Pautas de infraestructura para vendedores STAR

2020

MEJORES PRÁCTICAS DE LA INDUSTRIA Y RECOMENDACIONES SOBRE TECNOLOGÍA DE LA INFORMACIÓN PARA LA VENTA AUTOMOTRIZ MINORISTA

1. Pautas de Infraestructura para Vendedores STAR

1.1 Descripción general

Este documento exhaustivo - Pautas de Infraestructura para Vendedores STAR (DIG) - describe las mejores prácticas de la industria y los distribuidores deben referenciarse a el mismo para verificar las necesidades de la red e infraestructura. Los distribuidores pequeños y grandes, deben tener administradores de red internos, o gerentes de TI, que sean responsables de revisar estas pautas, listas de verificación y consejos junto con su Guía de Referencia Rápida para garantizar que su distribuidor haya implementado una solución segura y robusta que cumpla tanto con las necesidades de los clientes y los equipos de la concesionaria.

1.2 El Grupo de Trabajo DIG(WG)

Las Pautas de Infraestructura del Distribuidor (DIG) son respaldadas por uno de los varios Grupos de Trabajo (WG) dentro de la organización STAR. A diferencia de muchos WG que están diseñados para centrarse en las estructuras de datos y los transportes, Las DIG se establecieron para ayudar a los distribuidores, vendedores y OEM (Fabricante Original de Equipo) con una guía común para la infraestructura de TI, necesaria para respaldar a una concesionaria de automóviles segura, eficiente y robusta.

1.3 Beneficios de DIG – Vendedores, Proveedores y OEM

Al igual que otros minoristas, la concesionaria automotriz necesita contar con la tecnología adecuada para respaldar procesos robustos destinados a vender y reparar vehículos. Con el advenimiento del Internet, son aprovechados muchos sistemas diferentes dentro de una concesionaria para satisfacer las demandas cada vez mayores de los clientes. Estos sistemas para vendedores son proporcionados y respaldados por Proveedores de Sistemas para Concesionarias (DSP) e incluyen todo, desde el Sistema de Gestión de Concesionarias (DMS) hasta numerosas soluciones de soporte como Marketing de relaciones con el cliente (CRM), Gestión de Prospectos, Minería de Capitales, Manejo de Reputación, sitios web, marketing digital, gestión de inventarios en línea, herramientas de canal de servicio y muchos otros. Con la creciente necesidad de DSPs, también existe la necesidad de que los datos se compartan de manera eficiente y segura entre estos sistemas de distribuidores y los OEM. Estas DIG pretenden ser una guía para admitir la integración efectiva de datos, la protección de datos, la confiabilidad del sistema y los procesos comerciales eficientes.

1.4 Descargo de responsabilidad

Cualquier nombre de la empresa, aplicación, enlace a sitio web o referencia tecnológica mencionada en este documento no debe considerarse como una aprobación por parte de los OEM o de STAR a menos que dicha aprobación esté expresamente establecida.

Este documento proporciona una especificación básica o una guía para que los vendedores establezcan conexión por Internet. Es importante tener en cuenta que la infraestructura de red, los datos del vendedor y la seguridad del sistema son responsabilidad de la concesionaria. Las organizaciones de terceros, como los proveedores de servicios y los socios, pueden brindar orientación y recomendaciones. Algunas organizaciones pueden proporcionar software, hardware o elementos de red patentados para ayudar a racionalizar las operaciones de red. Sin embargo, estas aplicaciones, recomendaciones o herramientas no sustituyen a la administración de la red.

2. Infraestructura de Red de Vendedores

2.1 Descripción general

La infraestructura de red de una concesionaria consiste en los recursos de hardware y software utilizados para permitir la conectividad a la red, la comunicación, las operaciones y la administración de la red de área local (LAN) de la concesionaria. La infraestructura de red proporciona la ruta de comunicación y los servicios entre usuarios, proveedores de servicios, OEM y clientes finales. La selección e implementación adecuadas de la infraestructura de red son fundamentales para garantizar la eficiencia de la red y la compatibilidad con OEM, DSP y aplicaciones y datos de concesionarias.

2.2 Hardware

El hardware de la concesionaria es un dispositivo físico que sirve para capturar los datos de la concesionaria (p. Ej., PC, computadoras portátiles, dispositivos de mano), enrutar esos datos (p. Ej., Enrutadores, conmutadores, cortafuegos) y proporcionar esos datos cuando sea necesario (p. Ej., Servidores, monitores y periféricos).

La selección del hardware de red es un componente crítico a la hora de administrar la red de una concesionaria. Si bien el nuevo hardware puede representar un gasto de capital muy elevado, el hardware antiguo puede dificultar las operaciones comerciales debido a problemas de velocidad o compatibilidad, por ejemplo.

La siguiente sección detalla cuándo comprar nuevo hardware, pautas para la compra y recomendaciones para comprar computadoras de escritorio, laptops y equipos de red.

2.2.a ¿Cuándo Comprar Nuevo Hardware?

El hardware de TI bien mantenido puede durar de tres a cinco años o incluso más, en algunos casos. Sin embargo, en algún momento, el vendedor deberá barajar la posibilidad de actualizar - o reemplazar - el hardware actual.

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

- Cuando el hardware actual no cumpla con las especificaciones mínimas necesarias para operar una tecnología específica.
- El hardware actual cae por debajo de los estándares mínimos establecidos por un OEM, DSP u otros socios tecnológicos de la concesionaria.
- El hardware actual no posee las partes físicas, los accesorios o el soporte que los periféricos necesitan para realizar una función específica.
- El dispositivo funciona tan lentamente que afecta las operaciones comerciales. *Tenga en cuenta que esto no necesariamente se debe a un problema de hardware. La lentitud puede deberse a un error de configuración, almacenamiento, seguridad o usuario.*
- El nuevo software (como sistemas operativos, navegadores o aplicaciones de vendedores) no es compatible con el hardware actual.
- El nuevo hardware podría proporcionar mucho ahorro en costos, en cuestión de ahorro de tiempo, características adicionales o facilidad de uso.
- Los costos de actualización son iguales o cercanos al costo de un reemplazo; o el producto está llegando al final de su vida útil y/o ya no tiene soporte.
- El hardware ya no tiene soporte del fabricante. Es decir, los parches, las actualizaciones de seguridad y los avances de software no ya no se realizarán en el dispositivo de hardware. Cuando el hardware ya no es compatible, la concesionaria está expuesta a riesgos de seguridad y confiabilidad.

2.2.b Qué comprar: Hardware de Tipo Consumidor versus Tipo Corporativo

La mayoría de los fabricantes de computadoras ofrecen dos tipos diferentes de hardware: hardware tipo consumidor, destinado al uso doméstico y personal, y hardware tipo corporativo, destinado a empresas. Si bien el precio del hardware tipo consumidor puede parecer atractivo para las concesionarias, a menudo el costo total acaba siendo mayor debido a funcionalidad limitada, probabilidades de fallos más frecuentes y soporte más complejo.

STAR recomienda que las concesionarias compren hardware de tipo corporativo por los siguientes motivos:

- Los sistemas de tipo consumidor, generalmente se fabrican con piezas más genéricas o piezas que son menos costosas de ser suministradas a granel. Además, los fabricantes son conocidos por cambiar piezas, proveedores y componentees sin cambiar los modelos. Debido a estos factores, estas partes pueden tener una probabilidad de fallos más elevada. Esto puede generar más tiempo de inactividad, mayor tiempo de soporte y una tasa de respuesta de reemplazo del sistema más lenta.
- Los sistemas de tipo corporativo generalmente están hechos con piezas estandarizadas de marca, lo que facilita la estandarización de la red y el soporte para muchas empresas.
- Las PC de nivel de consumidor a menudo vienen con sistemas operativos destinados para uso doméstico. Esto puede dar lugar a complicaciones con las redes empresariales, como conectarse a servidores o a otras PC.
- El hardware de red de tipo consumidor a menudo está destinado solo a un pequeño número de conexiones. El hardware de tipo corporativo está diseñado para acomodar la gran cantidad de conexiones requeridas por las redes de las concesionarias.
- El hardware de tipo consumidor puede venir con garantías limitadas. Algunas garantías de tipo consumidor no aplican para uso corporativo.
- Los ahorros iniciales podrían ser contrarrestados por reemplazos más costosos y mayor soporte técnico, así como tiempos de respuesta más extensos a la hora de asegurar un reemplazo.

2.2.c Recomendaciones de hardware

PCs de Escritorio	
Componente	**Especificaciones**
Procesador	Intel Core i5 y superior, o su equivalente de AMD
Memoria (RAM)	4 GB o más
Unidad de Disco Rígido	500 GB o más
Unidad de CD/DVD	CD/DVD combo, o unidad externa
Puerto Serial	1 (Adaptador USB opcional)
Puertos USB	2 o más
Adaptador de Audio	16 bit
Parlante de Audio	Opcional
Pantalla	Resolución Mínima de 1280x768
Adaptador de Red	Cableado: Ethernet Gigabit (o superior) Inalámbrico: 802.11 n o ac

Garantía	de 3 años, en el sitio
Sistema Operativo	Los sistemas operativos Windows son compatibles con la mayoría de las aplicaciones de la concesionaria. Por favor verifique con su OEM y socios tecnológicos a la hora de escoger un sistema operativo.

Laptops	
Componente	**Especificaciones**
Procesador	Intel Core i5 y superior, o su equivalente de AMD
Memoria (RAM)	4 GB o más
Unidad de Disco Rígido	320 GB o más
CD/ DVD Drive	CD/DVD combo, o unidad externa
Puertos USB	2
Parlante de Audio	Opcional
Pantalla	Resolución Mínima de 1280x768
Adaptador de Red	Cableado: Ethernet Gigabit (o superior) Inalámbrico: 802.11 n o ac
Garantía	de 3 años, en el sitio
Sistema Operativo	Los sistemas operativos Windows son compatibles con la mayoría de las aplicaciones de la concesionaria. Por favor verifique con su OEM y socios tecnológicos a la hora de escoger un sistema operativo.

Ruteadores & Conmutadores	
Componentes	**Especificaciones**
Especificación estándar de Ethernet	IEEE 802.3 100baseT o 1000baseT
Redundancia	La conexión de varios conmutadores juntos debería usar enlaces redundantes de la velocidad más alta disponible, utilizando STP o rSTP para garantizar una topología sin bucles.
Fuente de alimentación	Se recomiendan fuentes de alimentación redundantes para reducir el tiempo de inactividad.
Velocidad	100 o 1000 Mbps
VLAN	Los swtiches con tecnología troncal VLAN y 802.1Q deben usarse para redes enrutadas con múltiples subredes o VLANs.
Protocolos de gestión	Los dispositivos administrados deben ser compatibles con los estándares de administración remota de la industria, como el Protocolo Simple de Administración de Redes (SNMP) y el Monitoreo Remoto de Redes (RMON).
Conmutadores inalámbricos	Los dispositivos inalámbricos deben ser de doble banda y compatibles con IEEE 802.11b/g/n.

2.2.d Tabletas & Dispositivos Móviles

Las tabletas son dispositivos portátiles diseñados para tener mayor movilidad y accesibilidad. Las tabletas no tienen la misma funcionalidad que una PC de escritorio o una laptop. Debido a esto, se recomienda encarecidamente que las concesionarias no reemplacen las PC de escritorio o laptops con tabletas, sino que usen las tabletas cuando una función pueda ser mejorada con su uso y se requiera de una mayor movilidad y accesibilidad.

Algunas aplicaciones están específicamente desarrolladas para ejecutarse en ciertos dispositivos de tableta, como iPads. Cuando se implementan estas aplicaciones, el OEM o DSP comunicará cuáles dispositivos están destinados a ser usados para dichas aplicaciones. Basándonos en la evolución tecnológica en el mundo móvil, la compatibilidad de ciertos programas podría estar limitada a tabletas específicas y/o a versiones de sistemas operativos de dispositivos móviles.

2.2.e Desmantelamiento & Reciclaje de Hardware

Es responsabilidad del propietario del dispositivo original asegurarse de que todos los dispositivos electrónicos usados se eliminen correctamente. Hay miles de recicladores electrónicos en los EE. UU., Pero es importante elegir al correcto. A continuación hay algunas sugerencias a la hora de elegir un reciclador.

Averigüe las políticas / prácticas del reciclador para destruir datos personales en equipos usados.

- Los datos se pueden borrar de los medios de almacenamiento utilizando un método de limpieza magnética o un programa para sobrescribir todos los sectores de un disco duro. Cualquier método utilizado para el borrado de datos debe realizarse más de una vez (varias pasadas).
- Los medios de almacenamiento pueden destruirse triturándolos, cortándolos, incinerándolos, realizándoles perforaciones múltiples o aplastándolos.
- Un reciclador debe poder proporcionar una certificación por escrito de que los datos fueron eliminados - o que los medios de almacenamiento fueron destruidos - así como proporcionar un registro de los métodos utilizados.

Averigüe la(s) certificación(es) de la empresa de reciclaje.

- El reciclador debe estar certificado. Si le dicen que no están certificados, que es un "secreto comercial", o que su método es "confidencial", evite contar con ellos.
- Las principales certificaciones de la industria son:
    - E-Stewards – www.e-stewards.org
    - Basel Action Network – www.ban.org
    - R2 – www.sustainableectronics.org
- Los recicladores y consolidadores deberían poder presentar pruebas de que cuentan con las instalaciones, la capacitación y equipamiento adecuados para realizar las operaciones declaradas, presentando un sistema de gestión/operaciones auditado completo con evidencia de auditorías recientes.
- Pregunte si la empresa de reciclaje cuenta con una certificación o sistema de gestión ambiental, ya sea una certificación de gestión ambiental 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).
- Para aquellos que no están certificados, se recomienda precaución. La concesionaria, como propietario original del dispositivo, tiene la responsabilidad de garantizar un reciclaje adecuado.

Averigüe si el reciclador ha tenido alguna violación ambiental o de seguridad (citaciones, multas, notificación de violación, órdenes de consentimiento, etc.) o si ha presentado reclamos de seguro por daños ambientales en los últimos 5 años.

- Se prefieren las empresas que posean un buen historial de cumplimiento de los requisitos ambientales y de seguridad.
- Una empresa que ha estado en el negocio durante varios años con solo algunas infracciones menores que han sido resueltas rápidamente puede ser tan responsable como una empresa sin infracciones que lleva tan solo uno o dos años en el negocio.
- Compruebe si hay infracciones importantes, como grandes cantidades de desechos o quejas importantes en el vecindario.

Averigüe si el reciclador envía equipos usados o desechos a otros socios comerciales o proveedores de servicios; estos se denominan "socios intermediarios".

- El buen mantenimiento de registros es una de las mejores prácticas de gestión de la industria. Busque empresas que mantengan registros detallados, incluidos dónde son enviados los materiales, cuánto envían y los números de serie de los artículos que se reutilizarán.
- Aunque hay varios recicladores de "servicio completo" en los EE. UU., Es probable que el reciclador no se encargue del procesamiento completo del dispositivo.
- La empresa de reciclaje debe tener registros escritos de qué procesamiento se realiza en el sitio (como clasificación y/o trituración) y quién recibe los materiales o productos luego del procesamiento inicial.
- Pregunte si los socios comerciales del reciclador (socios intermediarios) están sujetos contractualmente a los mismos estándares o mejores prácticas de gestión que el reciclador elegido. La lista completa de todos los socios intermediarios debe estar disponible en el reciclador elegido.
- Tenga cuidado con los recicladores que afirman que sus procesos y socios comerciales son "confidenciales", "propietarios" o que "no saben".
- Toda exportación debe realizarse de conformidad con las leyes aplicables tanto a los países exportadores como a los importadores.

Un reciclador debe tener un seguro de responsabilidad civil general y ambiental.

- Los requisitos de seguro varían de estado a estado, y la cantidad y tipo de cobertura necesaria variará según el tamaño y las operaciones en la instalación.
- La cantidad y la cobertura dependerán del alcance y la magnitud de las operaciones.

2.3 Software

El software es el programa o información operativa utilizada por el hardware de la concesionaria para capturar, almacenar, manipular y mostrar datos en el hardware de la red. Las concesionarias utilizan software para capturar datos de clientes, automatizar procesos comerciales para vender y dar servicio a vehículos, y comunicarse con otros sistemas o redes.

Para las concesionarias, estos programas o procesos a menudo residen en el sistema operativo o el navegador de Internet de la PC. El software a menudo está diseñado para sistemas operativos específicos o navegadores de Internet. Debido a que el software es crítico para las comunicaciones de la concesionaria y los procesos comerciales, es importante que las concesionarias utilicen sistemas operativos y navegadores que sean compatibles con el software de la concesionaria.

La siguiente sección detalla los sistemas operativos y navegadores comunes. El objetivo de esta sección es proporcionar orientación para comprender y seleccionar los sistemas operativos y las aplicaciones del navegador. Se recomienda encarecidamente que el vendedor consulte con su OEM y proveedores de servicios de la concesionaria para garantizar la compatibilidad del software con las aplicaciones de la concesionaria.

2.3.a Sistemas Operativos

A continuación se muestra una lista de los sistemas operativos más comunes en el mercado actual. Algunas aplicaciones no son compatibles con sistemas operativos específicos. Se recomienda que los vendedores verifiquen con sus OEM, DSP y otros proveedores para determinar qué sistemas operativos deberá usar. Tenga en cuenta que Microsoft finalizó el soporte para los sistemas operativos XP, Vista y Windows 7. Esto incluye actualizaciones críticas de seguridad. STAR recomienda que las concesionarias no utilicen Windows XP, Vista ni Windows 7.

Sistema operativos actuales típicos del cliente	Última actualización o *service pack**	Fin del soporte estándar	Fin del soporte extendido
Windows XP	Service Pack 3	14-Abr-09	8-Abr-14
Windows Vista	Service Pack 2	10-Abr-12	11-Abr-17
Windows 7	Service Pack 1	13-Ene-15	14-Ene-20
Windows 8	Windows 8.1	9-Ene-18	10-Ene-23
Windows 10,	N/A	13-Oct-20	14-Oct-25
MAC OS X	10.9 (o superior soportado) 10.11	Versiones 10.8 (Mountain Lion) e inferiores ya no son soportadas.	Versiones 10.8 (Mountain Lion) e inferiores ya no son soportadas.
IOS (para iPad y iPhone)	9.1		
Android	5		

**** Últimas actualizaciones / service pack a partir de noviembre de 2015***

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 navegadores específicos. Otras aplicaciones requieren configuraciones específicas del navegador, como el modo de compatibilidad. Se recomienda que los vendedores verifiquen con sus OEM, DSP y otros proveedores para determinar qué sistemas operativos deberán usar.

Navegador	Última actualización o service pack*	Notas
Google Chrome	77	
Mozilla Firefox	69	
Internet Explorer	11	
Apple Safari	13	No recomendado para sistemas operativos de Microsoft
Opera	63	
Edge	44	

**** Últimas actualizaciones / service pack a partir de enero de 2020***

2.3.c Licencia de Software

El cumplimiento de la licencia de software no es algo a lo que la mayoría de las concesionarias suelen prestarle atención. Sin embargo, ignorala puede costarle miles de dólares a una concesionaria. Estos son los errores más comunes con las Licencias de Software para concesionarias.

- 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 no utilizadas
- Comprar versiones de software "domésticas" en lugar corporativas o empresariales

- Uso de software pirateado, descargado gratis

Para abordar este problema, las empresas deben crear un programa de Gestión de Activos de Software (SAM). SAM es la práctica de administrar y optimizar la compra, implementación, mantenimiento y ciclo de vida de los activos de software dentro de una organización. Los dos mayores beneficios 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 concesionarias deben administrar una red para que los dispositivos en la concesionaria puedan comunicarse y compartir recursos de manera efectiva pero segura.

La gestión de la red puede ser una tarea difícil para las concesionarias de automóviles. Los distribuidores deben hacer que la red esté disponible para compartir datos y limitar el acceso por motivos de seguridad. Además de los empleados de la concesionaria, a menudo un proveedor de servicios, el OEM e incluso los clientes también pueden necesitar compartir los recursos de la red. Brindar acceso seguro a la red de concesionarias puede ser un desafío.

La siguiente sección proporciona recomendaciones para la configuración y administración de la red de área local. También brinda asesoramiento sobre redes inalámbricas, movilidad en la concesionaria y acceso al cliente.

2.4.a Configuración & Gestión de Red

Recomendación	Especificación
Red de área local (LAN)	Gigabit Ethernet
Cableado de datos	El cableado de red de datos existente debe aplicar, como mínimo, a los estándares TIA-568-A Categoría 5e. La categoría 6a debe usarse para cableados nuevos. Ningún cable horizontal debe exceder los 90 metros (295 pies). Se recomienda encarecidamente el uso de cables de fibra óptica en lugar de los cables de datos cuando la longitud exceda los 295 pies.
Ubicación del equipo	El equipo LAN debe estar alojado en un armario de cableado o sala de comunicaciones. Todo el equipo debe estar montado o asegurado a un *rack* o estante.
Direccionamiento IP	El ISP de la concesionaria debe proporcionar direccionamiento IP enrutable. Para la LAN del distribuidor, deberá utilizarse el direccionamiento dinámico (DHCP) para facilitar el soporte.
Adaptador de red	Gigabit Ethernet
Conmutador de Ethernet	Conmutador gestionado por Gigabit. Etiquete cada interfaz y cable. Esto ahorrará tiempo al rastrear los cables de red para soporte o instalación nueva.
Ruteadores	Enrutador de tipo corporativo. Los enrutadores deben admitir 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 al momento de la instalación y de manera continua y regular. - Mantenga la configuración de la copia de seguridad en archivos en caso de una falla de software o reemplazo de hardware.
Cortafuegos	Un dispositivo de Seguridad completamente administrado que monitorea continuamente las amenazas a través del Sistema de Detección de Intrusos "IDS", el

	Sistema de Prevención de Intrusos "IPS" y otros mecanismos como el filtrado de paquetes, antivirus e inspección de paquetes *stateful*. - Los cortafuegos deben admitir la traducción de direcciones de red / tecnología analítica de procesos (NAT / PAT). Los cortafuegos también deberían admitir el enrutamiento dinámico mediante RIPv2, OSPF y BGP. - Cambie la contraseña del dispositivo al momento de la instalación y de manera continua y regular. - Mantenga la configuración de la copia de seguridad en archivos en caso de una falla de software o reemplazo de hardware. - Para obtener más información sobre cortafuegos y seguridad de redes, consulte la sección 2.6.
Servicios de nombres de dominio (DNS)	Use un DNS público, excepto cuando use Windows Active Directory. (En cuyo caso, se requerirá que tenga un servidor DNS interno).

2.4.b Redes inalámbricas

Las LAN inalámbricas permiten la comunicación en red sin las restricciones físicas del cableado físico. La tecnología inalámbrica puede ser especialmente conveniente ya que puede proporcionar movilidad a los empleados, permitir a los clientes traer y usar su propio dispositivo y expandir la red de distribuidores más allá de las paredes físicas de la concesionaria. Los vendedores también deben entender que con la ubicuidad de las redes inalámbricas aparecerán desafíos relacionados al diseño, el soporte y la seguridad.

Use las siguientes pautas cuando diseñe, respalde y asegure la red inalámbrica de una concesionaria.

Diseño de Redes Inalámbricas	
Recomendación	**Especificación**
Hardware inalámbrico	Solo se deben utilizar puntos de acceso de tipo corporativo. Los puntos de acceso de tipo corporativo están diseñados para proporcionar *roaming* y otras características de clase corporativo (como VLAN y / o SSID múltiples) necesarios para admitir dispositivos inalámbricos para sus aplicaciones. Los puntos de acceso inalámbrico de tipo corporativo también están diseñados para acomodar una mayor cantidad de conexiones que el hardware a nivel de consumidor.
Segmentación de Red	Las concesionarias deben garantizar que el tráfico de invitados esté segmentado desde la red de la concesionaria a través de VLANs o una conexión a Internet separada.
SSIDs	Se recomienda que las concesionarias utilicen SSID separados para diferentes funciones comerciales (por ejemplo: ventas, servicio y administración). Sin embargo, las concesionarias no deben confundir los SSID con la segmentación de la red. Los SSID generalmente no separan el tráfico de red, sino que solo proporcionan una forma diferente de unirse a la red.
Cobertura	Implemente puntos de acceso inalámbrico para garantizar una cobertura adecuada. Las herramientas inalámbricas pueden proporcionar intensidad en la señal de todo el edificio. Tenga en cuenta las estructuras u objetos que puedan interferir con la cobertura inalámbrica (interferencia eléctrica, interferencia de radiofrecuencia o materiales físicos como metales u hormigón).
Autenticación & Cifrado	WPA2 con autenticación RADIUS y cifrado AES
Estándar de red	802.11n o 802.11ac

Detección inalámbrica no autorizada	Escanee, identifique y elimine cualquier punto de acceso inalámbrico no autorizado que pueda estar en la red de la concesionaria. -Un punto de acceso inalámbrico no autorizado se define como un punto de entrada inalámbrico en la red de la concesionaria que no ha sido autorizado o asegurado por la concesionaria, la administración de TI y tampoco es propio. -Todas las redes inalámbricas no autorizadas se deben detectar, encontrar y eliminar de inmediato. -STAR recomienda el uso de un servicio de detección inalámbrica administrada que esté continuamente escaneando la red en busca de amenazas inalámbricas.

Movilidad de la Concesionaria	
Recomendaciones	**Especificación**
Movilidad dentro de la concesionaria	Utilice una red de malla inalámbrica para garantizar que los usuarios finales puedan navegar en las instalaciones sin perder la conexión o sin necesidad de autenticarse de nuevo.
Controladores inalámbricos	Se puede usar un controlador de LAN inalámbrica en combinación con el Protocolo ligero de puntos de acceso (LWAPP) para administrar puntos de acceso ligeros en toda la red de la concesionaria. Esto ayudará a garantizar una cobertura, confiabilidad y eficiencia de red adecuadas.

Acceso de los Clientes	
Recomendaciones	**Especificación**
Priorización de tráfico	Las concesionarias deben utilizar un cortafuego u otro mecanismo para limitar el consumo de ancho de banda del invitado. Esto evitará que el acceso de los invitados interfiera con las operaciones comerciales al consumir demasiado ancho de banda.
Autenticación de invitados / Términos de Servicio	STAR recomienda que las concesionarias utilicen un portal cautivo que requiera que los invitados acepten los términos y condiciones de uso en la concesionaria. Esto puede incluir restricciones de contenido, limitaciones de ancho de banda y acuerdos de uso.
Ancho de banda de internet	Para garantizar que la concesionaria tenga suficiente ancho de banda, una concesionaria debe elegir la tecnología y la velocidad adecuadas. (Consulte la Sección 2.5a y 2.5b en STAR DIG para obtener más información sobre tecnologías y ancho de banda de Internet). -STAR también recomienda que cada concesionaria tenga una conexión ISP de respaldo de un proveedor diferente, utilizando una tecnología diferente. -Ver sección 2.5c para recomendaciones sobre conexiones de respaldo de internet.

2.5 Ancho de Banda de Internet

El ancho de Banda de Internet es la cantidad de datos que pueden enviarse desde y hacia la concesionaria, generalmente medidos en bits por segundo. La mayoría del software de las concesionarias depende de Internet para la comunicación de datos. La información de inventario, las órdenes de trabajo, los manuales de servicio y los datos del vehículo a menudo son accesibles a través

de Internet. Además, muchos empleados y clientes acuden al acceso a Internet de la concesionaria por razones personales, sea para consultar el correo electrónico o para navegar por la web. Dado que muchos usuarios dependen de Internet para obtener información, es fundamental que la concesionaria obtenga suficiente ancho de banda para proporcionar adecuadamente a cada recurso suficiente ancho de banda para acceder rápidamente a los datos. Para garantizar que la concesionaria tenga suficiente ancho de banda, una concesionaria debe elegir la tecnología y la velocidad adecuadas.

La siguiente sección detalla las tecnologías disponibles para el acceso a Internet y cómo planificar suficiente ancho de banda para cada recurso en la Red de Área Local (LAN).

2.5.a Tecnologías de internet

Tecnología	Descripción	Velocidad	Medio Físico	Comentarios
Cable	Se requiere cable módem especial y línea de cable.	Las velocidades pueden variar, pero generalmente se ejecutan entre 10 Mbps y 100 Mbps	Cable coaxial	El servicio de Internet por cable utiliza una infraestructura compartida y puede degradarse durante el uso intensivo. Las concesionarias deben buscar cuáles proveedores de cable ya tienen servicio en el área. El costo de llevar el servicio a un área y el soterramiento de cables puede ser prohibitivo. Ford recomienda que las concesionarias compren cable de calidad comercial y soliciten al proveedor un acuerdo de nivel de servicio (SLA) u objetivo de nivel de servicio (SLO) por escrito.
DSL	Esta tecnología utiliza la parte digital no utilizada de una línea telefónica regular de cobre para transmitir y recibir información. El ADSL es asimétrico, lo que significa que la velocidad de carga del servicio es más lenta que la velocidad de descarga. SDSL es simétrico y consta de las mismas velocidades de carga y descarga. VDSL es otra tecnología asimétrica que puede ofrecer velocidades de hasta 52 Mbps.	128 Kbps a 52 Mbps	Par trenzado (utilizado como medio digital de banda ancha)	Ford recomienda que las concesionarias compren líneas DSL de tpo comercial con suficiente velocidad de carga y descarga para ejecutar aplicaciones de Ventas Ford. VDSL es el único tipo de DSL recomendado, ya que puede ser el único servicio con suficiente ancho de banda para cumplir con los requisitos de ancho de banda recomendados.
T1	Se requieren 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 lograr mayores velocidades.
Satelital		6 Mbps o más	Ondas Puede usar el acceso telefónico para el tráfico de subida de datos	El ancho de banda no es compartido. Además, la latencia es típicamente alta. Esta alta latencia a menudo interfiere con las aplicaciones del vendedor. La satelital, no es una tecnología recomendada para las concesionarias.
Fibra Óptica	Los tipos de conectividad a Internet del servicio de fibra óptica operan a través de una red óptica.	Hasta 300Mbps	Red Óptica	Fiber ofrece altas velocidades, menores costos y buenos acuerdos de nivel de servicio. Sin embargo, la disponibilidad es limitada en algunas áreas del país.

2.5.b Planificación de ancho de banda

Comience por conocer el servicio de internet actual de la concesionaria
Muchos concesionarias desconocen su tecnología, velocidad y uso actuales de Internet. Comprender la tecnología puede ayudar a identificar posibles limitaciones y ahorros de costos. Use el cuadro anterior para comprender mejor las diferentes tecnologías disponibles en el mercado. Averigüe con el ISP (proveedor de servicios de internet) de la concesionaria las velocidades de carga y descarga de ancho de banda del servicio actual (generalmente identificadas en Mbps o Kbps). Finalmente, inicie sesión en el dispositivo de puerta de enlace de la concesionaria, consulte al ISP de la concesionaria o busque pruebas en línea para comprender la utilización actual del ancho de banda.

Planificación para picos de uso
El uso del ancho de banda no siempre es consistente. Los distribuidores verán picos en la utilización en función de los procesos comerciales (como "tiempos de actividad"), procesos tecnológicos (como ejecutar copias de seguridad o descargar actualizaciones) y el uso del cliente (como la transmisión de video desde la sala de espera del cliente). Se recomienda que las concesionarias promedien alrededor del 60% de su utilización para tener un margen para picos potenciales.

Planificación para avances tecnológicos
La mayoría de los OEM, DSP y distribuidores están desarrollando soluciones que aprovechan aún más las comunicaciones por Internet. Las concesionarias deben comprender que sus necesidades de ancho de banda no son estáticas, sino que continuarán creciendo a medida que la concesionaria, los proveedores y los socios implementen nuevas tecnologías.

Planificación para el Crecimiento
El IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) afirma que las redes deberán ser capaces de soportar tasas de crecimiento anual compuesto del 58% en el ancho de banda. El crecimiento está impulsado por aumentos simultáneos de usuarios, metodologías de acceso, tasas de acceso y servicios como video a pedido y redes sociales.

Manténgase Atento
Dado que el uso del ancho de banda no es estático, su planificación debe ser una actividad continua. Al obtener visibilidad de los patrones de uso de la concesionaria, un administrador de TI puede adelantarse mejor a la posible limitación del ancho de banda antes de que éste afecte el rendimiento comercial de la concesionaria. Se recomienda que las concesionarias configuren alertas para picos de utilización, uso de consumo promedio o tiempos en que el ancho de banda no esté disponible. Esto mitigará los riesgos, limitará el tiempo de inactividad y permitirá que la concesionaria se actualice antes de un impacto comercial significativo.

2.5.c Conexión de Respaldo

La disponibilidad del servicio de Internet es crítica para el negocio de las concesionarias. Debido a que las concesionarias confían en Internet para vender y reparar vehículos, se recomienda una conexión de respaldo.

Al elegir una Conexión de Respaldo, haga uso de las siguientes recomendaciones:

- Utilice un proveedor y una tecnología de Internet diferentes para su conexión de respaldo.
- Como mínimo, tenga disponible un servicio de respaldo / conmutación de banda ancha 3G/4G. Pruebe la señal inalámbrica con anticipación para garantizar una intensidad de señal adecuada. Los proveedores de servicios de Internet, la ubicación física y el diseño

del edificio son variables que determinan la fuerza de la señal de cualquier concesionaria.

- STAR recomienda un circuito dedicado para alta disponibilidad.
- STAR recomienda que las concesionarias utilicen un dispositivo de puerta de enlace que admita la conmutación automática para garantizar un tiempo de inactividad mínimo.
- Es posible que el servicio de respaldo no necesite tener la misma velocidad que la conexión principal, pero aún así debe tener suficiente ancho de banda para admitir las funciones comerciales críticas de la concesionaria.

2.6 Seguridad

El objetivo de la infraestructura de red de una concesionaria es compartir datos y recursos con empleados, clientes y proveedores o socios externos. Las concesionarias también deben tomar medidas para garantizar que estos datos se compartan de forma segura. Las concesionarias deben monitorear las conexiones conocidas y desconocidas para detectar signos de pérdida de datos. Una concesionaria 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 del vendedor no terminen en las manos equivocadas.

La siguiente sección revisa la protección de la red desde 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, el gobierno y el riesgo y el cumplimiento. Además, puede encontrar información sobre procesos y procedimientos de seguridad en la sección 6 titulada “Prácticas de Capacitación, Procedimientos y Documentación”.

2.6.a Políticas de seguridad

El marco de Políticas de seguridad de la concesionaria debe ser completo, consistente y aprobado por el órgano de administración de la concesionaria. Es importante asegurarse de que todas las partes interesadas se comprometan con las políticas y acuerden implementarlas en todos los aspectos relevantes de la concesionaria.

Las políticas deben reflejar la estrategia para asegurar la información, y no al revés, y comprender los requisitos de seguridad es el factor clave aquí. El enfoque básico debe estar en la confidencialidad, integridad y disponibilidad de datos y recursos confidenciales, incluido 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: con bastante frecuencia se deben considerar el no repudio, la trazabilidad o la autenticidad.

Además, cada industria tiene sus propias áreas sensibles. Por ejemplo: nos preocupamos mucho más por la integridad, en lugar de la confidencialidad, de un avión en el aire o de un automóvil en la carretera en comparación a preocuparnos por la confidencialidad del historial médico de un paciente (que también puede depender del contexto). Las políticas de seguridad deben reflejar estas consideraciones.

Hay muchas políticas o directivas estructurales listas para escoger e implementar en la seguridad de una empresa. Sin embargo, aunque este tipo de estructura pueda proporcionar una línea de base general, una empresa necesitará ajustar y desarrollar las políticas para su aplicación dentro de su contexto comercial.

2.6.b Gestión de Identidad y Acceso

Cubra la gestión de identidad y acceso de manera integral. Comience con la introducción y

conceptos básicos seguidos de subsecciones: gestión de identidad, autenticación, autorizaciones, por qué son tan importantes, proceso de gestión de acceso, usuarios finales, consideraciones físicas y niveles de protección. Cierre con una Introducción a los tres niveles de madurez.

2.6.c Gestión de Parches

Los Sistemas Operativos en los servidores/computadoras locales requieren actualizaciones de vez en cuando, muchos de los cuales se deben a riesgos de seguridad. Los parches enviados por el fabricante a menudo brindan protección contra exploits nuevos o previamente desconocidos. Es fundamental que estos parches se administren, implementen y verifiquen para garantizar una aplicación confiable y segura. Además, las concesionarias deben prestar especial atención a lo siguiente:

- Sistemas en su final de vida útil (EOL)
  - Mantenerse al tanto del final de la vida útil de (EOL) de los sistemas, le ayudará a garantizar que el local no esté utilizando sistemas operativos que ya no reciben actualizaciones de seguridad u otro tipo de actualizaciones porque el proveedor interrumpió el soporte.
  - Generalmente, los proveedores notifican los EOL y esto siempre se puede verificar en sus respectivos sitios web.
- Dispositivos Móviles
  - Los dispositivos móviles a menudo dejarán la protección de una red de concesionarias y se conectarán a otra red, a menudo menos segura. Debido a esto, estos dispositivos pueden considerarse más vulnerables. Es importante que los dispositivos móviles sean parchados rápidamente para limitar el riesgo y la exposición a amenazas y vulnerabilidades.

2.6.d Capacitación sobre Seguridad

La gran 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. Así como los técnicos están capacitados en los últimos desarrollos de vehículos y los vendedores están capacitados sobre las nuevas características de vehículos y técnicas de ventas, todos sus empleados deben recibir capacitación sobre cómo proteger su negocio contra robos, violaciones de datos y otros problemas de seguridad.

El objetivo del programa de capacitación no es solo educar a sus empleados, sino influir en su comportamiento. Deben convertirse en un cortafuegos humano para la empresa.

La seguridad no debe ser aburrida: si las personas no prestan atención, el mensaje no penetrará, así que no tenga miedo de ser creativo con el programa de capacitación y sensibilización. El humor, los ejemplos de la vida real, los concursos y los juegos son algunas formas de mantenerlo interesante y ganar el interés de los empleados.

Para mantener a los empleados comprometidos, considere utilizar módulos de capacitación de seguridad en línea más cortos, con mayor frecuencia, en vez de una sesión de capacitación larga una vez al año. Esto también ayudará a que la capacitación se mantenga actualizada sobre los últimos desarrollos en malware y ataques.

- La capacitación debe ser anual, como mínimo, y cubrir temas que incluyan:
  - Conocimiento de ingeniería social: *phishing*, Comprometimiento del Correo Comercial (BEC), vishing, ransomware, navegación web segura
  - Contraseñas
  - Datos sensibles - PII, PCI, PHI, etc. - y manejo de datos

- Políticas de uso compartido e intercambio de datos.
- Protección y destrucción de datos.
- Seguridad del dispositivo móvil
- Redes sociales seguras
- Violencia laboral
- Políticas de la empresa relacionadas con la seguridad.

- Es posible que se necesite más capacitación de acuerdo al rol del empleado en la empresa. Por ejemplo: los empleados que manejan las finanzas de la compañía pueden beneficiarse al comprender las formas únicas en que los ciberdelincuentes los atacan por el acceso que tienen a las cuentas bancarias. Considere la capacitación basada en roles para ayudar a los empleados a comprender el papel que desempeñan en la protección de la empresa en sus actividades diarias.
- Utilice materiales de concientización de seguridad en salas de descanso y otros espacios exclusivos para empleados, como carteles o volantes que les recuerden a los empleados sobre el manejo seguro de los datos de los clientes, conciencia sobre la ingeniería social, recordatorios de capacitación, etc.
- Utilice los boletines, correos electrónicos, sesiones de capacitación en vivo y otras funciones de la compañía para reforzar continuamente el mensaje de seguridad.
- Revise periódicamente los programas de capacitación y ajústese a las nuevas tecnologías, los cambios comerciales de la concesionaria y los comentarios de los empleados.
- Recursos. Estos pueden ser gratuitos o de pago, pero algunos de sus socios comerciales pueden ofrecer capacitación de seguridad en línea para sus empleados.
  - Proveedor de DMS
  - Proveedor de seguros
  - Firma contable
  - Firma legal
- Otros recursos:
  - https://staysafeonline.org/business-safe-online/train-your-employees
  - SANS Ouch – n boletín mensual de seguridad gratuito para empleados https://securingthehuman.sans.org/resources/newsletters/ouch/2016

2.6.e <u>Cumplimiento de las Leyes Federales</u>

Asegúrese de que la concesionaria cumpla con todas las regulaciones federales, estatales, locales y de la industria para instituciones financieras y minoristas, como la Ley Gramm-Leach-Bliley, la *Safeguards Rule*, PCI DDS, etc.

- Ley Gramm-Leach-Bliley (GLB) y la *Safeguards Rule*
  - 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 instituciones financieras. La Ley Gramm-Leach-Bliley (GLB) requiere que las empresas definidas como "instituciones financieras" garanticen la seguridad y confidencialidad de la información confidencial. Debido a que las concesionarias arriendan y prestan (incluso a través de terceros), deben cumplir con la Ley GLBA.
  - La *Safeguards Rule* fue emitida por la Comisión Federal de Comercio (FTC), como parte de la Ley GLB. La *Safeguards Rule* requiere que las instituciones financieras tengan medidas establecidas para mantener segura la información del cliente.
  - Para obtener 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

- Estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS)
  - PCI DSS es un estándar mundial de seguridad de la información creado por el Consejo de Estándares de Seguridad de la Industria de Tarjetas de Pago (PCI SSC). El estándar fue creado para ayudar a las organizaciones que procesan pagos con tarjeta de crédito eviten el fraude con tarjetas de crédito por medio de mayores controles sobre los datos y su exposición a comprometimientos.
  - Todos los comerciantes que almacenan, aceptan, procesan y / o transmiten datos de titulares de tarjetas deben cumplir con los requisitos técnicos y operativos establecidos por PCI DSS. Todas las concesionarias deben cumplir con las PCI DSS. Sin embargo, existen diferentes requisitos para la presentación de informes y la auditoría de las concesionarias en función del nivel de comerciante. El nivel de comerciante está determinado por el número de transacciones con tarjeta de crédito en la concesionaria. Para obtener más información sobre PCI DSS y estos requisitos, visite: https://www.pcisecuritystandards.org

- Recursos adicionales
  - Las siguientes organizaciones tienen información para ayudar a implementar salvaguardas apropiadas para los datos:
    - Centro de Recursos de Seguridad Informática Instituto Nacional de Estándares y Tecnología (NIST) - http://csrc.nist.gov
    - Estrategia nacional para asegurar el ciberespacio, Departamento de Seguridad Nacional - http://www.dhs.gov/files/publications/editorial_0329.shtm
    - El SysAdmin, Auditoría, Red, Seguridad (SANS) instituye las veinte vulnerabilidades de seguridad de Internet más críticas - www.sans.org/top20
    - Equipo de preparación para emergencias informáticas de los Estados Unidos - www.us-cert.gov/resources.html
    - Centro de Coordinación CERT del Instituto de Ingeniería de Software Carnegie Mellon- www.cert.org

2.6.f Seguridad de la Red

Las concesionarias deben enfocarse en la seguridad y la integridad de los datos de red de área local (LAN) de la concesionaria. Esto comienza 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 en la red puede acceder cada usuario y dónde se almacenan los datos en la red. Las políticas también deberían indicar deliberadamente en qué dispositivos se almacenan los datos de la compañía. Consulte la sección 2.6.a para obtener más orientación sobre políticas de seguridad y prácticas.

Más allá de las políticas, la red debe configurarse y segmentarse de la manera más segura posible para evitar el acceso no deseado. Use las siguientes recomendaciones cuando configure y asegure la red de la concesionaria.

Recomendación	Especificación
Cortafuegos / UTM	Un dispositivo de seguridad totalmente administrado que monitorea continuamente en busca de amenazas a través del 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 filtrado de paquetes, antivirus e inspección de paquetes *stateful*. ● Filtrar paquetes y protocolos (por ejemplo: IP, ICMP) ● Escaneo de antivirus ● Realizar una inspección *stateful* de las conexiones. ● Realizar operaciones proxy en aplicaciones seleccionadas ● Informar el tráfico permitido y denegado por el dispositivo de seguridad de forma regular (mensualmente, por ejemplo) Debido a la importancia del Cortafuegos y al hecho de que a menudo se encuentra en la ruta de datos para la mayoría del tráfico de concesionarias, STAR recomienda un dispositivo de respaldo en caso de falla. Para limitar el tiempo de inactividad, los distribuidores deben considerar una solución para la conmutación automática al dispositivo de respaldo en caso de una falla de hardware.
Segmentación de Red	La información de la tarjeta de pago, la información del cliente, el tráfico de la concesionaria y el tráfico del cliente deben segmentarse a través de la segmentación de la red (como VLAN) o una red diferente (como un circuito dedicado para invitados) para garantizar la seguridad de los datos.
Filtrado de contenido	La pérdida de datos puede provenirse si los empleados no navegaran por la web para actividades no relacionadas con el negocio. STAR recomienda que las concesionarias filtren contenido en la red para eliminar el posible tráfico nocivo, inapropiado u otro tráfico no relacionado con el negocio.
Gestión de eventos de información de seguridad (SIEM)	Una solución SIEM proporciona visibilidad más allá de la protección del AV o cortafuegos. El objetivo final de una solución SIEM es recopilar e inspeccionar el tráfico de la seguridad de la red para encontrar indicios de comprometimiento. Esta indicación debe enviarse, como una alerta, a un recurso calificado para que realice investigaciones y posibles actividades de remediación inmediatamente. Es importante tener en cuenta que la adopción del software SIEM por sí sola no es adecuada para proteger la red del distribuidor. Las concesionarias deben contar con procesos y recursos para responder a la información generada por la tecnología SIEM. La orientación general para la gestión de la información de seguridad de la concesionaria es la siguiente. Las concesionarias deben tener: ● Monitoreo proactivo de eventos en tiempo real que utilice un servicio SIEM. ● SIEM necesita poder recopilar datos con capacidad para agregar y correlacionar datos de seguridad variables de la red en tiempo real. ● El proveedor de servicios SIEM debe poder notificar al administrador de la red en el caso de un evento de seguridad, así como proporcionar la documentación adecuada para fines de cumplimiento. ● El objetivo final de un servicio SIEM es ayudar a identificar o prevenir una intrusión en su red. La respuesta inmediata a una violación puede reducir o prevenir en gran medida la pérdida de datos. **Nota**: El software de gestión reactiva (por ejemplo: cortafuegos de PC de escritorio o antivirus) no debe confundirse con un servicio SIEM proactivo.
Pruebas de penetración y escaneo de vulnerabilidades	Se recomienda realizar pruebas anuales de penetración interna y externa en la red de los distribuidores. Una prueba de penetración ("*pentest*") es un método para evaluar la seguridad de un sistema informático o una red mediante la simulación de un ataque desde una fuente maliciosa. Se debe realizar una prueba de penetración en cualquier sistema informático que se vaya a implementar en un entorno de red, en particular aquellos con cualquier sistema expuesto a Internet. Los trabajos de prueba de

	penetración pueden realizarse externamente (simulación de un ataque desde fuera de su red y exactamente como si se lanzara un intento de piratería desde un país extranjero), o puede realizarse internamente (desde dentro de su red para ver qué acceso y vulnerabilidades existen).
Socios de Integración Certificados	Asegúrese de que los integradores de datos del vendedor estén certificados con aplicaciones DMS y OEM. Los puntos de integración hostiles o no autorizados a menudo son menos seguros y, a veces, requieren que la concesionaria comparta información de usuario y contraseña.
Sistema de detección inalámbrico	Escanee, identifique y elimine cualquier punto de acceso inalámbrico no autorizado que pueda estar en la red de minoristas. Un punto de acceso inalámbrico no autorizado se define como un punto de entrada inalámbrico en la red de la concesionaria que no está autorizado, asegurado o no es conocido por la TI, la administración y la propiedad de la concesionaria. Todas las redes inalámbricas no autorizadas se deben detectar, encontrar y eliminar de inmediato. STAR recomienda el uso de un servicio de detección inalámbrica administrada que esté continuamente escaneando la red en busca de amenazas inalámbricas.

2.6.g Seguridad del Escritorio

Recomendación	Especificación
Monitoreo de Virus de PC	Los productos antivirus de nivel corporativo deben instalarse en todas las PC y configurarse para realizar automáticamente lo siguiente: ● Descargar e instalar las actualizaciones de firmas de virus más recientes ● Monitorear activamente en busca de virus ● Poner en cuarentena y erradicar archivos infectados ● 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 garantizar que cada estación de trabajo tenga los parches de Microsoft actualizados. La administración de la estación de trabajo debe incluir monitoreo remoto de fallas de hardware/software, servidores inactivos, poco espacio en disco, uso excesivo de CPU y uso excesivo de memoria.
Protección de contraseña	Las contraseñas se deben configurar para que caduquen cada 60 días o menos. Como mínimo, las concesionarias deben usar "contraseñas seguras" que contengan un mínimo de 8 caracteres compuestas por 3 de los siguientes 4 requisitos: 1) mayúsculas 2) minúsculas 3) números 4) caracteres especiales
Plataforma de detección y respuesta de punto final	Se debe implementar una plataforma singular de protección de punto final (EPP) y una solución de detección y respuesta de punto final (EDR) en dispositivos de punto final para evitar ataques de malware basados en archivos; detectar actividad maliciosa y proporcionar las capacidades de investigación y corrección necesarias para responder a los incidentes y alertas de seguridad dinámica. Las alertas de este servicio deben responderse de inmediato para mitigar el riesgo y la posible pérdida de datos. La oferta de los servicios deben proporcionar visibilidad multiplataforma en las actividades de servidor/punto final, así como: ● Detección de amenazas a través de motores de IA estáticos, de comportamiento y HIDS dentro del agente de punto final ● Contención de amenazas y orientación de remediación ● Informes de actividad y búsqueda de amenazas ● Visibilidad multiplataforma en la ejecución de procedimientos, comunicaciones de red, acceso a archivos, aplicaciones, solicitudes de DNS y tráfico web cifrado

2.6.h Seguridad del Correo Electrónico

Descripción general: La seguridad del correo electrónico es un riesgo crítico para muchas de las organizaciones más grandes del mundo. Hoy, 91% de todos los ataques exitosos en redes empresariales implican el uso del correo electrónico. Una solución para la seguridad del correo electrónico proporcionará inspección de contenido entrante y saliente, cifrado y alertas de seguridad para mitigar muchos de estos riesgos.

Seguridad del Correo Electrónico Saliente: identifique y responda ante malware, correos electrónicos inapropiados, contenido no autorizado e información privada de la compañía 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 ingresar a la red.

Encriptación: se recomienda el cifrado de correo electrónico TLS para que sea más difícil para terceros leer el correo electrónico en tránsito.

2.6.i Seguridad de la Aplicación

A continuación, suponga que todas las aplicaciones se adquieren de proveedores externos y se implementan sin ninguna modificación, o solo se aplica una pequeña personalización. Además, por una aplicación, se entiende que son aplicaciones comerciales y la seguridad de la aplicación se debe asegurar de que todos los datos procesados, y todas las funciones comerciales ofrecidas por la aplicación estén protegidas adecuadamente.

- Áreas y actividades clave
  - Realizar un inventario de aplicaciones. Documente qué aplicaciones hay en la red de la concesionaria, cuál es su propósito, quién es responsable y cómo obtener soporte. Realice el Análisis de Impacto Comercial (BIA) incluyendo la clasificación de información para comprender la importancia crítica 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 de distribuidores y la seguridad de los datos.
  - Proteger la información procesada en tránsito y en almacenamiento. Asegúrese de que los datos confidenciales y críticos estén bien protegidos, tanto desde una perspectiva de confidencialidad como desde su integridad. Revise tanto las integraciones de aplicación a aplicación como las aplicaciones de comunicación interna, especialmente las conexiones a la base de datos, que a menudo son olvidadas. Si es necesario, asegúrese de utilizar la criptografía correcta para la protección en el almacenamiento. Finalmente, asegúrese de que los flujos de información estén protegidos desde una perspectiva de extremo a extremo.
  - Considerar requisitos comerciales adicionales tales como autenticidad, no repudio o trazabilidad; a menudo requeridos para cumplir con las normas de privacidad (por ejemplo: GDPR).
  - Aplique el principio de Defensa en profundidad introduciendo la configuración precisa de zonas de seguridad y la colocación de componentes de la aplicación, servicios de infraestructura adicionales como servidores proxy inversos o cortafuegos de aplicaciones web y capas de control de acceso como autenticación multifactor, etc.
  - Aplicar la estrategia adecuada de Gestión de Identidad y Acceso (ver más en la sección IAM). Aplique los principios de menos privilegiados y necesarios de conocer.
  - Espere de un proveedor el resultado de un escaneo de vulnerabilidad de la aplicación, realizado por una empresa independiente. Asegúrese de que se aborden todos los riesgos altos y medios identificados.
  - Parte de una estrategia de seguridad también es asegurarse de que las transacciones comerciales se manejen sin errores y en el nivel esperado de calidad. Por eso, uno puede esperar que una compañía proveedora proporcione resultados de pruebas o informes de auditorías.
  - Introducir procesos para el manejo de incidentes, solicitudes de acceso, etc. Considere la introducción de monitoreo de aplicaciones comerciales para rastrear o incluso prevenir eventos no deseados. Por lo general, esto es parte de una implementación de administración de servicios de TI.
  - Realizar, de forma regular, actividades de modelado de amenazas para asegurarse de que los riesgos del entorno de la aplicación estén documentados, mitigados y mantenidos bajo control.

- Aplique actualizaciones y parches de aplicaciones lo antes posible para limitar la exposición a posibles vulnerabilidades.

2.6.j Movilidad

Esta área está fuertemente conectada a otras áreas como seguridad de la aplicación o seguridad del correo electrónico. Sin embargo, se considera por separado debido a los riesgos adicionales que introduce por tener mucho menos control sobre los tipos de dispositivos definidos. Los dispositivos móviles se definen aquí como teléfonos inteligentes, tabletas, computadoras portátiles y cualquier otro dispositivo especializado que procese o almacene datos de la compañía.

- Áreas y actividades clave
  - Crear políticas y procedimientos para quién, cuándo y cómo accede de forma remota 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 restrinjan el acceso a la red interna de la empresa; y permitir el acceso a la red interna de la empresa para computadoras portátiles administradas a través de VPN. Implemente una solución técnica adecuada para respaldar el enfoque establecido.
  - Definir qué información se puede procesar y almacenar en los dispositivos móviles; asegúrese de incluir consideraciones relacionadas con los dispositivos administrados y no administrados.
  - Introducir políticas, procedimientos y capacidades técnicas para definir qué software se puede instalar y ejecutar en todo tipo de dispositivos móviles. En el caso de dispositivos no administrados, introduzca condiciones en las que los datos de la empresa no estén expuestos a riesgos inaceptables (por ejemplo: mediante la instalación de soluciones como MobileIron o Microsoft iTunes para teléfonos inteligentes).
  - El acceso a los dispositivos debe estar restringido, lo que requiere la autenticación del usuario. La mayoría de los dispositivos se pueden bloquear con un bloqueo de pantalla, contraseña o PIN.
  - Aplicar la estrategia adecuada de gestión de identidad y acceso.
  - Asegúrese que la configuración y el “endurecimiento” del dispositivo y del sistema operativo sean los adecuados (por ejemplo: contraseña de BIOS, dispositivo encriptado, disponibilidad de puertos USB y SD). Asegúrese de que (especialmente en el caso de dispositivos Android e iOS) el dispositivo no esté rooteado ni liberado.
  - Mantenga su software antimalware actualizado y, preferiblemente, administrado centralmente tanto en computadoras portátiles como en teléfonos inteligentes.
  - Actualice el SO móvil con parches de seguridad. Puede encontrar más información sobre gestión de parches en la sección 2.6.c.
  - Aplique el cifrado adecuado de datos tanto en computadoras portátiles como en dispositivos móviles con especial cuidado en la administración 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 y también pueden ejecutarse ataques por un intermediario.
  - Habilite la opción de borrado de datos remotos si estuviera disponible.
  - Realice copias de seguridad del dispositivo móvil regularmente.

2.7 Proveedores de Servicios Gestionados

Los distribuidores a menudo recurren a proveedores o socios para ayudarlos a administrar, mantener y asegurar la infraestructura de la concesionaria. Un proveedor de servicios puede tener la tecnología o la experiencia para proporcionar a la concesionaria una solución para manejar de manera más efectiva diferentes aspectos de la red de concesionarias. Los vendedores a menudo no tienen el tiempo, los recursos o la experiencia para administrar una red empresarial 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 cuando se selecciona un tercero para ayudar con la asistencia de infraestructura de red. El proveedor se comprometerá de acuerdo al nivel de servicio esperado, el alcance del servicio(s) y cualquier reembolso o cargo compensatorio por compromisos incumplidos.

La siguiente sección proporciona una guía para seleccionar y comprender los acuerdos de nivel de servicio.

2.7.a Acuerdos de Nivel de Servicio(SLA)

Las concesionarias que reciben servicios de TI confían mucho en el Acuerdo de Nivel de Servicio (SLA) que seleccionan. El SLA detallará la calidad de servicio (QoS) que el proveedor ofrece con su servicio; en otras palabras, su garantía de que el servicio se efectuará según lo prometido.

Los SLA se usan en una amplia variedad de servicios de TI de distribuidores que incluyen (entre otros):

- Servicio de internet
- Servicios de integración de redes
- Servicios de soporte de hardware y software
- Soporte en el sitio
- Soporte de mesa de ayuda y centro de llamadas

Al elegir un proveedor de servicios, asegúrese de hacer las siguientes preguntas con respecto a los SLA.

- ¿Hay un SLA escrito?
- ¿Cuáles son los contratiempos, reembolsos u otras consecuencias si el proveedor no cumple con su SLA?
- ¿Hay informes disponibles contra el SLA?
- ¿Se puede cancelar el servicio si no se cumple el SLA?

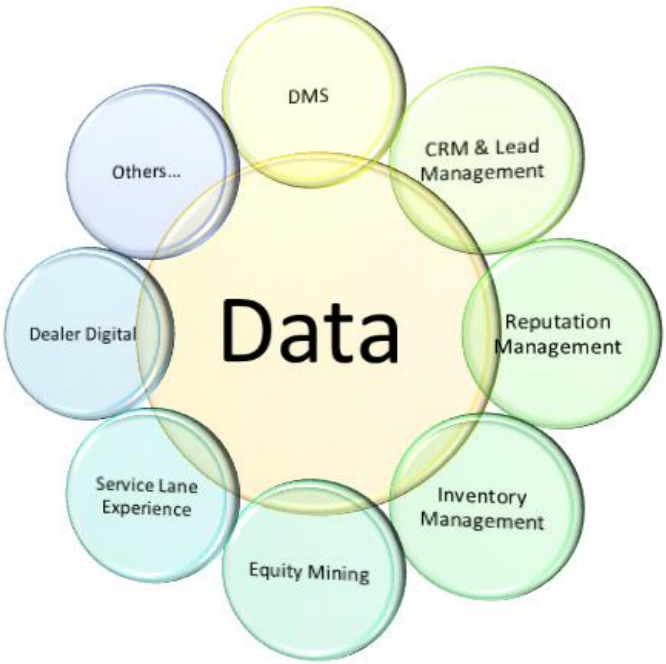
Los SLA comunes incluyen (pero no se limitan a):

- Disponibilidad de red
- Velocidad de red
- Latencia de red
- Tiempo de reemplazo de hardware
- Horas de soporte disponibles
- Compromisos de servicio en el sitio
- Acuerdos de mantenimiento de hardware o software

3. Proveedores de Sistemas de Concesionarias

3.1 Descripción general

La complejidad de una concesionaria y su tecnología asociada ha evolucionado mucho desde el inicio de STAR. Esta tecnología siempre cambiante ha continuado mejorando el valor comercial general de STAR y los estándares de integración utilizados para alinear los datos entre sistemas y procesos.



Mientras que un Sistema de Gestión de la Concesionaria (DMS) ha sido tradicionalmente el núcleo del Ecosistema de Tecnología de la Concesionaria, ahora hay muchos sistemas diferentes en los cuales todos necesitan compartir datos para garantizar que los clientes, vehículos y piezas se puedan administrar de manera efectiva en todo viaje en línea y fuera de línea. Este ecosistema de proveedor de servicios de distribuidor (DSP) cambia constantemente, y es absolutamente crítico garantizar que los procesos se implementen para una integración de datos segura y eficiente.

Las opciones de DSP cambian cada día y es fundamental que los distribuidores comprendan la importancia de una integración de datos segura y efectiva. Hay soluciones DSP que se centran en el *front-end* de la concesionaria y hay soluciones que se centran en el *back-end*. Otras soluciones están dirigidas a administrar clientes en línea y fuera de línea y algunas buscan específicamente ayudar a las concesionarias con la comercialización del inventario de vehículos nuevos / usados, la gestión y distribución de contenido, o para mantener una imagen positiva dentro de las redes sociales y el mundo en línea.

Ya sea que trabaje con un proveedor que ofrezca numerosos productos o que se especialice en una capacidad específica, es importante asegurarse de comprender cómo se integrarán y administrarán los datos en todo el ecosistema.

No existe un enfoque único para implementar una solución DSP para una concesionaria, pero es de vital importancia alinear las tecnologías con las prioridades comerciales e implementar procesos de administración de datos que respalden la experiencia deseada del cliente. Los clientes esperan cada vez más experimentar una transcisión perfecta entre contenido en línea y sin conexión que solo se puede lograr a través de la integración de datos.

La concesionaria tiene una gran cantidad de opciones al decidir qué DSP se utilizarán dentro de su huella de red. Los DSP a menudo sirven como un "centro" de datos de la concesionaria, comunicaciones y operaciones comerciales. Al revisar varias ofertas de DSP, la sección de Infraestructura de Red de Vendedores STAR DIG puede proporcionar orientación sobre las diferentes funciones que un proveedor de servicios del sistema puede ofrecer a las concesionarias.

3.2 Integración de datos y estándares: el beneficio STAR

La organización STAR y los estándares de integración contenidos dentro fueron creados para optimizar las actividades de integración de datos de la concesionaria entre el OEM y DSP (principalmente DMS al principio) utilizando Internet como medio principal.

Al igual que con toda la tecnología, Internet ha seguido evolucionando, y la infraestructura utilizada para operar negocios que la utilizan ha experimentado una enorme cantidad de innovación. Estas mejoras han resultado en un método extremadamente confiable para integrar procesos de negocios y sistemas asociados.

En el corazón de todos estos sistemas se encuentran los datos necesarios para respaldar el procedimiento comercial deseado. Los datos del vehículo, los datos de las piezas, los datos del cliente, los datos del servicio, los datos financieros y muchos otros grupos de datos deben pasar de un sistema a otro, y entre la concesionaria (junto con el DSP) y el OEM, de manera transparente y segura. Los estándares de integración de datos de STAR son estándares abiertos que permiten a los proveedores y OEM un método para reducir el tiempo de desarrollo general y simplificar las implementaciones a través de un conjunto de documentos que describen los elementos de datos necesarios para respaldar los objetivos comerciales (BODs – Documentos de Objetos Comerciales).

Con el tiempo, estos BOD se pueden mejorar con definiciones/reglas comerciales 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 simple. Con el panorama de la tecnología de la concesionaria cada vez más complicado con el paso de los años, ¡los estándares realmente comenzarán a demostrar los beneficios STAR!

3.3 Panorama Tecnológico de la Concesionaria (Opciones DSP)

Parece que el Panorama Tecnológico de la Concesionaria estará en un estado de cambio constante en un futuro previsible. Pasar cualquier cantidad de tiempo tratando de definir este panorama solo daría como resultado un documento que quedará desactualizado poco después de su publicación.

En los últimos años, varias categorías nuevas y significativas de productos DSP se han unido al DMS tradicional y han dejado una marca permanente dentro del ecosistema minorista automotriz, por lo que vale la pena proporcionar un poco de su información de fondo. Al igual que con todas las opciones de DSP, uno debe tomarse un tiempo para comparar capacidades y asegurarse de que la solución se alinee con las Pautas de Infraestructura STAR.

Además de comparar capacidades y comprender la integración general, es extremadamente importante comprender la gestión de datos y los elementos de entrada/salida asociados con la solución. La administración completa de los datos y la transparencia de uso son cruciales para cualquier solución DSP/OEM.

3.3.a DMS

El Sistema de Gestión de la Concesionaria (DMS) es un sistema de información de gestión integrada creado específicamente para las concesionarias de automóviles de la industria automotriz. Se ha adaptado aún más (generalmente como un producto DMS especializado) para vendedores de equipos pesados, botes, bicicletas, vehículos recreativos y equipos deportivos de potencia. El DMS contiene funcionalidades para respaldar los componentes de finanzas, ventas, inventario, piezas, servicio y contabilidad / oficina comercial para el funcionamiento de la concesionaria.

Algunas soluciones DMS se ofrecen con servidores centrales en el sitio, y otras se ofrecen aprovechando "la nube" utilizando un modelo de software como servicio (SaaS); Una solución en el sitio o basada en SaaS podría ser la adecuada, dependiendo de las necesidades de la concesionaria. Una consideración importante es el mantenimiento del hardware que se utiliza para atender las necesidades de la aplicación. Los servicios SaaS se generan en la nube y no requieren mucho mantenimiento, mientras que las soluciones en el sitio a menudo requieren de gestión de PARCHES, actualizaciones y un 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 regulaciones estatales/locales/de mercado/regionales y las marcas OEM para el grupo de concesionarias específico.

3.3.b CRM y Gestión de Prospectos

Los sistemas de Gestión de Relación con el Consumidor (CRM) y gestión de prospectos se utilizan para capturar, rastrear y administrar de manera efectiva la correspondencia en línea y fuera de línea con prospectos y clientes.

Las soluciones CRM y de gestión de prospectos requieren integración con datos DMS (clientes) y todas las fuentes de clientes potenciales (prospectos).

El sistema CRM proporciona una funcionalidad que ayuda al personal de la concesionaria a gestionar la relación con el cliente durante todo el ciclo de vida del cliente. Se pueden gestionar las fechas clave del cliente y del vehículo, las citas de servicio y muchos otros aspectos.

El sistema de gestión de prospectos proporciona funcionalidad para asignar clientes potenciales al personal de ventas y servicio (o a través de un centro de desarrollo empresarial definido) para su seguimiento. Estas actividades de seguimiento de prospectos tienen como objetivo aumentar las ventas y los ingresos.

Las consultas de los prospectos se recopilan y almacenan de muchas fuentes diferentes, entre otras:

- Visitas
- Prospectos de compras en línea
- Prospectos proporcionados por OEM
- Prospectos telefónicos
- Captura eventual de prospectos

Las soluciones CRM y Gestión de Prospectos también se utilizan para generar nuevos negocios. Al alinear las soluciones de la concesionaria con los manifiestos OEM, otras soluciones DSP (por ejemplo: Minería de Capitales) y las necesidades de automóviles usados, es posible llegar efectivamente a los clientes existentes y crear negocios adicionales.

Las concesionarias necesitan la infraestructura para soportar clientes potenciales de empresas de nivel 3. Una solución eficaz de gestión de prospectos también debería tener en cuenta las organizaciones de nivel 3 (como cars.com y truecar.com).

3.3.c Manejo de Reputación

Una solución de Manejo de Reputación proporciona funcionalidad para ayudarlo a monitorear, comprender, identificar y abordar lo que la gente escribe en línea sobre su concesionaria.

Una solución de Manejo de Reputación requiere integración con fuentes de datos DMS y OEM.

La reputación en línea de una concesionaria se define por los comentarios que se encuentran en los sitios de revisión de clientes, blogs, sitios web y sitios de redes sociales. Internet facilita la búsqueda de información sobre una concesionaria con poco esfuerzo. En unos pocos clics, un cliente tiene una instantánea de lo que trata una concesionaria, dónde está ubicada y cómo se sienten los clientes sobre la concesionaria en general. En la mayoría de los casos, los resultados de búsqueda incluyen calificaciones y reseñas en estrellas. Estas calificaciones y revisiones influyen en la decisión del cliente de comprar un vehículo en una concesionaria.

3.3.d Gestión de Inventario En Línea

Una solución de gestión de inventario de concesionaria proporciona funcionalidad para permitir la comercialización, la gestión de contenido y la distribución de inventario de vehículos. Esto incluye la distribución dirigida por la concesionaria del inventario de vehículos nuevos/usados en existencia a la web y/o publicaciones impresas junto con fotos del vehículo, videos, precios, incentivos, etc.

Una solución de gestión de inventario de la concesionaria requiere integraciones con el DMS, herramientas de precios de terceros, proveedores de servicios de lotes, proveedores de servicios de descripción de vehículos (validación de VIN y datos de construcción) y OEM.

3.3.e Minería de Capitales

Una solución de Minería de Capitales proporciona la funcionalidad para identificar a los consumidores cuyo vehículo supone un capital y luego los proporciona como posibles clientes potenciales a través de un Centro de Desarrollo de Negocios (BDC), gerente de Internet, equipo de ventas u otros representantes de distribuidores apropiados.

Una solución de Minería de Capitales requiere integración con datos DMS (clientes), CRM / LM (clientes potenciales), fuentes de intercambio, datos bancarios (financiamiento y arrendamiento) e incentivos.

3.3.f Herramientas de Canal de Servicio

Las Herramientas de Canal de Servicio son un procedimiento o solución basada en el flujo de trabajo que abarca la funcionalidad que se ha encontrado tradicionalmente en soluciones separadas relacionadas con el servicio (es decir, DMS, programa de servicios en línea, menús de servicio, controles de estado del vehículo, etc.). Permite una experiencia del cliente constante y sin problemas a través de las siguientes etapas: 1) programación de la cita, 2) redacción del servicio, 3) vehículo en servicio y 4) entrega del servicio.

Las Herramientas de Canal de Servicio requieren su integración con fuentes de datos DMS y OEM.

3.3.g Vendedor Digital

Un Paquete de Marketing Digital para Vendedores es un conjunto de servicios de marketing minorista que permite a los vendedores entregar mensajes coherentes y sincronizados a los consumidores que utilizan canales digitales emergentes. Proporciona una plataforma inteligente de mercadeo en red con alineación de mercadeo con la marca la concesionaria. También proporciona análisis que respaldan la optimización del gasto en marketing multinivel y la mejora del rendimiento de la red de distribuidores en los procesos de marketing y ventas.

Las soluciones de Vendedor Digital requieren integración con fuentes de datos DMS, CRM y OEM.

Los componentes principales de una solución de Vendedor Digital pueden incluir:

- Sitio web del vendedor (web y móvil)
- Optimización de motores de búsqueda (SEO)
- Gestión de audiencia
- Perspectivas y análisis
- Gestión de activos (imágenes, videos, etc.)
- Chat
- Citas

4. Recuperación de Desastres y Continuidad del Negocio

4.1 Descripción general

La recuperación de desastres y la continuidad del negocio es la capacidad de una organización para recuperarse ante un desastre y reanudar las operaciones normales de la red. Las concesionarias deben tener un plan que detalle la tecnología, los procesos y los pasos del procedimiento a seguir en caso de una falla. La clave para una recuperación de desastres exitosa es tener un plan mucho antes de que ocurra la interrupción.

La planificación de la recuperación ante desastres y la continuidad del negocio son procesos que ayudan a las organizaciones a prepararse para eventos disruptivos, ya sea que esos eventos puedan incluir un tornado devastador o simplemente una línea de internet rota causada por congelamiento y descongelamiento repetidos.

Para comprender lo que podría suceder en el caso de una falla de la red, se recomienda a una concesionaria que primero comprenda qué datos están en riesgo. ¿Cuánto tiempo pueden no estar disponibles esos datos? ¿Qué sucedería cuando no esten disponibles? ¿Qué pasos se pueden realizar para asegurarse de que se mitiga el riesgo? En esta sección se detallan algunas respuestas básicas a esas preguntas, así como algunas recomendaciones para planificar antes de una falla, como también la restauración de las operaciones de la red.

4.2 Análisis de Riesgos & Mitigación

El objetivo principal del análisis de riesgos es ayudar a la concesionaria a identificar todas las áreas en las cuales podría haber riesgo de pérdida. Esto puede ser en el hardware, en el software, en el edificio, en el personal, etc. Una vez que se hayan identificado los diversos elementos, la concesionaria puede clasificar el nivel de cada riesgo y determinar cómo ese riesgo afecta a la concesionaria.

A continuación se enumeran algunas de las diversas categorías de riesgo a las que se puede enfrentar una concesionaria.

- Personal clave
- Edificio
- Falla clave en el sistema
- Falla total del sistema
- Pérdida de datos

Hay varias formas en que una organización puede mitigar el riesgo. Estos planes o soluciones pueden ser internos o externos. Algunos ejemplos de cada uno siguen.

Opciones de mitigación de riesgos en el sitio	Opciones de mitigación de riesgos fuera del sitio
Hardware redundante	Software de respaldo remoto
Software y servidores de respaldo de datos en el sitio	Almacenamiento en la nube
Fuente de alimentación ininterrumpida (UPS)	Contratos de servicio de hardware de RMA
Generadores	

5. Computación en la Nube y Virtualización

5.1 Descripción general

Las tendencias emergentes importantes en tecnología de la información se pueden resumir como un paradigma basado en servicios y virtualización. Con un "*paradigma basado en el servicio*", condensamos diferentes acrónimos, como la Arquitectura orientada a servicios (SOA) y el concepto popular de Computación en la Nube (que tiene implicaciones comerciales relevantes). "*La principal tecnología habilitadora para la computación en la nube es la virtualización. La virtualización proporciona la agilidad requerida para acelerar las operaciones de TI y reduce los costos al aumentar la utilización de la infraestructura*" (Wikipedia)

5.2 Virtualización del Cliente/Servidor

La virtualización, en informática, significa crear una versión virtual de un dispositivo o recurso, como un servidor, dispositivo de almacenamiento, 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 recurso físico real y único. En un entorno de distribuidor, las áreas más relevantes para la virtualización son Server Virtualization y Client Virtualization; ambos son interesantes y aseguran ahorros constantes.

5.3 Computación en la Nube

"La computación en la nube es un modelo que permite el acceso ubicuo, conveniente y bajo demanda a la red de un grupo compartido de recursos informáticos configurables (Por ejemplo: Redes, servidores, almacenamiento, aplicaciones y servicios) que se pueden aprovisionar y liberar rápidamente con un mínimo esfuerzo de gestión o interacción del proveedor de servicios." (definición del NIST - Instituto Nacional de Estándares y Tecnología)

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

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

- Software como servicio (SaaS): la capacidad proporcionada al consumidor para usar las aplicaciones del proveedor que se ejecutan en una infraestructura en la nube.
- Plataforma como servicio (PaaS): la capacidad proporcionada al consumidor para implementar en la infraestructura de la nube aplicaciones creadas o adquiridas por el consumidor; diseñadas utilizando lenguajes de programación, bibliotecas, servicios y herramientas compatibles por el proveedor.
- Infraestructura como servicio (IaaS): la capacidad proporcionada al consumidor para aprovisionar procesamiento, almacenamiento, redes y otros recursos informáticos fundamentales donde el consumidor puede implementar 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 están ofreciendo algo similar a un modelo SaaS para su DMS. Los otros 2 modelos rara vez son adoptados por las concesionarias, con algunas excepciones (por ejemplo: la IaaS para desastres/recuperación es una opción interesante).

6. Prácticas de Capacitación, Procedimientos y Documentación

Muchos expertos argumentarán que la mayoría de las violaciones de datos se deben a errores humanos. En años anteriores, los estudios de Nuspire Networks, IBM, Verizon y The Ponemon Institute han concluido que la mayor amenaza para los datos de los distribuidores podrían ser los empleados. Más allá de la seguridad, los empleados son a menudo la causa de las interrupciones en la red, fallas del dispositivo y operaciones comerciales lentas. La mayoría de las veces, la causa principal no son empleados deficietes, sino su falta de capacitación y documentación. Los empleados a menudo dejan entrar un incidente de seguridad, no saben cómo usar los sistemas y/o causan fallas en la red porque no han recibido capacitación sobre qué hacer o qué no hacer. Esta falta de capacitación de empleados a menudo puede conducir a una falta de documentación.

La siguiente sección cubre consejos y pautas de capacitación desde una perspectiva tecnológica y de seguridad de datos. Se alienta a las concesionarias a adoptar políticas y procedimientos de capacitación. Estas políticas deben estar bien documentadas y deben ser utilizadas en la capacitación de empleados. La documentación, el proceso y el procedimiento por sí solos pueden tener un impacto positivo en las operaciones de red y la seguridad de los datos de la concesionaria.

6.1 Capacitación de Empleados

Recomendación	Especificación
Entrenamiento de seguridad	Tenga un programa de capacitación sobre seguridad formal y por escrito para cada empleado. La capacitación debe cubrir aspectos que incluyan el conocimiento de la ingeniería social, la gestión de contraseñas, las políticas de intercambio de datos y los procedimientos de manejo de datos confidenciales. Revise regularmente los programas de capacitación y ajústese a las nuevas tecnologías, los cambios comerciales de la concesionaria y los comentarios de los empleados.
Responsabilidad de seguridad diseñada	Designe a un empleado como Coordinador del Programa para su programa de seguridad de la información.
Capacitación en sistemas de TI para concesionarias	Brinde capacitación formal para aplicaciones críticas, hardware y otros sistemas de TI de la concesionaria. Un empleado bien informado puede aumentar la productividad, reducir los costos de soporte y mejorar la satisfacción del cliente.

6.2 Procedimiento

Recomendación	Especificación
Acceso de nuevos empleados	Tenga un procedimiento escrito y formal para otorgar acceso al sistema a los nuevos empleados. Esto debe incluir nombres de usuario y contraseñas únicos.
Acceso de empleado terminado	Tenga un procedimiento escrito y formal para eliminar a los empleados de la red de TI de la concesionaria, recuperar el hardware de la concesionaria e inactivar todas las cuentas de los empleados antes de que se vayan.
Capacitación en sistemas de TI	Tenga un programa formal para abordar la capacitación sobre tecnologías, aplicaciones y hardware de la concesionaria. Un empleado bien informado puede aumentar la productividad, reducir los costos de soporte y mejorar la satisfacción del cliente.
Evaluación de riesgos	Identifique riesgos internos, externos y razonablemente previsibles para la seguridad, confidencialidad e integridad de la información del cliente. Diseñe e implemente salvaguardas del cliente para controlar los riesgos identificados a través de la evaluación de riesgos.
Controles de seguridad de terceros (proveedor)	La selección de proveedores de servicios de confianza es muy importante. Seleccione proveedores de servicios con experiencia en la protección de la información del cliente de un distribuidor.
Manejo y respuesta de incidentes de seguridad	Tenga un procedimiento formal para responder ante incidentes de seguridad en la red. Cubra aspectos relacionados con la identificación de violaciones de seguridad, respuesta, comunicación y documentación.

6.3 Documentación

Recomendación	Especificación
Documentación de seguridad	Cree una política de seguridad escrita que aborde los estándares técnicos, de procedimiento y administrativos para afrontar la seguridad de los datos del cliente. La documentación debe incluir: ● Capacitación de Empleados ● Respuesta y gestión de incidentes/incumplimientos ● Acuerdos de uso de internet para empleados ● Políticas y procedimientos para el monitoreo y la gestión de la red.
Documentación para nuevos empleados	Tener un programa escrito para nuevos empleados. Esto debe incluir capacitación en seguridad, capacitación en sistemas y un procedimiento documentado para solicitar soporte técnico de TI.
Documentación de sistemas	Poner a disposición capacitación para aplicaciones críticas, hardware y otros sistemas informáticos de los distribuidores. Un empleado bien informado puede aumentar la productividad, reducir los costos de soporte y mejorar la satisfacción del cliente.

7. Apéndices

7.1 Guía de política de seguridad de la concesionaria

El marco de las Políticas de Seguridad de la concesionaria debe ser completo, consistente y aprobado por el órgano de administración de la concesionaria. Es importante asegurarse de que todas las partes interesadas se comprometan con las políticas y acuerden implementarlas en todos los aspectos relevantes de la concesionaria.

Las políticas deben reflejar la estrategia para asegurar la información, y no al revés, y comprender los requisitos de seguridad es el factor clave aquí. El enfoque básico debe estar en la confidencialidad, integridad y disponibilidad de datos y recursos confidenciales, incluido 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: con bastante frecuencia se debe considerar el no repudio, la trazabilidad o la autenticidad.

Además, cada industria tiene sus propias áreas sensibles. Por ejemplo: nos preocupamos mucho más por la integridad, en lugar de la confidencialidad, de un avión en el aire o de un automóvil en la carretera en comparación con la confidencialidad del historial médico de un paciente (que también puede depender del contexto). Las políticas de seguridad deben reflejar estas consideraciones.

Hay muchas políticas para la seguridad inmediatamente disponibles o directivas para ser usadas de las cuales seleccionar y aplicar en una empresa. Sin embargo, aunque este tipo de marco puede proporcionar una línea de base general, una empresa necesita ajustar y desarrollar las políticas para su aplicación dentro de su contexto comercial.

Reglas generales

- Asegúrese de que haya un entendimiento compartido con la Administración sobre lo que debe protegerse y el nivel de expectativa respecto a la protección de datos. Por un lado, es importante que las políticas garanticen el nivel de protección esperado. Sin embargo, también es muy importante que las políticas no sean tan restrictivas como para impedir que la empresa haga los negocios necesarios.
- Asegúrese de que las políticas estén alineadas con las leyes y regulaciones (por ejemplo: en el área de privacidad o las regulaciones específicas de la industria).

- Desarrollar políticas para reflejar prácticas de seguridad reales y alcanzables. Es mejor tener un pequeño conjunto de reglas en lugar de un documento completo que sea imposible de seguir. En caso de que el estado real esté lejos del nivel esperado, desarrolle un plan de transición acordado por todas las partes interesadas clave para llevar a una organización del estado actual al nivel esperado. Es muy importante desarrollar un buen plan de comunicación como parte del programa general de seguridad.
- Las políticas no deben cambiarse con demasiada frecuencia (para incluir la manera y el idioma en que se expresan). Sin embargo, si es necesario, se deben aplicar los cambios apropiados, ya que siempre deben reflejar los requisitos de seguridad actuales y las estrategias de seguridad de la información.
- Las políticas deben expresarse de tal manera 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 podría ser si la Administración está realmente comprometida con la política o si la política realmente refleja la estrategia de la compañía para la protección de la información.
- Las políticas deben expresarse de tal manera que no haya lugar para malinterpretaciones. Además, las políticas deben ser respaldadas por pautas, procesos, procedimientos, roles con responsabilidades e interpretaciones para que quede claro qué hacer en casos específicos. También debe quedar claro a quién acudir en caso de que se necesite una interpretación o una decisión. También es una buena práctica mantener artículos de base de conocimiento.
- Asegúrese de que las soluciones y tecnologías apropiadas estén disponibles para respaldar las expectativas de las políticas. Por ejemplo: cuando una política requiere la autenticación de dos factores en circunstancias específicas, entonces es importante que el entorno de TI existente permita la implementación de este nivel adicional de protección.
- Introducir un tablero que permita rastrear el nivel de implementación de las políticas, lo que permite una gestión de riesgos confiable, así como la priorización de esfuerzos.

Las pautas con ejemplos de políticas, consideradas especialmente válidas desde la perspectiva de una concesionaria, son las siguientes.

7.1.1 Política de Uso Aceptable

Describe el uso aceptable de los recursos físicos y digitales de una empresa. Cubre también la propiedad y el control. Enfatiza 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 dimensiones físicas como lógicas.

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

Lógico. Es importante que una empresa desarrolle estándares que regulen la recopilación, retención y uso de datos apropiados. Estas normas deben considerar qué información se recopila, cuánto tiempo se guarda, cómo se almacena, quién puede acceder a ella y cómo se logra el acceso. Esto está muy relacionado con el papel cada vez mayor de la regulación de la privacidad en diferentes países.

Además, se debe desarrollar una política de clasificación de información con propiedad clara de la información y requisitos de protección a diferentes niveles. Esto es tan importante, que a veces se considera en una política aparte.

7.1.3 Política de Aplicaciones Comerciales

Introducir una política de clasificación de aplicaciones comerciales. Describa los requisitos de protección a nivel de la aplicación, para diferentes niveles de criticidad (por ejemplo: ubicación de zonas de seguridad, métodos de conectividad, control de identidad y acceso, aplicación de defensa en profundidad, falla segura, privilegio mínimo y principios similares). Incluya las expectativas con respecto a la arquitectura de la aplicación, la comunicación con otros sistemas y la separación de datos entre clientes. Defina las expectativas hacia soluciones basadas en la nube (que se están volviendo cada vez más populares).

Otros aspectos a especificar son la forma en que la empresa adquiere una aplicación, cuáles son los pasos obligatorios, cuáles son los requisitos comunes para los proveedores tanto funcionales como no funcionales (por ejemplo: SLA, seguridad, gestión de identidad, integraciones). Defina auditorías esperadas sobre la aplicación adquirida (por ejemplo: informes de Pentest o escaneo de vulnerabilidad). Provea políticas con plantillas y pautas para compartir con los proveedores.

7.1.4 Política de Comunicación Electrónica

En la era tecnológica actual, las empresas tienen muchas opciones para la comunicación y el intercambio de información. Sin embargo, los riesgos están asociados con estas opciones. Por ejemplo: uno puede usar un servicio en la nube para comunicarse, pero éste también puede estar recompilando 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 Gestión de Identidad y Políticas de Acceso

Es una de las áreas más críticas. Se pueden encontrar más detalles en la sección correspondiente de esta guía. La política de contraseña debe incluirse en esta sección.

7.1.6 Política de Gestión de Incidentes de Seguridad

No existe un entorno de TI que pueda asegurarse en un 100%. Una empresa necesita estar lista para cuando haya un incidente de seguridad. La Política de Gestión de Incidentes de Seguridad debe ser parte de, o contribuir a, la gestión general de incidentes. Proporcione la definición de un incidente de seguridad, introduzca procesos y procedimientos (es decir, plan de respuesta) para saber qué hacer en caso de un incidente de seguridad (dependiendo de la categoría del incidente; por ejemplo: piratería, comportamiento incorrecto, falla del equipo) y la importancia crítica. Definir los procedimientos exactos de respuesta y acción. Por ejemplo:

- Si una computadora se ve comprometida, desconéctela inmediatamente de la red.
- Si alguien ingresa sin una tarjeta de acceso, pregunte sobre su identidad.
- Considere más investigación forense.
- Considere soluciones de emergencia para respaldar los planes de servicio y continuidad del negocio.
- Considere a quién notificar en caso de un incidente, tanto dentro como fuera de la organización. Es posible que sea necesario informar a las siguientes partes: consumidores, agentes de la ley, clientes y oficinas de crédito y otras empresas que puedan verse afectadas por el incumplimiento.
- Muy a menudo también hay leyes y reglamentos que requieren un comportamiento específico en caso de que se produzca una violación de datos y dependerá del país, el estado y la industria.

La política también podría esperar introducir soluciones técnicas apropiadas para apoyar la implementación de dicha política.

Se puede encontrar información más específica sobre la respuesta ante incidentes en: https://www.sans.org/reading-room/whitepapers/incident.

Puede encontrar ejemplos de formularios de manejo de incidentes y documentación en: https://www.sans.org/score/incident-forms.

7.1.7 Política de Redes

La política de redes es otro aspecto muy importante de la seguridad general. En el desarrollo de una política de redes, se recomienda considerar los siguientes aspectos:

- Definir las tipos de zona de red con una organización de soporte (propietario de la zona, operador de la zona, etc.), asigne un nivel de confianza a cada tipo, defina conexiones permitidas entre diferentes niveles de confianza. Introduzca segmentos de red más restringidos para aplicaciones y datos más sensibles.
- Una lista de los dispositivos de red y configuraciones asociadas, así como a qué debe permitírsele la conexión 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 y el alcance de soporte
- Cortafuegos, 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 estándares inalámbricos sobre autenticación y protección en tránsito. Segmentos separados, específicos y muy limitados para clientes.
- mantenimiento remoto
- VoIP, telefonía y conferencias.

7.1.8 Política de Gestión de Riesgos y Auditoría

Defina el marco de riesgo y las consideraciones de auditoría de apoyo. Describa 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

Defina los requisitos sobre protección contra malware, registro de eventos de seguridad y solución SIEM adecuada, detección de intrusos y escaneo de vulnerabilidades. Establezca el nivel esperado adecuado en los horarios de escaneo, así como en otros sistemas de soporte; todo debería estar conectado a la gestión de riesgos.

Además de los ejemplos enumerados anteriormente, existen otras políticas de seguridad y procedimientos que una empresa debería considerar implementar para salvaguardar los datos. Puede encontrar más información sobre dichas políticas en este documento. Además, el Instituto SANS es un gran recurso para desarrollar e implementar dichas políticas.

Para obtener una variedad de ejemplos de plantillas de políticas de seguridad, visite: https://www.sans.org/securityresources/policies.

Aquí también hay un gran artículo sobre la introducción de políticas de seguridad en una empresa: https://www.csoonline.com/article/2124114/it-strategy/strategic-planning-erm-how-to-write-an-information-security-policy.html.

7.2 Guía de Gestión de Identidad y Acceso

Cubra la gestión de identidad y acceso de manera integral. Comience con la introducción y conceptos básicos seguidos de las siguientes subsecciones: gestión de identidad, autenticación, autorizaciones y por qué son tan importantes, procedimiento de gestión de acceso, usuarios finales y consideraciones físicas y niveles de protección. Cierre con una introducción a los tres niveles de madurez.

7.2.1 Introducción

Gartner, Inc. define la Gestión de Identidad y Acceso (IAM) como una disciplina de seguridad que permite:

- Acceso a las personas adecuadas
- a los recursos correctos en
- los tiempos correctos por
- los motivos correctos.

Aunque la definición es bastante simple, captura la esencia e implica muchas consideraciones en diferentes áreas.

7.2.2 Conceptos y Definiciones Básicos

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

- **Entidad**: una 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 identifica la identidad (por ejemplo: SSN, correo electrónico, huella digital)
- **Autenticación**: un procedimiento para confirmar la identidad reclamada por una entidad (por ejemplo: al proporcionar una contraseña)
- **Autorizaciones**: conjunto de permisos asignados a alguien o algo (por ejemplo: "usted está autorizado para ver los registros médicos del paciente XYZ")
- **Contabilidad/Auditoría**: historial de lo que sucedió.

Lo anterior debe considerarse tanto en dimensiones físicas como lógicas, donde lo físico se refiere a limitar el acceso a edificios, habitaciones y otros activos físicos de TI, y lo lógico se refiere a limitar el acceso al mundo virtual de las computadoras, como las conexiones a redes de computadoras, sistemas de información, archivos o datos. Una vez que se implemente lo anterior, presente el elemento clave en este rompecabezas.

- **Control de acceso:** es para asegurarse de que se ejecutan las reglas de autorización. Uno puede pensarlo como la implementación de autenticación, autorización y contabilidad (AAA) en dimensiones físicas y lógicas.

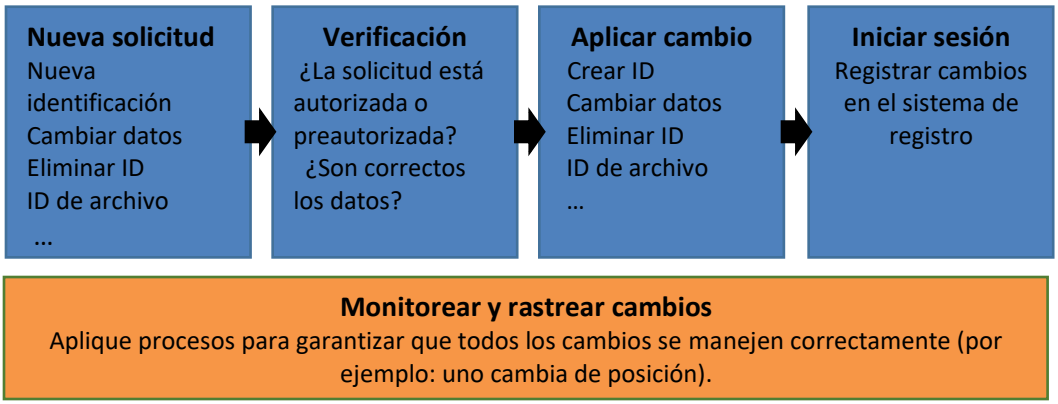
7.2.3 Gestión de Identidad

Los siguientes aspectos de la gestión de identidad deben considerarse cuidadosamente:

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

Ciclo de vida de las identidades

El ciclo de vida debe considerarse desde el momento en que comienza una relación hasta el momento en que finaliza y se supervisa a lo largo del tiempo en busca de cambios de contexto (por ejemplo: el empleado está cambiando de tarea). El procedimiento puede ilustrarse de la siguiente manera:



- Limite el número de identidades relacionadas con una entidad específica y centralice la administración de ellas (por ejemplo: trate de evitar situaciones en las que haya cuentas específicas de la aplicación).
- Intente evitar las cuentas grupales. En caso de que sea realmente necesario, nuevamente, asegúrese de que cada uno tenga su propio custodio responsable de ello.
- Recuerde que las identidades están relacionadas no solo con los usuarios finales, sino también con los servicios o las redes, y este tipo de identidades también debe gestionarse y mantenerse con cuidado. Asegúrese de que cada identidad no personal tenga su propio custodio responsable de ello.
- Asegúrese de que el almacenamiento de las identidades esté protegido, especialmente cuando se almacene información confidencial. Por lo general, las contraseñas se conocen como un ejemplo, pero también pueden referirse a información confidencial del usuario (por ejemplo: coordenadas GPS de las ubicaciones visitadas).

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

Gestión de contraseñas

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

- **Desde el lado del servidor-** donde se gestiona la identidad (por ejemplo: Directorio Activo, aplicación comercial, etc.).
    - Aspectos Clave
        - La contraseña no debe almacenarse en un texto sin formato y - en caso de que esté cifrada de forma reversible - la clave para descifrarla debe protegerse de manera correcta.
        - Todas las contraseñas predeterminadas proporcionadas por el proveedor deben cambiarse antes de poner en funcionamiento cualquier sistema de información.
- **Desde el lado del cliente-** donde se utiliza una contraseña para acceder a los recursos. Si es necesario almacenar una contraseña, se recomienda almacenarla en forma cifrada (por ejemplo: en una aplicación KeyPass, un archivo cifrado de Excel). Entonces, es importante proteger la contraseña maestra de manera segura. Es muy importante desalentar a los empleados de ...

- escribir contraseñas y mantenerlas en un lugar visible para otros (por ejemplo: en una nota adhesiva cerca del lugar de trabajo)
- divulgar contraseñas a cualquier persona a menos que sea absolutamente necesario (por ejemplo: asistencia técnica); y luego recordar cambiar la contraseña después de divulgarla)

Todas las contraseñas deben cambiarse de inmediato si se sospecha/se sabe o se divulga a los proveedores para mantenimiento/soporte.

También es importante asegurarse de que todas las copias de seguridad donde se almacenen las contraseñas también estén protegidas cuidadosamente.

Procedimientos comunes que deben diseñarse de manera segura:

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

Federación de Identidad e Inicio de Sesión Único
En caso de que se establezca una empresa con otros socios a nivel de sistemas de TI, vale la pena echar un vistazo a la política de la Federación de Identidad. En resumen, se trata de compartir la misma identidad entre empresas, basada en cierto nivel de confianza. Hay un conjunto de tecnologías maduras que respaldan el enfoque. Estos son los beneficios inmediatos:

- Inicio de sesión único: el usuario final debe autenticarse una vez y obtener acceso a una serie de aplicaciones (sin necesidad de volver a autenticarse)
- Menor costo relacionado con la gestión del ciclo de vida de la identidad.
- Menor riesgo relacionado a la necesidad de mantener identidades separadas por un usuario final

Al final, se debe realizar un cálculo para determinar si vale la pena invertir en Identity Federation en un contexto específico.

7.2.4 Autenticación

La prueba más común en autenticación es la contraseña, pero también hay un problema: las contraseñas son difíciles de recordar. Por lo tanto, se ha vuelto cada vez más popular usar frases de contraseña en su lugar. Hay que recordar que recomendar frases de contraseña requiere cambios en las políticas y en los sistemas de TI para que admitan las nuevas políticas.

Hay otras opciones para la autenticación aparte de la contraseña, como la biometría, contraseñas de un solo uso o tarjetas inteligentes compatibles con tokens RSA, aplicaciones móviles como Google Authenticator o Yubikey. Cada método generalmente se clasifica en una de tres categorías:

- Algo que se sepa (contraseñas, patrones visuales)
- Algo que se tenga (tarjeta inteligente, token RSA, teléfono inteligente)
- Algo que eres (biometría, comportamiento)

Hay 2 razones para aplicar diferentes métodos de Autenticación:

- Mejor experiencia del usuario (por ejemplo: biometría)
- Mayor seguridad (tarjeta inteligente)

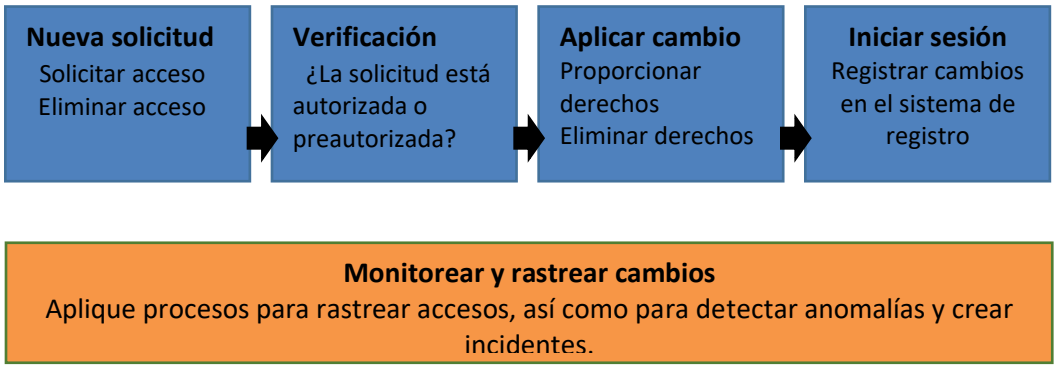
Cuando se combinan dos o más métodos de diferentes categorías, esto se define como ***Autenticación multifactor*** que consiste en aumentar el nivel de seguridad.

7.2.5 Procedimiento para la Gestión de Autorizaciones y Acceso

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

- Definir una estructura de roles y niveles de acceso.
- Definir un conjunto de permisos para un rol determinado.
- Asegúrese de que las autorizaciones estén documentadas y sean de fácil acceso.
- Asegúrese de que las autorizaciones se implementen en los sistemas de control de acceso.
- Las solicitudes de acceso son aprobadas por las personas correctas y se define claramente quiénes son los aprobadores.
- Monitoreo y revisión (auditorías) de derechos de acceso y autorizaciones

Además, el ***Procedimiento de Gestión de Acceso*** debe establecerse e implementarse para garantizar que las autorizaciones definidas se apliquen en todos los lugares en cualquier momento. El procedimiento es similar al procedimiento de gestión del ciclo de vida de la identidad y se puede ilustrar de la siguiente manera:



Los elementos clave de dicho procedimiento que deben ser tenidos en cuenta:

- El acceso se revoca o modifica cada vez que un empleado abandona la empresa o cambia de puesto.
- El acceso debe actualizarse de manera oportuna para reflejar las necesidades comerciales.
- El acceso debe revisarse periódicamente en una cadencia documentada (trimestral, semestral, anual). Esta evaluación, no motivada por la salida o transición del empleado, es para determinar si el nivel de acceso actualmente otorgado corresponde con la posición de la persona en el negocio. Tenga en cuenta que la frecuencia de las revisiones puede variar según la importancia de los activos que están siendo protegidos.
- Una buena práctica es también aplicar el principio de "necesidad de saber", es decir, el acceso a los recursos debe darse solo si hay una necesidad comercial.

Una vez más, la importancia de monitorear y auditar las autorizaciones y los derechos de acceso, especialmente para asegurarse de que la eliminación del acceso se implemente correctamente, no puede exagerarse. Desafortunadamente, es muy común que se otorguen derechos de acceso y luego nunca se eliminen.

7.2.6 Usuarios Finales y Consideraciones Físicas

Es de conocimiento común que la mayoría de los problemas de seguridad a menudo son causados por un comportamiento incorrecto del usuario. (Las relacionadas con las dimensiones lógicas -como hacer clic en correos electrónicos peligrosos- están cubiertas en otras secciones). Los elementos relacionados con el control de acceso físico siguen y también deberían ser la base para una estrategia educativa adecuada.

- Las salas de servidores/equipos deben estar cerradas. El acceso de los empleados debe limitarse solo a aquellos que tienen una necesidad comercial legítima. Deben existir mecanismos para saber si alguien accede al sitio y cuándo lo hace.
- Requerir que los archivos que contengan datos e información confidencial se guarden en archivadores cerrados en todo momento, excepto cuando un empleado esté trabajando en el archivo. Además, cuando un empleado esté trabajando en el archivo, asegurarse de que personas no autorizadas no puedan ver el archivo (por ejemplo: cuando vuelan en el avión).
- Recuerde a los empleados que no dejen documentos/información confidencial en escritorios cuando estén lejos de las estaciones de trabajo.
- Exigir a los empleados que guarden los archivos, cierren las computadoras y cierren los gabinetes y las puertas de las oficinas al final del día.
- Implemente controles de acceso adecuados para su edificio. Indique a los empleados qué hacer y a quién notificar si se ve a una persona desconocida en las instalaciones.
- Si se mantienen instalaciones de almacenamiento fuera del sitio, limite el acceso de los empleados a aquellos con una necesidad comercial legítima. Deben existir mecanismos para saber si alguien accede al sitio y cuándo.
- Si se utilizan dispositivos que recompilan información confidencial, como almohadillas de PIN, asegure el equipo para reducir el riesgo de manipulación. Dicho equipo también debe asegurarse para reducir el riesgo de que un atacante cambie de equipo con un dispositivo ficticio.

7.2.7 Niveles de Protección

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

- **Aplicaciones comerciales:** aplicaciones necesarias para administrar pedidos, programar trabajos, organizar recursos humanos y finanzas, etc. El enfoque está en la protección de la información y las funcionalidades comerciales sensibles. Las identidades generalmente se relacionan con los usuarios finales.
- **Sistemas Operativos:** base para ejecutar aplicaciones en computadoras portátiles, computadoras de escritorio, servidores, teléfonos, tabletas, etc. El enfoque está en la protección de archivos y datos, contra malware y lo que el control de acceso puede soportar. Las identidades generalmente se relacionan con usuarios finales (computadoras portátiles, teléfonos, etc.) y servicios (servidores).

- **Dispositivos de infraestructura y servicios de soporte:** enrutadores, conmutadores, puntos de acceso, servicios de autenticación, etc. La atención se centra en la protección de un tráfico de red correcto, manteniendo la comunicación segura y alejando a los intrusos. Las identidades generalmente se relacionan con usuarios y servicios técnicos.

- **Dispositivos móviles:** dispositivos como teléfonos, tabletas e incluso computadoras portátiles. El foco está en la protección de los datos almacenados en los dispositivos y en asegurarse de que sea accesible de forma segura para incluir escenarios como el uso fuera de línea o el robo del dispositivo.

- **Instalaciones/físico:** edificios, salas de servidores, salas de impresión, oficinas, talleres, salas de exposición, etc. El objetivo es asegurarse de que las personas puedan ingresar a los lugares correctos y tener acceso a los activos correctos.

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

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

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

- Implemente una protección integral en todas las capas y para todo tipo de aplicaciones y dispositivos, tanto en dimensiones físicas como lógicas.

7.3 Orientación sobre el Nivel de Madurez en la Seguridad de la Concesionaria

Las concesionarias a menudo tienen dificultades para implementar recomendaciones de seguridad. Esto a menudo se atribuye al nivel de madurez de la concesionaria en términos de TI y sofisticación de seguridad. Utilice esta guía para ayudar a identificar el nivel de madurez de su concesionaria y los siguientes pasos a seguir para ayudarlo a mejorar su postura en cuanto a la seguridad.

7.3.1 Orientación al Vendedor Sobre Políticas de Seguridad

Al determinar los próximos pasos para madurar las políticas de seguridad de una concesionaria, primero identifique el nivel de madurez actual de la concesionaria. Luego, determine las acciones que se pueden llevar a cabo para avanzar en la postura de seguridad de la concesionaria. Use la guía a continuación para ayudarse.

- **Nivel de madurez básico:** las concesionarias han identificado y documentado políticas sobre el uso aceptable, la auditoría, la gestión de acceso (incluida la contraseña) y la consideración básica de la red (incluido el acceso externo y los estándares inalámbricos).
- **Nivel de madurez intermedio:** las concesionarias han identificado y documentado políticas para todas las áreas esperadas. Además, cuentan con procesos para entregar, educar y apoyar al personal de la concesionaria con políticas de seguridad documentadas.
- **Nivel de madurez avanzado:** las concesionarias regularmente prueban, auditan y refinan las políticas de seguridad y los procedimientos.

7.3.2 Orientación al Vendedor sobre la Gestión de Identidad y Acceso (IAM)

Al determinar los próximos pasos para madurar el IAM de una concesionaria, primero identifique el nivel de madurez actual de la concesionaria. Luego, determine las acciones que se pueden tomar para avanzar en la postura de seguridad de la concesionaria. Utilice la guía a continuación para ayudarse.

Nivel básico de madurez

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

Nivel de madurez intermedio

- Procesos explícitos para gestionar el ciclo de vida de las identidades y los derechos de acceso.
- Auditorías periódicas y revisiones de permisos para sistemas críticos.
- Procesos explícitos para la gestión de contraseñas y recomendaciones sobre el almacenamiento de contraseñas por parte del cliente
- Educación regular de los empleados.
- Sistema de control de acceso para todas las instalaciones físicas.
- Nivel de protección (por ejemplo: autenticación multifactor, defensa en profundidad) relacionada con la importancia de la información y las funciones comerciales

Nivel de madurez avanzado

- Procesos automatizados para gestionar el ciclo de vida de las identidades y los derechos de acceso.
- Almacenamiento y gestión de identidades centralizadas, incluida la federación del nivel correcto de identidades
- Procesos centralizados para la gestión de contraseñas y Autenticación.
- Recomendaciones (o políticas) sólidas sobre el almacenamiento de contraseñas por parte del cliente
- Nivel de protección (por ejemplo: autenticación multifactor, defensa en profundidad) relacionada con la importancia de la información y las funciones comerciales
- Sistema de control de acceso centralizado para todas las instalaciones físicas.
- Educación regular 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 dimensiones físicas como lógicas

7.3.3 Orientación al Vendedor sobre la Gestión de Parches

Nivel de madurez básico: las concesionarias tienen cada sistema configurado para actualizarse automáticamente para parches críticos o de seguridad.

Nivel de madurez intermedio: las concesionarias cuentan con un sistema de gestión de parches para toda la empresa.

Nivel de madurez avanzado: las concesionarias prueban, implementan y validan parches a medida que están disponibles lo antes posible.

7.3.4 Orientación a la Concesionaria sobre Recuperación de Desastres

Al determinar los próximos pasos para madurar la recuperación ante desastres de una concesionaria/continuidad comercial, primero identifique el nivel de madurez actual de la concesionaria. Luego, determine las acciones que se pueden tomar para avanzar en la postura de seguridad de la concesionaria. Use la guía a continuación para ayudarse.

- **Nivel de Madurez Básico**: las concesionarias regularmente respaldan todos los sistemas.
- **Nivel de Madurez Intermedio**: las concesionarias realizan copias de seguridad incrementales regulares y almacenan imágenes de copias de seguridad fuera del sitio.
- **Nivel de Madurez Avanzado**: las concesionarias implementan un sistema de continuidad del negocio para incluir copias de seguridad completas del sistema fuera del sitio en un entorno virtual que permitirá a la concesionaria recobrar la imagen de la copia de seguridad inmediatamente en caso de una interrupción o falla.

7.3.5 Orientación al Vendedor sobre la Capacitación sobre Seguridad

Al determinar los próximos pasos para madurar el programa de concientización de seguridad de una concesionaria, primero identifique el nivel de madurez actual de la concesionaria. Luego, determine las acciones que se pueden tomar para avanzar en la postura de seguridad de la concesionaria. Use la guía a continuación para ayudarse.

- **Nivel de Madurez Básico**: todos los empleados reciben capacitación anual en seguridad. La finalización de la capacitación está documentada y los informes están disponibles para su auditoría. Los empleados pueden no estar seguros de su papel en la protección de la organización. La organización puede ser compatible, pero no segura. No existe un procedimiento establecido para y/o los empleados no se sienten facultados para reportar comportamientos sospechosos o pérdida accidental de datos.
- **Nivel de Madurez Intermedio**: el programa de capacitación puede ser más frecuente que el anual y se realiza un seguimiento para garantizar que todos los empleados participen como condición de empleo. Los temas cubiertos se centran en los mayores riesgos para la organización. Los materiales de concientización se publican en las áreas de descanso de los empleados. Los empleados conocen las políticas de seguridad de la compañía y saben cómo reconocer e informar un incidente de seguridad.
- **Nivel de Madurez Avanzado**: el programa de capacitación para todos los empleados y contratistas incluye módulos cortos pero frecuentes sobre temas oportunos relevantes para su función. A los empleados se les evalúa su capacidad de defenderse contra diversas tácticas de ingeniería social como phishing, caídas de USB, fraude, etc. Los empleados saben cómo informar un incidente de seguridad y, cuando se realizan las pruebas, al menos el 50% de los empleados informan sobre algo sospechoso. Cuando se prueba, menos del 10% hace clic en correos electrónicos de prueba de phishing. La concesionaria tiene una cultura de seguridad: los empleados comprenden su papel en la protección de la organización, buscan procesos seguros y alientan a sus compañeros de trabajo a realizar negocios de una manera que valore la seguridad y proteja a la organización del fraude, el robo y los datos accidentales o pérdidas financieras.

7.3.6 Orientación al Vendedor sobre el Cumplimiento de las Leyes Federales

Al determinar los próximos pasos para madurar el cumplimiento de una concesionaria con las legislaciones de seguridad, primero identifique el nivel de madurez actual de la concesionaria. Luego, determine las acciones que se pueden tomar para avanzar en la postura de seguridad de la concesionaria. Use la guía a continuación para ayudarse.

- **Nivel de Madurez Básico**: las concesionarias han investigado el PCI y GLBA para determinar el cumplimiento de la legislación federal. Los distribuidores han documentado políticas y procesos para cumplir con el cumplimiento.
- **Nivel de Madurez Intermedio**: las concesionarias revisan periódicamente el cumplimiento de la legislación de seguridad federal
- **Nivel de Madurez Avanzado**: los distribuidores realizan auditorías periódicas de los sistemas y rastrean los resultados hasta los requisitos de la legislación.

7.3.7 Orientación al Vendedor sobre la Seguridad de la Red

Al determinar los próximos pasos para madurar la seguridad de la red de una concesionaria, primero identifique el nivel de madurez actual de la concesionaria. Luego, determine las acciones que se pueden tomar para avanzar en la postura de seguridad de la concesionaria. Use la guía a continuación para ayudarse.

- **Nivel de Madurez Básico**: las concesionarias han desarrollado y documentado una política de uso de Internet. Las concesionarias tienen protección en la puerta de enlace de red y han configurado y segmentado la red para evitar el acceso no deseado a los recursos de la red. La red es monitoreada por tecnologías de gestión de eventos de información de seguridad en tiempo real para proteger contra el acceso no deseado a la red. El acceso remoto es monitoreado y restringido en la red.
- **Nivel de Madurez Intermedio**: las concesionarias han utilizado políticas y procesos documentados para establecer una red de concesionarias segura y segmentada. Las concesionarias regularmente prueban la red contra riesgos conocidos. La red es monitoreada 24x7x365 por expertos en seguridad utilizando tecnologías de gestión de eventos de información de seguridad. Acceso remoto monitoreado y restringido a vendedores y empleados conocidos.
- **Nivel de Madurez Avanzado**: las concesionarias han utilizado políticas y procesos documentados para establecer una red de concesionarias segura y segmentada. Las concesionarias regularmente prueban la red contra riesgos conocidos. La red es monitoreada 24x7x365 por un proveedor de servicios certificado SOC 2. La red es monitoreada 24x7x365 por expertos en seguridad. Acceso remoto monitoreado y restringido a vendedores y empleados conocidos. El acceso VPN de los empleados se logra mediante autenticación de dos factores.

7.3.8 Orientación sobre el AntiVirus de la Concesionaria

Al determinar los próximos pasos para madurar la seguridad del AV de una concesionaria, primero identifique el nivel de madurez actual de la concesionaria. Luego, determine las acciones que se pueden tomar para avanzar en la postura de seguridad de la concesionaria. Use la guía a continuación para ayudarse.

- **Nivel de Madurez Básico**: las concesionarias han identificado todos los sistemas y el software antivirus ha sido aplicado en cada sistema de la red.
- **Nivel de Madurez Intermedio**: las concesionarias cuentan con un sistema antivirus corporativo. Esto incluye la gestión de licencias en toda la empresa, un portal empresarial para informes y respuestas, y auditorías e informes en toda la red.
- **Nivel de Madurez Avanzado**: los distribuidores realizan una respuesta proactiva e inmediata a las alertas generadas por la solución AV corporativa.

7.3.9 Orientación al Vendedor sobre la Seguridad del Correo Electrónico

Al determinar los próximos pasos para madurar la seguridad del correo electrónico de una concesionaria, primero identifique el nivel de madurez actual de la concesionaria. Luego, determine las acciones que se pueden tomar para avanzar en la postura de seguridad de la concesionaria. Use la guía a continuación para ayudarse.

- **Nivel de Madurez Básico**: las concesionarias han tomado medidas para implementar tecnologías para proteger los sistemas de correo electrónico de la concesionaria.
- **Nivel de Madurez Intermedio**: los vendedores realizan una inspección y protección activa de seguridad en correos electrónicos entrantes y salientes. Los vendedores encriptan datos confidenciales por correo electrónico.
- **Nivel de Madurez Avanzado**: las concesionarias llevan un monitoreo del correo electrónico y respuesta activa ante amenazas de correo electrónico.

7.3.10 Orientación con UTM/Cortafuegos/IDS

Al determinar los próximos pasos para madurar el sistema unificado de gestión de amenazas, cortafuegos y detección de intrusos de una concesionaria, primero identifique el nivel de madurez actual de la concesionaria. Luego, determine las acciones que se pueden tomar para avanzar en la postura de seguridad de la concesionaria. Use la guía a continuación para ayudarse.

- **Nivel de Madurez Básico**: las concesionarias implementan un UTM totalmente administrado 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 concesionarias responden a alertas y eventos del UTM 24x7x365 en tiempo real. Las concesionarias utilizan un SIEM (consulte la sección 3.5) para alertar y responder a eventos en la puerta de enlace de la red.
- **Nivel de Madurez Avanzado**: las concesionarias recurren a un proveedor de servicios de seguridad gestionados (MSSP) para una gestión, supervisión y respuesta proactiva de UTM, 24x7x365.

7.3.11 Orientación con SIEM

Al determinar los próximos pasos para madurar la gestión de eventos de información de seguridad de una concesionaria, primero identifique el nivel de madurez actual de la concesionaria. Luego, determine las acciones que se pueden tomar para avanzar en la postura de seguridad de la concesionaria. Use la guía a continuación para ayudarse.

- **Nivel de Madurez Básico**: las concesionarias instalan y utilizan el software SIEM. Todas las alertas se responden casi en tiempo real 24x7x365. Todos los registros del sistema se almacenan de acuerdo con la legislación federal (consulte la sección 2.6 sobre cumplimiento de las leyes federales).
- **Nivel de Madurez Intermedio**: las concesionarias utilizan un proveedor de servicios de seguridad gestionados para una supervisión y respuesta avanzadas. Inteligencia de amenazas integrado a las concesionarias para un monitoreo avanzado, con alertas.
- **Nivel de Madurez Avanzado**: las concesionarias recurren a un proveedor de servicios de seguridad gestionados (MSSP) certificado SOC 2 para una gestión, supervisión y respuesta proactiva de UTM, 24x7x365. Las concesionarias integran inteligencia de amenazas en la solución SIEM. Los tickets, las alertas y la actividad son revisados regularmente por la gerencia de la concesionaria y el MSSP para mejorar la postura en cuestiones de seguridad, documentación y mejoras.

7.3.12 Orientación al Vendedor sobre la Seguridad de la Aplicación

Al determinar los próximos pasos para madurar la seguridad de la aplicación de una concesionaria, primero identifique el nivel de madurez actual de la concesionaria. Luego, determine las acciones que se pueden tomar para avanzar en la postura de seguridad de la concesionaria. Use la guía a continuación para ayudarse.

Nivel de Madurez Básico

- Presenta un catálogo de aplicaciones.
- Mantiene una gestión básica de identidad y acceso.
- Aplica actualizaciones y parches de aplicaciones de forma regular.

Nivel de madurez intermedio

- Mantiene el catálogo de aplicaciones comprendiendo el análisis de impacto empresarial y la clasificación de la información.
- Implementa una estrategia madura de gestión de identidad y acceso.
- Protege los flujos de información de un extremo al otro, tanto en tránsito como en almacenamiento.
- Presenta procesos para gestionar incidentes y solicitudes de acceso.

- Aplica la estrategia de defensa en profundidad.

Nivel de madurez avanzado

- Aplica todos los elementos de la sección anterior.

7.3.13 Orientación al Vendedor sobre la Movilidad

Al determinar los próximos pasos para madurar la seguridad de una concesionaria en cuanto a movilidad, primero identifique el nivel de madurez actual de la concesionaria. Luego, determine las acciones que se pueden tomar para avanzar en la postura de seguridad de la concesionaria. Use la guía a continuación para ayudarse.

Nivel de Madurez Básico

- Mantiene actualizado el software antimalware.
- Define qué información puede procesarse y almacenarse en los dispositivos móviles; incluye consideraciones relacionadas con dispositivos administrados y no administrados.
- El acceso a los dispositivos está restringido, lo que requiere la autenticación del usuario. La mayoría de los dispositivos se pueden bloquear con un bloqueo de pantalla, contraseña o PIN.
- Actualiza el sistema operativo móvil con parches de seguridad. Puede encontrar más información sobre Gestión de Parches en la sección 2.6.3.

Nivel de madurez intermedio

- Todos los artículos del nivel de madurez básico.
- Aplica el cifrado adecuado de datos tanto en computadoras portátiles como en dispositivos móviles con especial cuidado en la administración 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 y se puede ejecutar un ataque por parte de un intermediario.
- Cree políticas y procedimientos sobre quién, cuándo y cómo accederá de forma remota al entorno de la empresa (red, servidores, aplicaciones, etc.) y a qué partes del mismo. Implemente la solución técnica adecuada para respaldar el enfoque establecido.
- Realice regularmente una copia de seguridad del dispositivo móvil.

Nivel de madurez avanzado

- Aplicar todos los elementos de las secciones anteriores.

7.4 Glosario

802.11: 802.11 es un grupo de de especificaciones inalámbricas desarrolladas por el IEEE para comunicaciones inalámbricas de red de área local (WLAN). Detalla una interfaz inalámbrica entre dispositivos para administrar el tráfico de paquetes para evitar colisiones. Algunas especificaciones comunes incluyen 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: Un dispositivo para transmitir y recibir señales de radiofrecuencia (RF). A menudo camuflado en edificios existentes, árboles, torres de agua u otras estructuras altas, el tamaño y la forma de las antenas generalmente están determinadas por la frecuencia de la señal que manejan.

Aplicación (Aplicación): herramientas descargables, recursos, juegos, redes sociales o casi cualquier cosa que agregue una función o característica a un dispositivo inalámbrico que esté disponible de forma gratuita o de pago. Algunas aplicaciones también pueden ofrecer a los usuarios la posibilidad de comprar contenido o funciones mejoradas dentro de la aplicación. Los padres pueden limitar la capacidad de sus hijos para descargar o realizar estas compras en la aplicación protegiendo con contraseña esas funciones en un dispositivo inalámbrico. CTIA creó un sistema de calificación de aplicaciones para ayudar a informar a los padres sobre una aplicación para que puedan determinar si es apropiada para sus hijos: **http://bit.ly/JtPvve**.

Banda ancha: una instalación de transmisión que tiene un ancho de banda (capacidad) suficiente para transportar múltiples canales de voz, video o datos simultáneamente. La banda ancha generalmente se equipara con la entrega de mayores velocidades y capacidades avanzadas, incluido el acceso a Internet y servicios relacionados

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

Cat5e: La especificación de categoría 5e mejora a las especificaciones de categoría 5 al mejorar algunas especificaciones de interferencia e introducir nuevas especificaciones de interferencia 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: un estándar de cable para Gigabit Ethernet y otros protocolos de red que es retrocompatible con los estándares de cable de Categoría 5/5e y Categoría 3. El Cat-6 presenta especificaciones más estrictas para la interferencia y el ruido del sistema. El estándar de cable proporciona un rendimiento de hasta 250 MHz y es adecuado para 10BASE-T / 100BASE-TX y 1000BASE-T (gigabit Ethernet). Se espera que se adapte al estándar 10GBASE-T (10 gigabit Ethernet), aunque con limitaciones de longitud si no está protegido, se utiliza un cable Cat 6. La Ford Motor Company recomienda el cableado Cat6 cuando se haga un cableado nuevo o cuando se reemplazan nuevos segmentos de red cableados.

DSL (Línea de Suscriptor digital): una línea digital que conecta el terminal del suscriptor a la oficina central de la empresa que presta servicios, que proporciona múltiples canales de comunicaciones capaces de transportar comunicaciones de voz y datos simultáneamente.

Cifrado: codificación digital de información para que pueda transmitirse a través de una red no segura. En el otro extremo, el destinatario generalmente usa una "clave" digital para descifrar la información y restaurarla a su forma original.

Hand-held / Tablet PC: estos dispositivos son computadoras que pueden ser transportadas por un usuario. Por lo general, son mucho más pequeños que una computadora portátil típica y no tienen la capacidad total de una computadora de escritorio, pero aún pueden realizar las tareas más necesarias. También permitirán que un usuario realice trabajos en varias ubicaciones de una concesionaria, lo que puede aumentar la productividad.

IEEE (Instituto de Ingenieros Eléctricos y Electrónicos): una asociación profesional con sede en la ciudad de Nueva York que se dedica a promover la innovación tecnológica y la excelencia. Tiene alrededor de 425.000 miembros en aproximadamente 160 países, un poco menos de la mitad de los cuales reside en los Estados Unidos (**http://www.ieee.org**).

LAN (Red de Área local): La red de área local (LAN) es una pequeña red de datos que cubre un área limitada, como un edificio o grupo de edificios. La mayoría de las LAN conectan estaciones de trabajo o computadoras personales. Esto permite que muchos usuarios compartan dispositivos como impresoras láser, así como datos. La LAN también permite una comunicación fácil, facilitando el correo electrónico o apoyando sesiones de chat.

Malware: El Malware (por "software malicioso") es cualquier programa o archivo perjudicial para un usuario de la computadora. Por lo tanto, el malware incluye virus informáticos, gusanos y caballos de Troya y también software espía, programa que recopila información sobre un usuario de la computadora sin permiso.

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

Sistema Operativo: El componente de software de un sistema informático responsable de la gestión y coordinación de actividades y el intercambio de los recursos de la computadora. El Sistema Operativo (OS) actúa como un host para los programas de aplicación que se ejecutan en la máquina. Como host, uno de los propósitos de un Sistema Operativo es manejar los detalles de la operación del hardware. La Ford Motor Company recomienda el sistema operativo Windows 7 para obtener compatibilidad con las aplicaciones de Ford.

Gestión de Parches: El procedimiento de actualización de servidores o PC. Esto a menudo se hace para actualizar las máquinas a los últimos parches de seguridad y paquetes de servicio. Los creadores de virus, spyware y otro software malicioso aprovechan los defectos existentes en el software cargado en una PC para propagarse y causar daños. STAR recomienda que las concesionarias apliquen parches críticos, como los de seguridad, lo antes posible.

Punto de acceso inalámbrico no autorizado: un punto de entrada inalámbrico a la red de la concesionaria que no está autorizado, asegurado o no es conocido por la TI, la administración y la propiedad de la concesionaria. Cualquier red inalámbrica no autorizada debe ser detectada, encontrada y eliminada de inmediato.

Enrutadores: Permiten que las computadoras de diferentes redes y subredes se comuniquen. En las concesionarias, los enrutadores se pueden usar para conectar una LAN de OEM, LAN de concesionaria y LAN de DMS a Internet.

Ruteadore: las frecuencias de radio designadas para un uso específico, como servicios de comunicaciones personales y seguridad pública.

Spyware: cualquier tecnología que ayude a recopilar información sobre una persona u organización sin su conocimiento. En Internet (donde a veces se le llama spybot o software de seguimiento), el spyware es un programa que se coloca en la computadora de alguien para recopilar información secretamente sobre el usuario y transmitirla a los anunciantes u otras partes interesadas. Los distribuidores deben implementar sistemas para detectar y eliminar spyware para proteger los datos del cliente y la integridad de seguridad de la red.

SSID (identificación de conjunto de servicios): en redes de computadoras, un SSID es un conjunto que consta de todos los dispositivos asociados con una red de área local inalámbrica IEEE 802.11x. Los SSID deben estar asociados con una VLAN específica.

TCP/IP (Protocolo de control de transmisión / Protocolo de Internet): un protocolo que permite comunicaciones a través y entre redes; El protocolo TCP/IP es la base de las comunicaciones de Internet.

Troyano (caballo de Troya): un troyano es un programa en el que el código malicioso o dañino está contenido dentro de un programa o datos aparentemente inofensivos de tal manera que puede obtener el control y causar la forma de daño elegida, como arruinar cierta área de su disco duro.

VPN (redes privadas virtuales): una VPN permite a un usuario realizar transacciones seguras a través de una red pública o no segura. Al encriptar 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 de computadoras, una sola red de capa 2 (basada en conmutadores) puede dividirse para crear múltiples dominios de difusión distintos, que están aislados entre sí para que los paquetes solo puedan pasar entre ellos a través de uno o más enrutadores; dicho dominio se denomina red de área local virtual, LAN virtual o VLAN. Esto generalmente se consigue en dispositivos conmutadores o enrutadores.

VoIP (Voz sobre Protocolo de Internet): El VoIP no solo es capaz de entregar voz sobre IP, sino que también está diseñado para acomodar videoconferencias bidireccionales y compartir aplicaciones. Basado en la tecnología IP, VoIP se utiliza para transferir una amplia gama de tráfico de diferentes tipos.

WAN (Red de Área Amplia): un término general que se refiere a una gran red que abarca un país o alrededor del mundo. Internet es una WAN. Un sistema público de comunicaciones móviles, como una red celular o PCs, es una WAN. Las concesionarias pueden conectar en red ubicaciones y edificios remotos a través de la tecnología WAN. En la mayoría de los términos de la concesionaria, WAN se refiere al proveedor de servicios de Internet de la concesionaria.

Gusano: un gusano es un virus autorreplicante que no altera los archivos sino que se duplica a sí mismo. Es común que los gusanos se noten solo cuando su replicación incontrolada consume recursos del sistema, ralentiza o detiene otras tareas.

Wi-Fi: el Wi-Fi proporciona conectividad inalámbrica sobre espectro sin licencia (utilizando los estándares IEEE 802.11a o 802.11b), generalmente en las bandas de radio de 2.4 y 5 GHz. El Wi-Fi ofrece conectividad de área local a computadoras habilitadas para Wi-Fi.

WPA (Acceso Protegido a Wi-Fi): protocolos de seguridad y programas de certificación de seguridad desarrollados por Wi-Fi Alliance para proteger las redes inalámbricas de computadoras. La Wi-Fi Alliance lo concibió como una medida intermedia en previsión de la disponibilidad del WPA2, más seguro y complejo. WPA no es seguro y no debe ser utilizado por distribuidores.

WPA-2 (Acceso Protegido Wi-Fi II): El WPA2 ha reemplazado a WPA. WPA2, que requiere pruebas y certificación de la Wi-Fi Alliance, implementa los elementos obligatorios del IEEE 802.11i.

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