Marco de control de seguridad del concesionario John Deere· Información de control requerida

Número de	Control De	Control	Descripción del control	Pruebas/documentación
1,1	Requerido	Asegurarse de que no Software y Las Firmas Actualizado	Asegurarse de que la organización el software de malware está configurado para para actualizaciones de su motor de análisis y base de datos de firmas al menos cada 24 horas.	Captura de pantalla que muestra la configuración de las actualizaciones de directiva de grupo que requiere que los dispositivos comprueben si hay definiciones al menos cada 24 horas. Una captura de pantalla de la configuración suficiente para aquellos que usan una solución de detección y respuesta de puntos finales (EDR).
1,2	Requerido	Configurar el bloqueo Análisis de malware de desmontaje Dispositivos	Configurar los dispositivos de modo que llevar a cabo automáticamente un escaneo de medios extraíbles cuando se cuando se ejecutan archivos en.	Captura de pantalla que muestra la configuración de los análisis automáticos de directiva de grupo de empresa que requiere que los dispositivos analicen medios extraíbles cuando se insertan o cuando se ejecutan archivos.
1,3	Requerido	Configurar a No Auto-Run Contenido	Configurar los dispositivos para que no de medios extraíbles.	Captura de pantalla que muestra una directiva de sistema empresarial o configuración que impide que el contenido se ejecute automáticamente en medios. Nota: Las directivas deben configurarse para desactivar la reproducción automática y la ejecución automática.
1,4	Requerido	Utilizar Centralmente Antiarranque Software de malware	Utilice un sistema antimalware gestionado de software para monitorear continuamente cada estación de trabajo y servidor.	Captura de pantalla de la gestión antimalware centralizada de su organización consola.
1,5	Requerido	Regularmente Actualice/Parche su Sistemas y Software	Instalar la versión más reciente de cualquier actualización relacionada con la dispositivos que se conectan a la red.	Una copia de la política, el proceso o los procedimientos del concesionario para los dispositivos conectados reciben todas las actualizaciones de seguridad
2,1	Requerido	Apero a Completo Seguridad anual Programa de	Crear un programa de seguridad para todos los miembros de la fuerza de trabajo base definida para garantizar que entienden y exhibir los comportamientos necesarios y habilidades para reforzar la seguridad de la organización. La formación debe incluir ataques de ingeniería social, seguros prácticas de autenticación y información gestión de datos	Una copia de la política o proceso del concesionario que rige la seguridad anual requisitos de formación, incluida la frecuencia de la formación, el contenido de la frecuencia de revisión. Este proceso puede incluir el uso de un servicio plataforma de formación.
2,2	Requerido	Bloqueo no deseado, Innecesario y Correos electrónicos y accesorios	Bloquear todos los archivos adjuntos de puerta de enlace de correo electrónico de la los tipos son innecesarios para el negocio de la organización.	Captura de pantalla de la consola de gestión de la puerta de enlace de correo herramienta similar que filtra los archivos adjuntos de correo electrónico) bloqueado o permitido. Esto también puede incluir el uso de una protección de política.

2,3	**Requerido**	**Bloquear acceso A/De Conocido Sitios web maliciosos y Países Donde No Hacer negocios**	**Usar el filtrado del Sistema de nombres de servicios para bloquear el acceso a dominios malintencionados. Exigir red- filtros de URL basados que limitan la capacidad de conectarse a sitios web no aprobado por la organización. Este filtrado para cada uno de los los sistemas de la organización, si físicamente en las instalaciones de una no. Denegar comunicaciones con direcciones IP de Internet malintencionadas o y limitar el acceso solo a intervalos de direcciones IP necesarios en los límites de la red de la organización.**	Captura de pantalla del filtrado de contenido, DNS, URL y/o IP del concesionario consola de administración que muestra dominios, sitios, categorías y/o direcciones de red.
3,1	**Requerido**	**Establecer proceso para revocar Cuentas**	**Establecer y seguir una proceso para revocar el acceso al sistema desactivar cuentas inmediatamente después cese o cambio de responsabilidades de un empleado o contratista. Desactivación estas cuentas, en lugar de eliminarlas cuentas, permite conservar la auditoría senderos.**	Una copia del proceso documentado del concesionario para revocar el acceso al desactivar cuentas asociadas con empleados o contratistas que han sido finalizado en 4 horas. El proceso debe incluir los períodos de tiempo asociado con una terminación (4 horas).
3,2	**Requerido**	**Desactivar Cualquiera No asociado Cuentas**	**Desactivar cualquier cuenta que no se pueda asociado a un proceso comercial o propietario de la empresa.**	Un registro que incluye un inventario de todas las cuentas administrativas y de e indica cuándo se produjo la revisión. Además, el registro debe incluir explicar qué cuentas fueron desactivadas y, si no, explicar por qué.
3,3	**Requerido**	**Desactivar latente Cuentas**	**Desactivar las cuentas inactivas después de período de inactividad.**	Una copia del proceso o procedimiento documentado del concesionario para las cuentas que han estado inactivas durante al menos 6 meses están
3,4	**Requerido**	**Menos apero Acceso privilegiado Controles**	**El principio de privilegio mínimo se refiere a control de seguridad de la información en el el usuario tiene los niveles mínimos de - o permisos - necesarios para realizar sus funciones de trabajo.**	Una copia de la política documentada del concesionario que rige el principio de acceso privilegiado o una captura de pantalla que demuestra la implementación de privilegio.
3,5	**Requerido**	**Apero Política de**	**Una directiva de contraseñas es un conjunto diseñado para mejorar la seguridad animar a los usuarios a emplear y usarlas correctamente. A la directiva de contraseñas suele formar parte reglamento oficial de la organización y mayo se enseñará como parte del conocimiento de formación.**	Una copia de la política de contraseñas documentada del concesionario.

3,6	**Requerido**	**Cambiar Contraseñas Hardware anterior Implementación**	**Antes de implementar cualquier hardware , asegúrese de que las contraseñas para cumplir con los requisitos de la directiva de contraseñas de la organización**	Una copia del proceso o flujo de trabajo documentado del concesionario para recursos de hardware que garantizan que las contraseñas predeterminadas se los nuevos requisitos de contraseña de la organización.
3,7	**Requerido**	**Apero múltiple Factor Autenticación (AMF)**	**Multi Factor Authentication (también MFA) es un método de confirmación de identidades reclamadas mediante una de al menos dos factores diferentes: 1) algo que saben, 2) algo que saben tienen, o 3) algo que son.**	Una captura de pantalla de la configuración multifactor o una copia de la registros de acceso agregados que muestran que se está aplicando Multi Factor aplicaciones, sistemas y servicios orientados a internet.
4,1	**Requerido**	**Mantenimiento del Inventario de activos**	**Mantener un registro preciso y actualizado inventario de todos los activos de hardware (ordenadores de sobremesa, portátiles, dispositivos móviles, tecnología operativa) que pueden almacenar o procesar**	Una copia actual del inventario de activos de hardware de la organización, validado en el último trimestre.
4,2	**Requerido**	**Dirección Activos no**	**Asegurarse de que cualquier dispositivo no o bien se ha retirado de la red, puesto en cuarentena o añadido al lista de inventario de equipos dentro de un modo**	Captura de pantalla de un sistema automatizado capaz de detectar y direccionar dispositivos no autorizados en la red en un plazo de 48 horas, o documentos que conciliación manual de inventarios de activos de hardware, como dos inventarios con anotaciones para dispositivos recién inventariados y comentarios cómo se están abordando los nuevos dispositivos.
4,3	**Requerido**	**Proteger información A través de Access Control**	**Protege la información confidencial sistemas, recursos compartidos de red, bases de datos con controles de acceso para solo las personas autorizadas tienen acceso a información basada en su función en el organización.**	Una política de clasificación de datos documentada y/o una captura de pantalla de consola de administración adecuada que rige el acceso a datos confidenciales que muestra la implementación de los controles de acceso en un sistema de archivos, compartir, aplicación o base de datos.
4,4	**Requerido**	**Cifrar todo lo sensible Información en Tránsito**	**Cifrar toda la información confidencial (p. ej. PII del cliente, información de compra) durante el transporte.**	Captura de pantalla de la configuración o copia del proceso/política de la que rige el cifrado de la información confidencial en tránsito (correo electrónico,
4,5	**Requerido**	**Extracción de Datos o sistemas no Acceso regular por organización**	**Retirar los datos sensibles o los sistemas que se accede regularmente desde la red. Estos sistemas deben usarse como soporte sistemas independientes (desconectados de red) por el grupo que necesita utilice ocasionalmente el sistema o virtualice estos sistemas y mantenerlos apagados hasta necesario.**	Una política de retención de datos documentada, o un registro documentado o un cualquier formato - mostrando a) la fecha más reciente en que se realizó una una declaración de si se identificaron sistemas o datos para la extracción; y c) las fechas en que esos sistemas y/o datos fueron eliminados de la red.
4,6	**Requerido**	**Permitir solo acceso a nube autorizada Almacenamiento o Proveedores**	**Permitir acceso solo a la nube autorizada proveedores de almacenamiento o correo las fuentes deben estar bloqueadas.**	Captura de pantalla de una consola de administración, como una solución de o Cloud Access Security Broker que muestra que el almacenamiento no autorizado y los proveedores de correo electrónico han sido bloqueados.

5,1	**Requerido**	**Nombrar una garantía Campeón**	**Un campeón de seguridad es alguien que sirve como mentor y animador de deportes, involucrar y alentar a todos empleados para aprender, adoptar y comprometidos con los protocolos de los campeones pueden no tener una comprensión de la seguridad como alguien infosec o IT, pero saben lo suficiente para responder a preguntas básicas y servir como puente entre los gurús de infosec y el empleados ordinarios.**	Enviar el nombre, la posición, la dirección de correo electrónico y el número de Campeón de seguridad. Esta persona debe residir dentro de la organización.
5,2	**Requerido**	**Copia de seguridad Datos y sistemas Periódicamente y Fuera de línea**	**Asegurarse de que todas las claves de la los sistemas de procesamiento comercial completamente a través de la imagen, para una rápida recuperación de todo un sistema.**	Proceso documentado que rige el proceso de copia de seguridad, incluida la qué copias de seguridad se realizan y la certificación de si lo son o no se mantiene en un lugar distinto de la red del concesionario.
5,3	**Requerido**	**Datos de prueba en Medios**	**Probar la integridad de los datos en un medio de forma regular mediante la realización de proceso de restauración para garantizar que la copia de seguridad funciona**	Un registro documentado de esta prueba, en cualquier formato, que muestre todo a) lista de los diferentes tipos de medios de copia de seguridad utilizados; b) la se realizó una prueba de restauración de datos para ese tipo de medio y c) los la prueba (p. ej., se restauraron los datos correctamente).
5,4	**Requerido**	**Publicar información A la fuerza de trabajo Cómo Informar Ordenador Anomalías y Incidentes**	**Publicar información a todos los empleados cómo y cuándo informar al equipo anomalías e incidentes según corresponda personal, incluido el tercero necesario partes, cuando corresponda**	Una copia o imagen de la información publicada que informa a los empleados informar de anomalías e incidentes informáticos.
5,5	**Requerido**	**Desarrollar un Plan de respuesta**	**Desarrollar y documentar un incidente plan de respuesta que define las funciones y responsabilidades para el personal y gestión en respuesta a una seguridad incidente**	Una copia del plan de respuesta a incidentes documentado de la organización.