos y las auditorías de la información y los recursos de la empresa.

7.1.9 Política de gestión de amenazas y vulnerabilidades

Una evaluación/escaneo de vulnerabilidades identificará los puntos débiles de seguridad en su ordenador, sistemas de red y, posiblemente, aplicaciones. Se realiza con herramientas que escanearán automáticamente su entorno de ordenadores, aplicaciones y componentes de red en busca de lo que actualmente son vulnerabilidades conocidas con el fin de exponer cualquier vulnerabilidad que detecte. Estas exploraciones también se realizan con las credenciales administrativas necesarias para realizar los diagnósticos seguros dentro de los sistemas a los que sólo puede acceder un nivel administrativo.

El resultado proporcionaría un nivel de gravedad y promovería una acción correctiva recomendada para cada problema detectado. Estas exploraciones deben realizarse periódicamente, como mínimo una vez al año, pero se recomienda que sean al menos dos veces al año o más.

Una prueba de penetración ("pen test") es un método para simular un ataque real y evaluar así la seguridad de un sistema informático y un entorno de red. No se realiza con ningún acceso administrativo como para emular a un actor hostil no autorizado. Es diferente de un escaneo de vulnerabilidades en que intentará encontrar una vulnerabilidad real y explotarla si está presente. La prueba de penetración intentará replicar métodos maliciosos de violación de estos sistemas para mostrar cómo la amenaza puede interrumpir, detener, sobrepasar o robar de esos sistemas, pero lo haría de una manera que sólo pruebe que podría realizar esas acciones sin dañar realmente los sistemas objetivo. Los sistemas internos accesibles desde Internet deben evaluarse desde un punto de acceso externo (basado en Internet), desde un sistema que emule a una entidad hostil que ataca desde lejos, desde fuera de la red de la empresa, como el ejemplo de un intento de pirateo lanzado desde un país extranjero. Las pruebas de penetración pueden utilizar algunas herramientas automatizadas, pero se orquestan con un profesional experto en el uso de dichas herramientas y tácticas. Los ataques de ingeniería social también se incluyen en esta prueba para determinar si los errores humanos pueden exponer una debilidad y proporcionar un vector de ataque exitoso, exponiendo el acceso a sistemas y datos que no deberían haber sido proporcionados/expuestos. Además, siempre se recomienda realizar la prueba de penetración física (ataque, evaluación) desde dentro de la red como si la amenaza/ataque se hubiera lanzado desde dentro del entorno de la organización (como si el ataque lograra eludir o frustrar las defensas perimetrales).

Objetivamente, tanto el escaneo de vulnerabilidades como la prueba de penetración deberían realizarse de forma periódica. El ciclo consistiría en realizar el escaneo de vulnerabilidades para identificar y remediar los problemas de vulnerabilidad encontrados. La intención de esto es frustrar idealmente la acción de la prueba de penetración subsiguiente que está intentando derrotar la seguridad explotando las vulnerabilidades que pueden existir/permanecer.

Tenga en cuenta que una protección de punto final de alta calidad instalada en todos los ordenadores/portátiles/servidores/tabletas de punto final es una mejor práctica prescriptiva para reducir la vulnerabilidad, para proporcionar protección contra amenazas supervisada continuamente, prevención y notificación. La mejor solución para que esta protección sea más eficaz es la protección de puntos finales que proporciona comunicación instantánea a un centro de operaciones de seguridad (SOC) para su revisión inmediata por profesionales de la seguridad.

Si desea consultar diversos modelos de políticas de seguridad, visite: https://www.sans.org/information-security-política.

7.2 Guía de gestión de identidades y accesos

Abarcar la gestión de identidades y accesos de forma exhaustiva. Comience con la introducción y los conceptos básicos, seguidos de las subsecciones: gestión de identidades, autenticación, autorizaciones y por qué son tan importantes, proceso de gestión de accesos, usuarios finales y consideración física, y niveles de protección. Concluya con una introducción a los tres niveles de madurez.

7.2.1 Introducción

Gartner, Inc. define la Gestión de Identidades y Accesos (IAM) como una disciplina de seguridad que permite lo siguiente:

- las personas adecuadas para acceder
- los recursos adecuados en
- los momentos adecuados para
- las razones correctas.

Aunque la definición es bastante sencilla, capta la esencia e implica muchas consideraciones en distintos ámbitos.

7.2.2 Conceptos básicos y definiciones

Para establecer una línea de base, defina los términos básicos relacionados con la Gestión de Identidades y Accesos.

- **Entidad**: persona real o sistema de información
- **Identidad**: entidad en un contexto específico (por ejemplo, en el trabajo o en las redes sociales)
- **Identificador**: conjunto de atributos que identifican la identidad (por ejemplo, SSN, correo electrónico, huella dactilar)
- **Autenticación**: proceso de confirmación de la identidad reivindicada por una entidad (por ejemplo, proporcionando una contraseña)
- **Autorizaciones**: conjunto de permisos asignados a alguien o algo (por ejemplo, "está usted autorizado a ver la historia clínica del paciente XYZ")
- **Contabilidad/Auditoría**: historia de lo sucedido

Lo anterior debe considerarse en las dimensiones física y lógica, donde la física se refiere a limitar el acceso a edificios, salas y otros activos informáticos físicos, y la lógica se refiere a limitar el acceso al mundo informático virtual, como conexiones a redes informáticas, sistemas de información, archivos o datos. Una vez implementado lo anterior, introduzca el elemento clave de este rompecabezas.

- **Control de acceso**: consiste en asegurarse de que se ejecutan las reglas de autorización. Se puede considerar como la implementación de autenticación, autorización y contabilidad (AAA) en dimensiones tanto físicas como lógicas.

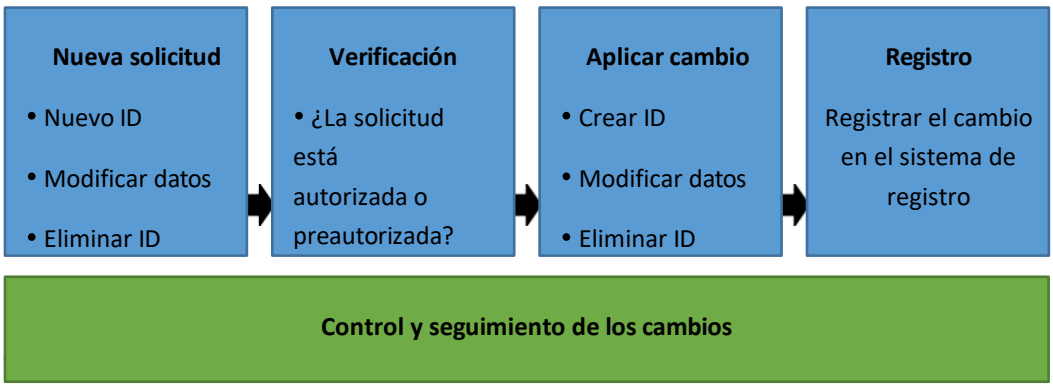
7.2.3 Gestión de identidades

Deben tenerse muy en cuenta los siguientes aspectos de la gestión de identidades:

- Ciclo de vida de las identidades
- Gestión y almacenamiento de identidades
- Gestión de contraseñas
- Federación de identidades

Ciclo de vida de Identidades

El ciclo de vida debe considerarse desde el momento en que comienza una relación hasta el momento en que finaliza, y debe supervisarse a lo largo del tiempo para detectar cambios en el contexto (por ejemplo, si el empleado cambia de destino). El proceso puede ilustrarse del siguiente modo:



Haga hincapié en los siguientes aspectos clave:

- Limite el número de identidades relacionadas con una entidad específica y centralice la gestión de estas (por

ejemplo, intente evitar situaciones en las que existan cuentas específicas de una aplicación).

- Intente evitar las cuentas de grupo. En caso de que sea realmente necesario, de nuevo, asegúrese de que cada uno tiene su propio custodio responsable de ello.
- Recuerde que las identidades no sólo están relacionadas con los usuarios finales, sino también con los servicios o las redes, y que este tipo de identidades también deben gestionarse y mantenerse con cuidado. Asegúrese de que cada identidad no personal tenga su propio custodio responsable de ella.
- Asegúrese de que el almacenamiento de identidades está protegido, especialmente cuando se almacena información confidencial. Suele referirse, por ejemplo, a contraseñas, pero también puede referirse a información sensible del usuario (por ejemplo, coordenadas GPS de lugares visitados).

Se recomienda seguir las normas comunes del mercado y los protocolos de seguridad, así como los productos.

Gestión de contraseñas

Las contraseñas deben estar protegidas tanto en tránsito como en almacenamiento. Además, los procedimientos relativos a las contraseñas deben diseñarse con cuidado. El almacenamiento de contraseñas puede considerarse desde dos perspectivas.

- **Del lado del servidor:** donde se gestiona la identidad (por ejemplo, Active Directory, aplicación empresarial, etc.).
    - Aspectos clave
        - La contraseña no debe almacenarse en texto plano y, en caso de que se cifre de forma reversible, la clave para el descifrado debe protegerse de forma correcta.
        - Todas las contraseñas predeterminadas suministradas por el proveedor deben cambiarse antes de poner en funcionamiento cualquier sistema de información.
- **Del lado del cliente -** donde se utiliza una contraseña para acceder a los recursos. Si es necesario almacenar una contraseña, se recomienda encarecidamente guardarla de forma encriptada (por ejemplo, en una aplicación KeyPass, archivo Excel encriptado). A continuación, es importante proteger la contraseña maestra de forma segura. Es especialmente importante disuadir a los empleados de que anoten las contraseñas y las guarden en un lugar visible para los demás (por ejemplo, en una nota adhesiva cerca del lugar de trabajo)
        - divulgar las contraseñas a nadie a menos que sea absolutamente necesario (por ejemplo, asistencia técnica); y acordarse de cambiar la contraseña después de divulgarla.

    Todas las contraseñas deben cambiarse de inmediato si se sospecha que se las está utilizando o se las reveló a proveedores para mantenimiento/soporte.

    También es importante asegurarse de que todas las copias de seguridad en las que se almacenan

    contraseñas también están protegidas con cuidado. Procedimientos habituales que deben diseñarse de

    forma segura:

        - Enviar la contraseña inicial de forma segura
        - Recuperación de contraseña en caso de olvido
        - Desbloqueo en caso de bloqueo
        - Autoservicio de cambio de contraseña
        - Políticas en torno al ciclo de vida de las contraseñas (véase la sección de políticas para las contraseñas);
          pero recuerde que unas políticas demasiado restrictivas también pueden tener consecuencias

negativas.

Federación de identidades e inicio de sesión único

En caso de que una empresa esté establecida con otros socios a nivel de sistemas informáticos, merece la pena echar un vistazo a la política de federación de identidades. En resumen, se trata de compartir la misma identidad entre empresas sobre la base de cierto nivel de confianza. Existe un conjunto de tecnologías maduras que respaldan este planteamiento. Estos son los beneficios inmediatos:

- Inicio de sesión único: el usuario final necesita autenticarse una vez y obtiene acceso a varias aplicaciones (sin necesidad de volver a autenticarse)
- Menos costos relacionados con la gestión del ciclo de vida de la identidad
- Menor riesgo relacionado con la necesidad de mantener identidades separadas por parte de un usuario final

Al final, hay que hacer un cálculo para determinar si merece la pena invertir en la federación de identidades en un contexto específico.

7.2.4 Autentificación

La prueba más común en la autenticación es la contraseña, pero también hay un problema: las contraseñas son difíciles de recordar. Por ello, cada vez es más popular el uso de frases de contraseña. Hay que recordar que recomendar frases de contraseña obliga a hacer cambios en las políticas, así como en los sistemas informáticos para respaldar las nuevas políticas.

Existen otras opciones de autenticación además de la contraseña, como la biometría, las contraseñas de un solo uso o las tarjetas inteligentes compatibles con RSA Tokens, aplicaciones móviles como Google Authenticator o Yubikey. Cada método suele clasificarse en una de estas tres categorías:

- Algo que conoce (contraseñas, patrones visuales)
- Algo que tenga (tarjeta inteligente, token RSA, smartphone)
- Algo que es (biometría, comportamiento)

Hay dos (2) razones para aplicar diferentes métodos de autenticación:

- Mejor experiencia de usuario (por ejemplo, biometría)
- Mayor seguridad (tarjeta inteligente)

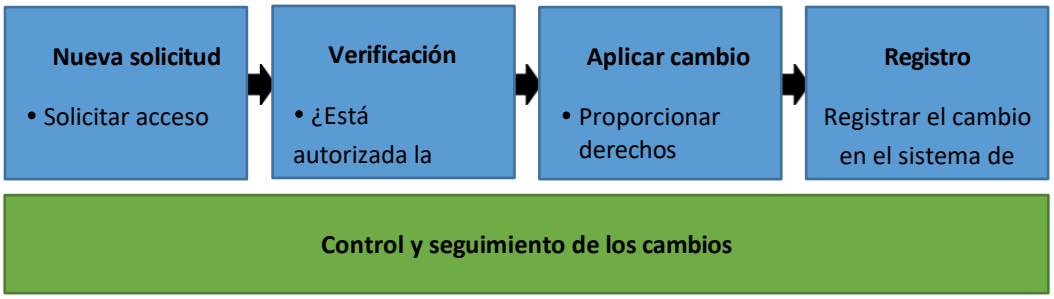
Cuando se combinan dos o más métodos de categorías diferentes, se habla de ***autenticación multifactor***, que consiste en aumentar el nivel de seguridad.

7.2.5 Proceso de gestión de autorizaciones y accesos

Las autorizaciones correctas -es decir, la definición de los permisos y su representación en los sistemas informáticos- son uno de los elementos más importantes del panorama general de la seguridad informática. Los siguientes aspectos deben asegurarse correctamente:

- Definir una estructura de funciones y niveles de acceso.
- Definir un conjunto de permisos para una función determinada.
- Asegúrese de que las autorizaciones estén documentadas y sean de acceso fácil.
- Asegúrese de que se aplican autorizaciones en los sistemas de control de acceso.
- Las solicitudes de acceso son aprobadas por las personas correctas, y está claramente definido quiénes son los aprobadores
- Control y revisiones (auditorías) de los derechos de acceso y las autorizaciones

Además, es necesario establecer y aplicar el ***proceso de gestión de accesos*** para garantizar que las autorizaciones definidas se aplican en todos los lugares y en cualquier momento. El proceso es similar al de la gestión del ciclo de vida de las identidades y puede ilustrarse del siguiente modo:



Los elementos clave de dicho proceso que deben tenerse en cuenta:

- El acceso se revoca o modifica cada vez que un empleado abandona la empresa o cambia de puesto.
- El acceso debe actualizarse oportunamente para reflejar las necesidades de la empresa.
- El acceso debe revisarse periódicamente según una cadencia documentada (trimestral, semestral, anual). Esta evaluación, que no está motivada por la salida o la transición del empleado, tiene por objeto determinar si el nivel de acceso concedido actualmente se corresponde con la posición de la persona en la empresa. Tenga en cuenta que la frecuencia de las revisiones puede variar en función de la criticidad de los activos que se protegen.
- Una buena práctica es también aplicar el principio de "necesidad de saber", es decir, sólo se debe dar acceso a los recursos si existe una necesidad empresarial.

Una vez más, nunca se insistirá lo suficiente en la importancia de supervisar y auditar las autorizaciones y los derechos de acceso, en especial para asegurarse de que la eliminación de accesos se aplica correctamente. Por desgracia, es bastante habitual que se proporcionen derechos de acceso y luego nunca se eliminen.

7.2.6 Usuarios finales y consideración física

Es sabido que la mayoría de los problemas de seguridad suelen deberse a un comportamiento incorrecto de los usuarios. (Las relacionadas con las dimensiones lógicas (como hacer clic en correos electrónicos peligrosos) se tratan en otras secciones) A continuación se exponen los elementos relacionados con el control de acceso físico, que también deben constituir la base de una estrategia educativa adecuada.

- Las salas de servidores/equipos deben estar cerradas con llave. El acceso de los empleados debe limitarse solo a aquellos que tengan una necesidad empresarial legítima. Deben existir mecanismos para saber si alguien accede al sitio y cuándo lo hace.
- Exija que los archivos que contengan datos e información confidenciales se guarden en archivadores cerrados con llave en todo momento, salvo cuando un empleado esté trabajando en el archivo. Además, cuando un empleado esté trabajando en el archivo, asegúrese de que las personas no autorizadas no puedan verlo (por ejemplo, cuando viaja en avión).
- Recuerde a los empleados que no deben dejar documentos ni información confidencial en las mesas cuando no estén en su puesto de trabajo.
- Exija a los empleados que guarden los archivos, cierren los ordenadores y cierren los archivadores y las puertas de las oficinas con llave al final de la jornada.
- Implemente controles de acceso adecuados para su edificio. Indique a los empleados qué hacer y a quién avisar si ven a una persona desconocida en las instalaciones.
- Si se mantienen instalaciones de almacenamiento externas, limite el acceso de los empleados a aquellos que tengan una necesidad empresarial legítima. Deben existir mecanismos para saber si alguien accede al sitio y cuándo lo hace.
- Si se utilizan dispositivos que recopilan información confidencial, como teclados con PIN, asegure el equipo para reducir el riesgo de manipulación. Estos equipos también deben estar protegidos para reducir el riesgo de que un atacante los cambie por un dispositivo ficticio.

7.2.7 Niveles de protección

El control de acceso (incluida la consideración de la identidad) debe tenerse en cuenta en muchos niveles diferentes.

- **Aplicaciones empresariales**: aplicaciones necesarias para gestionar pedidos, programar el trabajo, organizar los RR. HH. y las finanzas, etc. La atención se centra en la protección de la información y las funcionalidades empresariales sensibles. Las identidades suelen referirse a los usuarios finales.
- **Sistemas operativos**: base para ejecutar aplicaciones en portátiles, ordenadores de sobremesa, servidores, teléfonos, tabletas, etc. La atención se centra en la protección de archivos y datos, contra el malware, y en lo que puede soportar el control de acceso. Las identidades suelen referirse a usuarios finales (portátiles, teléfonos, etc.) y servicios (servidores).
- **Dispositivos de infraestructura y servicios de apoyo**: enrutadores, conmutadores, puntos de acceso, servicios de autenticación, etc. Se centra en la protección del tráfico de red correcto, manteniendo la comunicación segura y alejando a los intrusos. Las identidades suelen referirse a usuarios y servicios técnicos.
- **Dispositivos móviles**: dispositivos como teléfonos, tabletas e incluso computadoras portátiles. La atención se centra en la protección de los datos almacenados en los dispositivos y en garantizar que se pueda acceder a ellos de forma segura para incluir situaciones como el uso sin conexión o el robo del dispositivo.
- **Locales/físicos**: edificios, salas de servidores, salas de impresión, oficinas, talleres, salas de exposición, etc. La atención se centra en garantizar que las personas puedan entrar en los lugares adecuados y acceder a los activos adecuados.

Además, se puede asignar lo anterior a las distintas capas de la red:

- Capa de aplicación (por ejemplo, HTTP)
- Capa de transporte (por ejemplo, TCP)
- Capa de Internet (por ejemplo, IP)
- Capa de red (por ejemplo, Ethernet)

Es importante asegurarse de que hay una cobertura completa de la IAM en diferentes capas y áreas de acuerdo con los requisitos que deben basarse en la criticidad de la información.

- Implemente una protección completa en todas las capas y para todos los tipos de aplicaciones y dispositivos, tanto en las dimensiones físicas como lógicas.

7.3 Guía de madurez del nivel de seguridad de la distribuidora

Las distribuidoras suelen tener dificultades para aplicar las recomendaciones de seguridad. Esto suele atribuirse al nivel de madurez de la distribuidora en términos de sofisticación informática y de seguridad. Utilice esta guía para identificar el nivel de madurez de su distribuidora y los pasos por seguir para mejorar la seguridad de la distribuidora.

7.3.1 Orientación para el distribuidor sobre políticas de seguridad

A la hora de determinar los próximos pasos para madurar las políticas de seguridad de una distribuidora, primero hay que identificar el nivel de madurez real de la distribuidora. A continuación, determine las medidas que pueden adoptarse para mejorar la seguridad de la distribuidora. Utilice la siguiente guía como ayuda.

- **Nivel de madurez básico:** Las distribuidoras han identificado y documentado políticas en torno al uso aceptable, la auditoría, la gestión del acceso (incluida la contraseña) y la consideración básica de la red (incluido el acceso externo y las normas inalámbricas).
- **Nivel de madurez intermedio:** Las distribuidoras han identificado y documentado políticas para todas las áreas previstas. Además, cuentan con procesos para entregar, educar y apoyar al personal de la

distribuidora con políticas de seguridad documentadas.

- **Nivel de madurez avanzado:** Las distribuidoras prueban, auditan y perfeccionan periódicamente las políticas y procedimientos de seguridad.

7.3.2 Guía para distribuidores sobre gestión de identidades y accesos (IAM)

A la hora de determinar los próximos pasos para madurar el IAM de una distribuidora, primero hay que identificar el nivel de madurez real de esa distribuidora. A continuación, determine las medidas que pueden adoptarse para mejorar la seguridad de la distribuidora. Utilice la siguiente guía como ayuda.

Nivel de madurez básico

- Procesos explícitos para gestionar el ciclo de vida de las identidades y los derechos de acceso
- Auditorías y revisiones periódicas de los permisos de los sistemas críticos
- Procesos explícitos para la gestión de contraseñas
- Capacitación básica de los empleados (al menos para los recién contratados)
- Sistema de control de acceso a instalaciones físicas críticas

Nivel de madurez intermedio

- Procesos explícitos para gestionar el ciclo de vida de las identidades y los derechos de acceso
- Auditorías y revisiones periódicas de los permisos de los sistemas críticos
- Procesos explícitos para la gestión de contraseñas y recomendaciones sobre el almacenamiento de contraseñas en el lado del cliente
- Capacitación periódica de los empleados
- Sistema de control de acceso a todos los locales físicos
- Nivel de protección (por ejemplo, autenticación multifactor, defensa en profundidad) en relación con la criticidad de la información y las funciones empresariales

Nivel de madurez avanzado

- Procesos automatizados para gestionar el ciclo de vida de las identidades y los derechos de acceso
- Almacenamiento y gestión centralizados de identidades, incluido el nivel adecuado de federación de identidades
- Procesos centralizados de gestión de contraseñas y autenticación
- Recomendaciones (o políticas) firmes sobre el almacenamiento de contraseñas en el lado del cliente
- Nivel de protección (por ejemplo, autenticación multifactor, defensa en profundidad) en relación con la criticidad de la información y las funciones empresariales
- Sistema de control de acceso centralizado para todos los locales físicos
- Capacitación periódica de los empleados
- Auditorías y revisiones periódicas de permisos e identidades
- Protección integral en todas las capas y para todo tipo de aplicaciones y dispositivos, tanto en las dimensiones físicas como lógicas

7.3.3 Orientación del distribuidor sobre la gestión de parches

Nivel de madurez básico: Las distribuidoras tienen cada sistema configurado para actualizarse automáticamente en busca de parches críticos o de seguridad.

Nivel de madurez intermedio: Las distribuidoras disponen de un sistema de gestión de parches para toda la empresa .

Nivel de madurez avanzado: Las distribuidoras prueban, despliegan y validan los parches a medida que están disponibles lo antes posible.

7.3.4 Guía del distribuidor para la recuperación en caso de catástrofe

A la hora de determinar los siguientes pasos para madurar la recuperación ante desastres/continuidad del negocio de una distribuidora, primero hay que identificar el nivel de madurez actual de esa distribuidora. A continuación, determine las medidas que pueden adoptarse para mejorar la seguridad de la distribuidora. Utilice la siguiente guía como ayuda.

- **Nivel de madurez básico:** Las distribuidoras hacen periódicamente copias de seguridad de todos los sistemas.
- **Nivel de madurez intermedio:** Las distribuidoras hacen copias de seguridad incrementales periódicas y almacenan las imágenes de seguridad fuera de sus instalaciones.
- **Nivel de madurez avanzado:** Las distribuidoras despliegan un sistema de continuidad de negocio que incluye copias de seguridad completas del sistema fuera de las instalaciones en un entorno virtual que permitirá a la distribuidora poner en marcha de inmediato la imagen de copia de seguridad en caso de interrupción o fallo.

7.3.5 Orientación para los distribuidores sobre la capacitación en materia de concientización en seguridad

A la hora de determinar los próximos pasos para madurar el programa de concientización de seguridad de una distribuidora, primero hay que identificar el nivel de madurez actual del concesionario. A continuación, determine las medidas que pueden adoptarse para mejorar la seguridad de la distribuidora. Utilice la siguiente guía como ayuda.

- **Nivel de madurez básico:** Todos los empleados reciben capacitación anual sobre seguridad. La finalización de la capacitación se documenta y los informes están disponibles para auditoría. Los empleados pueden no estar seguros de su función en la protección de la organización. La organización puede ser conforme, pero no segura. No existe un proceso establecido o los empleados no se sienten capacitados para denunciar comportamientos sospechosos o pérdidas accidentales de datos.
- **Nivel de madurez intermedio:** El programa de capacitación puede ser más frecuente que anual, y se realiza un seguimiento para garantizar que todos los empleados participan como condición de empleo. Los temas tratados se centran en los mayores riesgos para la organización. En las zonas de descanso de los empleados se ha colocado material de concientización. Los empleados conocen las políticas de seguridad de la empresa y saben cómo reconocer y notificar un incidente de seguridad.
- **Nivel de madurez avanzado:** El programa de capacitación para todos los empleados y contratistas incluye módulos breves pero frecuentes sobre temas oportunos y pertinentes para su función. Se pone a prueba la capacidad de los empleados para defenderse de diversas tácticas de ingeniería social, como el phishing, las descargas de USB, el fraude, etc. Los empleados saben cómo informar de un incidente de seguridad y, cuando se les pone a prueba, al menos el 50 % de los empleados informan de algo sospechoso. En las pruebas, menos del 10 % hace clic en los correos electrónicos de prueba de phishing. La distribuidora tiene una cultura de seguridad: los empleados comprenden su función en la protección de la organización, buscan procesos seguros y animan a sus compañeros de trabajo a llevar a cabo sus actividades de una forma que valore la seguridad y la protección de la organización frente al fraude, el robo y la pérdida accidental de datos o financiera.

7.3.6 Orientación para los distribuidores sobre el cumplimiento de la legislación federal

A la hora de determinar los pasos por seguir para que una distribuidora cumpla con la legislación en materia de seguridad, primero hay que identificar el nivel de madurez actual de esa distribuidora. A continuación, determine las medidas que pueden adoptarse para mejorar la seguridad de la distribuidora. Utilice la siguiente guía como ayuda.

- **Nivel de madurez básico:** Las distribuidoras han investigado PCI y GLBA para determinar el cumplimiento de la legislación federal. Los distribuidores cuentan con políticas y procesos documentados para cumplir la normativa.
- **Nivel de madurez intermedio:** Las distribuidoras examinan y revisan periódicamente el cumplimiento de la legislación federal en materia de seguridad
- **Nivel de madurez avanzado:** Los distribuidores implementan auditorías periódicas de los sistemas y rastrean los resultados hasta los requisitos de la legislación.

7.3.7 Orientación para los distribuidores sobre la seguridad de la red

A la hora de determinar los próximos pasos para mejorar la seguridad de la red de una distribuidora, identifique primero el nivel de madurez actual de esa distribuidora. A continuación, determine las medidas que pueden adoptarse para mejorar la seguridad de la distribuidora. Utilice la siguiente guía como ayuda.

- **Nivel de madurez básico:** Las distribuidoras han elaborado y documentado una política de uso de Internet. Las distribuidoras disponen de protección en la puerta de enlace de la red y han configurado y segmentado la red para evitar accesos no deseados a los recursos de la red. La red se supervisa en tiempo real mediante tecnologías de gestión de eventos de información de seguridad para protegerla de accesos no deseados. El acceso remoto está supervisado y restringido en la red.
- **Nivel de madurez intermedio:** Las distribuidoras han utilizado políticas y procesos documentados para establecer una red de concesionarios segura y segmentada. Las distribuidoras prueban periódicamente la red frente a riesgos conocidos. La red está vigilada 24 horas al día, 7 días a la semana, 365 días al año por expertos en seguridad que utilizan tecnologías de gestión de eventos de información de seguridad. Acceso remoto supervisado y restringido a proveedores y empleados conocidos.
- **Nivel de madurez avanzado:** Las distribuidoras han utilizado políticas y procesos documentados para establecer una red de concesionarios segura y segmentada. Las distribuidoras prueban periódicamente la red frente a riesgos conocidos. La red está supervisada 24 horas al día, 7 días a la semana, 365 días al año por un proveedor de servicios con certificación SOC 2. La red está vigilada 24 horas al día, 7 días a la semana, 365 días al año por expertos en seguridad. Acceso remoto supervisado y restringido a proveedores y empleados conocidos. El acceso de los empleados a la VPN se consigue mediante la autenticación de dos factores.

7.3.8 Orientación sobre el antivirus de la distribuidora

A la hora de determinar los siguientes pasos para mejorar la seguridad audiovisual de un concesionario, primero hay que identificar su nivel de madurez actual. A continuación, determine las medidas que pueden adoptarse para mejorar la seguridad de la distribuidora. Utilice la siguiente guía como ayuda.

- **Nivel de madurez básico:** Las distribuidoras han identificado todos los sistemas y aplicado software antivirus a cada sistema de la red.
- **Nivel de madurez intermedio:** Las distribuidoras disponen de un sistema antivirus empresarial. Esto incluye la gestión de licencias en toda la empresa, un portal empresarial para la elaboración de informes y la respuesta, así como la auditoría y la elaboración de informes en toda la red.
- **Nivel de madurez avanzado:** Los distribuidores emplean respuestas proactivas e inmediatas a las alertas

generadas por la solución audiovisual corporativa.

7.3.9 Orientación para los distribuidores sobre la seguridad del correo electrónico

A la hora de determinar los siguientes pasos para mejorar la seguridad del correo electrónico de una distribuidora, identifique primero el nivel de madurez actual de esa distribuidora. A continuación, determine las medidas que pueden adoptarse para mejorar la seguridad de la distribuidora. Utilice la siguiente guía como ayuda.

- **Nivel de madurez básico:** Las distribuidoras han tomado medidas para implantar tecnologías que protejan sus sistemas de correo electrónico.
- **Nivel de madurez intermedio:** Los distribuidores implementan una inspección y protección activas de la seguridad del correo electrónico entrante y saliente. Los distribuidores cifran los datos confidenciales a través del correo electrónico.
- **Nivel de madurez avanzado:** Las distribuidoras tienen una vigilancia activa del correo electrónico y responden a las amenazas de éste.

7.3.10 Orientación acerca de UTM/Firewall/IDS

A la hora de determinar los siguientes pasos para hacer madurar el sistema unificado de gestión de amenazas, firewall y detección de intrusiones de una distribuidora, primero hay que identificar el nivel de madurez actual de esa distribuidora. A continuación, determine las medidas que pueden adoptarse para mejorar la seguridad de la distribuidora. Utilice la siguiente guía como ayuda.

- **Nivel de madurez básico:** Las distribuidoras despliegan un UTM totalmente gestionado y con licencia que incluye licencias para AV, SPAM e IDS/IPS. Las firmas se actualizan automáticamente en tiempo real.
- **Nivel de madurez intermedio:** Las distribuidoras responden a las alertas y eventos del UTM 24x7x365 en tiempo real. Las distribuidoras utilizan un SIEM (véase la sección 3.5) para alertar y responder a los eventos en la puerta de enlace de la red.
- **Nivel de madurez avanzado:** Las distribuidoras recurren a un proveedor de servicios de seguridad gestionados (MSSP) para la gestión, supervisión y respuesta proactivas de UTM 24x7x365.

7.3.11 Orientación sobre SIEM

A la hora de determinar los próximos pasos para madurar la gestión de eventos de información de seguridad de una distribuidora, primero hay que identificar el nivel de madurez actual de esa distribuidora. A continuación, determine las medidas que pueden adoptarse para mejorar la seguridad de la distribuidora. Utilice la siguiente guía como ayuda.

- **Nivel de madurez básico:** Las distribuidoras instalan y utilizan software SIEM. Todas las alertas se responden prácticamente en tiempo real, 24 horas al día, 7 días a la semana, 365 días al año. Todos los registros del sistema se almacenan de acuerdo con la legislación federal (véase la sección 2.6 sobre el cumplimiento de las legislaciones federales).
- **Nivel de madurez intermedio**: Las distribuidoras recurren a un proveedor de servicios de seguridad gestionados para una supervisión y respuesta avanzadas. Inteligencia de amenazas de integración de distribuidoras para una supervisión y alerta avanzadas.
- **Nivel de madurez avanzado:** Las distribuidoras recurren a un proveedor de servicios de seguridad gestionada (MSSP) con certificación SOC 2 para una gestión, supervisión y respuesta proactivas de UTM 24x7x365. Las distribuidoras integran la inteligencia sobre amenazas en la solución SIEM. La dirección del concesionario y el MSSP revisan periódicamente los tickets, las alertas y la actividad para perfeccionar, documentar y mejorar la postura de seguridad.

7.3.12 Orientación para los distribuidores sobre la seguridad de las aplicaciones

A la hora de determinar los próximos pasos para madurar la seguridad de las aplicaciones de una distribuidora, primero hay que identificar el nivel de madurez actual de esa distribuidora. A continuación, determine las medidas que pueden adoptarse para mejorar la seguridad de la distribuidora. Utilice la siguiente guía como ayuda.

Nivel de madurez básico

- Introducir un catálogo de aplicaciones.
- Mantener una gestión básica de identidades y accesos.
- Aplique actualizaciones y parches de las aplicaciones con regularidad .

Nivel de madurez intermedio

- Mantener un catálogo de aplicaciones que comprenda el análisis del impacto empresarial y la clasificación de la información.
- Aplicación de una estrategia madura de gestión de identidades y accesos .
- Protección de los flujos de información desde la perspectiva de extremo a extremo, tanto en tránsito como en almacenamiento.
- Introducir procesos para gestionar incidentes y solicitudes de acceso.
- Aplicar la estrategia de defensa en profundidad .

Nivel de madurez avanzado

- Aplique todos los puntos de la sección anterior.

7.3.13 Orientación para los distribuidores sobre la movilidad

A la hora de determinar los próximos pasos para madurar la seguridad en movilidad de una distribuidora, primero hay que identificar el nivel de madurez actual de esa distribuidora. A continuación, determine las medidas que pueden adoptarse para mejorar la seguridad de la distribuidora. Utilice la siguiente guía como ayuda.

Nivel de madurez básico

- Mantenga actualizado el software antimalware .
- Definir qué información se puede procesar y almacenar en los dispositivos móviles; incluir consideraciones relacionadas con los dispositivos gestionados y no gestionados.
- El acceso a los dispositivos debe estar restringido y exigir la autenticación del usuario. La mayoría de los dispositivos pueden bloquearse con un bloqueo de pantalla, una contraseña o un PIN.
- Actualice el sistema operativo móvil con parches de seguridad. Encontrará información sobre la gestión de parches en la sección 2.6.3.

Nivel de madurez intermedio

- Todos los elementos del nivel de madurez básico .
- Aplique el cifrado de datos tanto en computadoras portátiles como en dispositivos móviles, prestando especial atención a la gestión de claves para el descifrado.
- Revise todos los métodos de conectividad, tenga cuidado con la conectividad inalámbrica automatizada ya que las contraseñas pueden quedar expuestas, así como puede ejecutarse un ataque del intermediario.
- Crear políticas y procedimientos sobre quién, cuándo y cómo acceder a distancia al entorno de la empresa (red, servidores, aplicaciones, etc.) y a qué partes de dicho entorno. Implantar la solución técnica adecuada para apoyar el enfoque establecido .

Nivel de madurez avanzado

- Aplique todos los puntos de las secciones anteriores.

8. Glosario

802.11: 802.11 es un grupo de especificaciones inalámbricas desarrolladas por el IEEE para comunicaciones de red de área local inalámbrica (WLAN). Detalla una interfaz inalámbrica entre dispositivos para gestionar el tráfico de paquetes y evitar colisiones. Algunas especificaciones habituales son las siguientes: 802.11a, 802.11b, 802.11g, 802.11n, etc. El estándar 802.1X está diseñado para mejorar la seguridad de las redes de área local cableadas e inalámbricas que siguen el estándar IEEE.

Antena: Dispositivo de transmisión y recepción de señales de radiofrecuencia (RF). A menudo camufladas en edificios existentes, árboles, torres de agua u otras estructuras altas, el tamaño y la forma de las antenas vienen determinados en general por la frecuencia de la señal que gestionan.

App (Aplicación): Herramientas descargables, recursos, juegos, redes sociales o casi cualquier cosa que añada una función o característica a un dispositivo inalámbrico y que esté disponible de forma gratuita o de pago. Algunas aplicaciones también pueden ofrecer a los usuarios la posibilidad de comprar contenidos o funciones mejoradas dentro de la aplicación. Los padres pueden limitar la capacidad de sus hijos para descargar o realizar estas compras dentro de la aplicación mediante la protección con contraseña de estas funciones en un dispositivo inalámbrico. La CTIA ha creado un sistema de clasificación de aplicaciones para ayudar a los padres a informarse sobre una aplicación y poder determinar si es apropiada para sus hijos: **https://www.ctia.org/the-wireless-industry/industry- commitments/app-content-classification-ratings-guidelines**

Banda ancha: Instalación de transmisión con un ancho de banda (capacidad) suficiente para transportar simultáneamente varios canales de voz, vídeo o datos. La banda ancha suele equipararse al suministro de mayores velocidades y capacidades avanzadas, incluido el acceso a Internet y los servicios conexos

Cat5: Tipo de cable de par trenzado diseñado para una alta integridad de la señal. Muchos de estos cables no están apantallados, pero algunos sí lo están. La Categoría 5 ha sido sustituida por la especificación de la Categoría 5e. Este tipo de cable se utiliza a menudo en el cableado estructurado de redes informáticas como Ethernet y también para transportar muchas otras señales, como servicios básicos de voz, token ring y ATM (hasta 155 Mbit/s, en distancias cortas).

Cat5e: La especificación de la categoría 5e mejora las especificaciones de la categoría 5 al hacer más estrictas algunas especificaciones de diafonía e introducir nuevas especificaciones de diafonía que no estaban presentes en las especificaciones originales de la categoría 5. El ancho de banda de las categorías 5 y 5e es el mismo: 100 MHz

Cat6: Norma de cable para Gigabit Ethernet y otros protocolos de red que es compatible con las normas de cable de Categoría 5/5e y Categoría 3. La Cat-6 presenta especificaciones más estrictas para la diafonía y el ruido del sistema. El cable estándar ofrece un rendimiento de hasta 250 MHz y es apto para10BASE-T / 100BASE-TX y 1000BASE-T (gigabit Ethernet). Se espera que se adapte a la norma 10GBASE-T (10gigabit Ethernet), aunque con limitaciones de longitud si se utiliza cable Cat-6 sin apantallar. Ford Motor Company recomienda el cableado Cat-6 cuando se instalen nuevos cables o se sustituyan nuevos segmentos de red cableada.

DSL (línea de abonado digital): Línea digital que conecta el terminal del abonado a la oficina central de la compañía de servicio, proporcionando múltiples canales de comunicación capaces de transportar simultáneamente comunicaciones de voz y datos.

Cifrado: Codificación digital de la información para poder transmitirla a través de una red no segura. En el otro extremo, el destinatario suele utilizar una "clave" digital para descifrar la información y devolverla a su forma original.

Computadoras portátiles o tabletas: Estos dispositivos son computadoras que un usuario puede transportar consigo. Suelen ser mucho más pequeños que una portátil normal y no tienen toda la capacidad de una computadora de escritorio, pero pueden ejecutar la mayoría de las tareas necesarias. También permitirán a un usuario hacer trabajos en varios lugares de una distribuidora, lo que puede aumentar la productividad.

IEEE (Instituto de Ingenieros Eléctricos y Electrónicos): Asociación profesional con sede en Nueva York dedicada a fomentar la innovación y la excelencia tecnológicas. Cuenta con unos 425 000 miembros en unos 160 países, algo menos de la mitad de los cuales residen en Estados Unidos.(**http://www.ieee.org**)

LAN (red de área local): Una red de área local (LAN) es una red de datos pequeña que cubre un área limitada, como un edificio o un grupo de edificios. La mayoría de las LAN conectan estaciones de trabajo o computadoras personales. Esto permite a muchos usuarios compartir dispositivos como impresoras láser, así como datos. La red LAN también facilita la comunicación, ya sea por correo electrónico o mediante sesiones de chat.

Malware: Malware (por "software malicioso") es cualquier programa o archivo que sea dañino para un usuario de computadora. Así, el malware incluye virus informáticos, gusanos y troyanos y también spyware, programación que recopila información sobre un usuario de ordenador sin permiso.

Megahercios: Megahercio (MHz) es una unidad de frecuencia igual a un millón de hercios o ciclos por segundo. Las comunicaciones móviles inalámbricas en Estados Unidos se producen generalmente en las bandas de frecuencias del espectro de 800 MHz, 900 MHz y 1900 MHz (Wi- Fi = 250, 400).

Autenticación multifactor (AMF): Medida de seguridad, proceso o tecnología que obliga a los usuarios a proporcionen más de una credencial para acceder. Por lo general, a los usuarios se les pide que proporcionen una combinación de algo que saben (como una contraseña, un Q&A o un PIN), algo que tienen (como un teléfono inteligente o una llave USB) o algo que son (como una huella dactilar o un reconocimiento facial)

Sistema operativo: Componente de software de un sistema informático responsable de la gestión y coordinación de actividades y del uso compartido de los recursos de la computadora. El sistema operativo (SO) actúa como anfitrión de los programas de aplicación que se ejecutan en la máquina. Como anfitrión, uno de los propósitos de un sistema operativo es manejar los detalles del funcionamiento del hardware. Ford Motor Company recomienda el sistema operativo Windows 7 por su compatibilidad con las aplicaciones Ford.

Gestión de parches: Proceso de actualización de servidores o computadoras. Esto se hace a menudo para actualizar las máquinas a los últimos parches de seguridad y service packs. Los creadores de virus, programas espía y otros programas maliciosos aprovechan los fallos existentes en el software cargado en una computadora para propagarse y causar daños. STAR recomienda a las distribuidoras que apliquen los parches críticos, como los de seguridad, lo antes posible.

Punto de acceso inalámbrico falso: Un punto de entrada inalámbrico a la red de la distribuidora que no está autorizado, protegido ni reconocido por el departamento de TI, la dirección y los propietarios del distribuidor. Cualquier red inalámbrica fraudulenta debe ser detectada, localizada y eliminada de inmediato.

Enrutadores: Permiten la comunicación entre computadoras de redes y subredes diferentes. En las distribuidoras, se pueden utilizar enrutadores para conectar una LAN de OEM, una LAN de distribuidora y una LAN de DMS a Internet.

Espectro: Las frecuencias de radio designadas para un uso específico, como los servicios de comunicaciones personales y la seguridad pública.

Spyware: Cualquier tecnología que ayude a recopilar información sobre una persona u organización sin su conocimiento. En Internet (donde a veces se denomina spybot o software de rastreo), los programas espía son programas que se instalan en la computadora de una persona para recopilar en secreto información sobre el usuario y transmitirla a anunciantes u otras partes interesadas. Los distribuidores deben implantar sistemas de detección y eliminación de programas espía para proteger los datos de los clientes y la integridad de la seguridad de la red.

SSID (Service Set identification): En redes informáticas, un SSID es un conjunto formado por todos los dispositivos asociados a una red de área local inalámbrica IEEE 802.11x. Los SSID deben estar asociados a una VLAN específica.

TCP/IP (Protocolo de Control de Transmisión/Protocolo de Internet): Protocolo que permite las comunicaciones en y entre redes. El protocolo TCP/IP es la base de las comunicaciones por Internet.

Troyano (caballo de Troya): Un troyano es un programa en el que un código malicioso o dañino está contenido dentro de programas o datos aparentemente inofensivos, de tal forma que puede hacerse con el control y causar el daño que desee, por

ejemplo, arruinar una zona determinada de su disco duro.

VPN (redes privadas virtuales): Una VPN permite al usuario realizar transacciones seguras a través de una red pública o no segura. Al cifrar los mensajes enviados entre dispositivos, la integridad y confidencialidad de los datos transmitidos se mantiene en privado.

VLAN (red de área local virtual): En las redes informáticas, una única red de capa 2 (basada en conmutadores) puede dividirse para crear varios dominios de difusión distintos, aislados entre sí, de modo que los paquetes sólo puedan pasar de uno a otro a través de uno o varios enrutadores. Un dominio de este tipo se denomina red de área local virtual, LAN virtual o VLAN. Esto se consigue normalmente en dispositivos conmutadores o enrutadores.

VoIP (Voz sobre Protocolo de Internet): VoIP no sólo es capaz de ofrecer voz sobre IP, sino que también está diseñado para dar cabida a videoconferencias bidireccionales y aplicaciones compartidas. Basada en la tecnología IP, la VoIP se utiliza para transferir una amplia gama de tipos de tráfico.

WAN (red de área amplia): Término general que se refiere a una gran red que abarca un país o todo el mundo. Internet es una WAN. Un sistema público de comunicaciones móviles, como una red celular o PCS, es una WAN. Las distribuidoras pueden conectar en red ubicaciones y edificios remotos mediante tecnología WAN. En la mayoría de los distribuidores, WAN se refiere al proveedor de servicios de Internet de la distribuidora.

Gusano: Un gusano es un virus autorreplicante que no altera los archivos, sino que se duplica a sí mismo. Es habitual que los gusanos sólo se detecten cuando su replicación incontrolada consume recursos del sistema, lentificando o deteniendo otras tareas.

Wi-Fi: Wi-Fi proporciona conectividad inalámbrica a través de espectro sin licencia (utilizando los estándares IEEE 802.11a o 802.11b), generalmente en las bandas de radio de 2,4 y 5 GHz. Wi-Fi ofrece conectividad de área local a ordenadores con Wi-Fi.

WPA (Acceso Wi-Fi Protegido): Protocolos de seguridad y programas de certificación de seguridad desarrollados por la Wi-Fi Alliance para proteger las redes informáticas inalámbricas. La Wi-Fi Alliance la concibió como una medida intermedia en previsión de la disponibilidad de la más segura y compleja WPA2. WPA no es seguro y los distribuidores no deben usarla.

WPA-2 (Acceso protegido Wi-Fi II): WPA2 ha sustituido a WPA. WPA2, que exige pruebas y certificación por parte de la Wi-Fi Alliance, implementa los elementos obligatorios de IEEE 802.11i.

Red de área local inalámbrica (WLAN): Gracias a la tecnología de radiofrecuencia (RF), las WLAN transmiten y reciben datos de forma inalámbrica en una zona determinada. Esto permite a los usuarios de una zona pequeña transmitir datos y compartir recursos, como impresoras, sin estar físicamente conectados al dispositivo.