**Ciberseguridad Chevrolet**

****

Alumnos

My. Gómez Rodríguez Mauricio

My. Carlos Andrés Rey Castiblanco

My. Fuyo Rodríguez Giovanny

My. Diego Granja

Docente:

**Jaider Ospina Navas**

“Gestión de Riesgos Cibernéticos”

**Escuela Superior de Guerra**

Bogotá D.C 03 de marzo 2025

# INTRODUCCIÓN

La transformación digital en la industria automotriz ha evolucionado la forma en que las empresas operan, y Chevrolet no es la excepción. A través de la adopción de tecnologías avanzadas, como la manufactura inteligente, la conectividad de vehículos y la integración de plataformas de trabajo colaborativo, la empresa ha optimizado sus procesos de producción, ventas y atención al cliente. Sin embargo, esta digitalización también ha traído consigo una mayor exposición a riesgos cibernéticos, especialmente en un entorno de trabajo híbrido donde los empleados acceden a sistemas corporativos desde ubicaciones remotas.

El modelo de trabajo híbrido, adoptado por Chevrolet para mejorar la flexibilidad laboral, implica el uso de redes domésticas, dispositivos personales y conexiones a la nube, lo que amplía la superficie de ataque para posibles amenazas. Entre los riesgos más comunes se encuentran el phishing, el ransomware, la suplantación de identidad y las vulnerabilidades en la infraestructura de red. Estos ataques pueden afectar no solo la operatividad de la empresa, sino también la confidencialidad de la información sensible, como datos de clientes, patentes y planes de desarrollo.

Para mitigar estos riesgos, Chevrolet implementa controles basados en estándares internacionales, como la ISO 27001:2022, y utiliza modelos de análisis de amenazas como STRIDE, PASTA y DREAD. Este enfoque permite identificar, priorizar y abordar las vulnerabilidades, garantizando la resiliencia de la empresa frente a amenazas cibernéticas en un entorno digital y de trabajo distribuido.

# ****DESCRIPCIÓN DEL ESCENARIO****

Chevrolet, como una de las marcas más reconocidas en la industria automotriz y una filial de General Motors, ha adoptado tecnologías avanzadas para optimizar sus procesos de fabricación, distribución y gestión de vehículos. La transformación digital ha sido clave para mejorar la eficiencia operativa, la seguridad vehicular y la experiencia del cliente. Sin embargo, la creciente dependencia de sistemas digitales introduce una serie de **riesgos de seguridad cibernética** que pueden comprometer tanto la infraestructura interna de la empresa como sus productos finales.

## ****Digitalización y Tecnologías Implementadas****

### En los últimos años, Chevrolet ha integrado **Internet de las Cosas (IoT), inteligencia artificial (IA), machine learning y computación en la nube** para mejorar el rendimiento de sus operaciones. Las fábricas de ensamblaje utilizan robots industriales y sensores conectados que optimizan la producción, mientras que la conectividad vehicular permite a los clientes acceder a funciones avanzadas como sistemas de navegación, monitoreo remoto y asistencia de conducción.

## ****Principales Riesgos de Seguridad****

A medida que Chevrolet avanza en su transformación digital, surgen diversas amenazas cibernéticas, entre ellas:

### ****Ciberataques a la infraestructura de producción:****

Sistemas de manufactura basados en (IoT) pueden ser vulnerables a ataques de ransomware o sabotajes que detengan la producción.

### ****Interrupción en la cadena de suministro:****

Los proveedores de software y hardware pueden ser un punto débil si no cumplen con los estándares de ciberseguridad.

### ****Brechas de seguridad en vehículos conectados:****

Funcionalidades como el acceso remoto y la telemetría pueden ser explotadas para manipular sistemas críticos del automóvil.

### ****Filtración de datos confidenciales:****

Información de clientes, patentes y desarrollos tecnológicos pueden ser blanco de ataques.

Para mitigar estos riesgos, Chevrolet debe implementar **estrategias de ciberseguridad avanzadas** que protejan su ecosistema digital y garanticen la integridad de sus operaciones y productos.

# **ANÁLISIS DE RIESGOS**

## Modelo STRIDE aplicado a Chevrolet

Se emplea el modelo STRIDE para identificar amenazas en seis categorías

### ****Spoofing (Suplantación de identidad)****

Riesgo de acceso no autorizado a sistemas internos de producción y gestión de flotas.

### ****Tampering (Manipulación de datos)****

Posibilidad de alteración de software en vehículos conectados, afectando su rendimiento o seguridad.

### ****Repudiation (Repudio de acciones)****

Falta de registros fiables en transacciones y operaciones digitales dentro de la cadena de suministro.

### ****Information Disclosure (Divulgación de información confidencial)****

Filtración de diseños y tecnología propietaria de Chevrolet a competidores o actores malintencionados.

### ****Denial of Service (Denegación de servicio)****

Posibles ataques a sistemas de producción y redes vehiculares, generando interrupciones en las operaciones.

### ****Elevation of Privilege (Escalamiento de privilegios)****

Vulnerabilidades en accesos administrativos que podrían ser explotadas por atacantes internos o externos.

## Evaluación de Riesgos

Se analiza la probabilidad e impacto de cada amenaza, priorizando los riesgos más críticos con base en una matriz de riesgos, considerando la operación global de Chevrolet y su infraestructura digital.

## Matriz de Riesgos con las Amenazas

| Amenaza | Probabilidad | Impacto | Riesgo | Mitigación |
| --- | --- | --- | --- | --- |
| Phishing (Spoofing) | Alta | Alta | Crítico | MFA, concienciación y filtrado de correos. |
| Manipulación de Datos | Media | Alta | Alto | Controles de integridad y auditoría. |
| Repudio | Baja | Media | Medio | Logs inmutables y blockchain. |
| Divulgación de Información | Alta | Alta | Crítico | Cifrado fuerte y segmentación de datos. |
| Ataque DDoS | Media | Alta | Alto | Firewalls anti-DDoS y balanceo de carga. |
| Elevación de Privilegios | Media | Alta | Alto | Privilegio mínimo y monitoreo constante. |

# ****IMPLEMENTACIÓN DEL SGSI SEGÚN LA ISO/IEC 27001****

## ****Alcance del SGSI en Chevrolet****

El **Sistema de Gestión de Seguridad de la Información (SGSI)** de Chevrolet se enfoca en los siguientes aspectos clave:

* **Protección de la información corporativa y de los clientes**: Seguridad en datos de clientes, patentes y proyectos de desarrollo.
* **Ciberseguridad en vehículos conectados**: Protección de telemetría y sistemas remotos.
* **Seguridad en la infraestructura de TI y fabricación**: Prevención de ciberataques en la red interna y en sistemas de manufactura.
* **Gestión de riesgos en la cadena de suministro**: Aseguramiento de estándares de ciberseguridad en proveedores de hardware y software.

## ****Evaluación de Riesgos****

Para identificar amenazas y vulnerabilidades, Chevrolet emplea el modelo **STRIDE**, en conjunto con la **ISO/IEC 27005**, la norma de gestión de riesgos de seguridad de la información. Se desarrollan matrices de riesgos en las que se evalúan:

* **Probabilidad de ocurrencia** de incidentes de seguridad.
* **Impacto sobre las operaciones** y la reputación de la empresa.

# DISEÑO DE CONTROLES DE SEGURIDAD

## ****Controles Técnicos****

Para mitigar los riesgos identificados y fortalecer la seguridad digital en Chevrolet, se implementarán los siguientes controles técnicos:

## ****Implementación de autenticación multifactor (MFA) en sistemas internos y vehiculares****

Se aplicará MFA en los accesos a sistemas internos de Chevrolet, como plataformas de gestión de producción, logística y sistemas administrativos.

Para los vehículos conectados, se integrará MFA en aplicaciones móviles y plataformas de gestión remota, garantizando que solo usuarios autorizados puedan acceder a funciones críticas del automóvil, como arranque remoto y monitoreo de telemetría.

Se utilizarán métodos avanzados de autenticación, incluyendo biometría, tokens físicos y autenticación basada en contexto para detectar accesos sospechosos.

## ****Cifrado de datos en comunicaciones entre vehículos conectados y servidores****

Se implementarán protocolos de cifrado robustos como **TLS 1.3 y AES-256** para proteger la transmisión de datos entre vehículos inteligentes y los servidores de Chevrolet.

Se cifrarán las bases de datos que almacenan información sensible de los clientes, telemetría vehicular y registros de mantenimiento.

Se aplicarán políticas de cifrado de extremo a extremo para evitar la intercepción de datos por parte de actores malintencionados.

## ****Monitoreo continuo de ciber amenazas y detección de intrusiones en la red corporativa****

Se implementarán **Sistemas de Detección y Prevención de Intrusos (IDS/IPS)** en la red corporativa para identificar y bloquear actividades sospechosas en tiempo real.

Se establecerá un **Centro de Operaciones de Seguridad (SOC)** que supervisará continuamente el tráfico de la red y responderá a incidentes de seguridad.

Se utilizarán tecnologías de **inteligencia artificial y machine learning** para detectar patrones anómalos en los sistemas de producción, distribución y gestión de vehículos.

Se realizará una auditoría y análisis forense después de cada incidente para reforzar la postura de seguridad.

Estos controles técnicos garantizarán una mayor protección contra ciberamenazas y permitirán una respuesta más rápida y efectiva ante posibles ataques dirigidos a la infraestructura digital de Chevrolet.

## ****Controles Administrativos****

Para garantizar una correcta gestión de la seguridad en Chevrolet, se implementarán medidas administrativas que permitan reforzar el acceso a la información, la concienciación del personal y el cumplimiento normativo en toda la organización y su cadena de suministro.

## ****Políticas estrictas de acceso y control de credenciales para empleados y proveedores****

Se aplicará el principio de **mínimos privilegios** para que los empleados y proveedores solo accedan a la información y sistemas que requieran para sus funciones específicas.

Se implementará un sistema de **gestión de identidades y accesos (IAM)** con autenticación basada en roles y revisiones periódicas de permisos.

Se exigirá el uso de **contraseñas robustas y autenticación multifactor (MFA)** para acceder a sistemas críticos.

Se establecerán mecanismos de **control de accesos físicos y digitales** para restringir la entrada a áreas sensibles dentro de las instalaciones y sistemas de TI.

Se reforzará la seguridad en la contratación de proveedores, evaluando sus medidas de ciberseguridad antes de conceder acceso a infraestructura de Chevrolet.

## ****Programas de concienciación y capacitación en ciberseguridad dirigidos a todo el personal.****

Se impartirán capacitaciones periódicas sobre **buenas prácticas de seguridad digital**, abordando temas como ingeniería social, phishing, uso seguro de dispositivos y protección de datos.

Se implementarán simulaciones de ataques de phishing para evaluar la preparación de los empleados y reforzar la cultura de seguridad.

Se desarrollarán **manuales y guías de ciberseguridad** accesibles a todos los empleados y proveedores.

Se incluirán sesiones específicas para altos ejecutivos sobre **gestión de riesgos cibernéticos y respuesta a incidentes**.

Se establecerá un canal de comunicación interno para reportar actividades sospechosas o intentos de ataque en la infraestructura digital de Chevrolet.

## ****Evaluaciones periódicas de cumplimiento de normativas de seguridad en la cadena de suministro****

Se realizarán auditorías regulares para verificar el cumplimiento de estándares de ciberseguridad como **ISO/IEC 27001, ISO/SAE 21434** y regulaciones automotrices como **UNECE WP.29**.

Se exigirán **pruebas de penetración** y auditorías de seguridad en las soluciones digitales y hardware proporcionados por terceros.

Se implementarán contratos de **acuerdos de nivel de servicio (SLA)** con cláusulas específicas de ciberseguridad para proveedores de software y hardware.

Se realizarán inspecciones y revisiones a los procesos de fabricación y distribución para detectar posibles vulnerabilidades en la cadena de suministro.

Se fortalecerán las políticas de **evaluación de riesgos y gestión de incidentes** en colaboración con socios comerciales y proveedores estratégicos.

## ****Controles Físicos****

Para proteger la infraestructura crítica de Chevrolet y minimizar los riesgos de accesos no autorizados, sabotajes y fallos operativos, se implementarán los siguientes controles físicos:

## ****Restricción de acceso a plantas de fabricación y laboratorios de diseño****

Se establecerán **zonas de acceso restringido** en plantas de producción y laboratorios de innovación, donde solo personal autorizado podrá ingresar.

Se implementarán **sistemas de control de acceso biométrico** (huella dactilar, reconocimiento facial) y tarjetas RFID para verificar la identidad de empleados y visitantes.

Se aplicará una **política de acceso basado en roles (RBAC)** para que cada empleado solo pueda ingresar a las áreas necesarias según su función.

Se exigirá **identificación obligatoria** y registros de entrada/salida para cualquier visitante o proveedor externo que acceda a las instalaciones.

Se utilizarán **puertas de seguridad y esclusas** en áreas sensibles para evitar la entrada no autorizada.

## ****Vigilancia perimetral en instalaciones estratégicas****

Se instalarán **sistemas de videovigilancia (CCTV) de alta resolución** con monitoreo en tiempo real en puntos clave de las instalaciones.

Se establecerán **rondas de seguridad y patrullas físicas** en zonas críticas para detectar actividades sospechosas.

Se integrarán **sensores de movimiento, alarmas y detección de intrusos** para alertar sobre accesos no autorizados.

Se implementarán sistemas de **control de drones de vigilancia** para patrullar áreas de difícil acceso en las instalaciones de producción y almacenamiento.

Se coordinará con **autoridades locales y fuerzas de seguridad** para reforzar la protección en situaciones de emergencia.

## ****Implementación de redundancias para la continuidad operativa en caso de incidentes****

Se establecerán **centros de datos redundantes** en ubicaciones geográficamente dispersas para garantizar la continuidad operativa en caso de fallos o ataques cibernéticos.

Se dispondrá de **fuentes de energía de respaldo**, como generadores y sistemas de alimentación ininterrumpida (UPS), para mantener en funcionamiento las operaciones en caso de apagones.

Se realizarán pruebas periódicas de **planes de contingencia y recuperación ante desastres** para evaluar la capacidad de respuesta de la organización.

Se implementarán **almacenes seguros de repuestos y suministros críticos**, garantizando la disponibilidad de materiales esenciales en caso de interrupciones en la cadena de suministro.

Se aplicará un sistema de **resguardo de datos y copias de seguridad fuera del sitio (offsite backup)** para proteger información clave de la empresa ante incidentes físicos o ciberataques.

Estos controles físicos permitirán reforzar la seguridad en las instalaciones de Chevrolet, protegiendo tanto la integridad de su infraestructura como la continuidad de sus operaciones en un entorno cada vez más expuesto a riesgos internos y externos.

# ****CONCLUSIONES Y RECOMENDACIONES****

El análisis de riesgos realizado en Chevrolet ha identificado varias amenazas críticas derivadas de la digitalización de sus procesos, la conectividad de sus vehículos y la complejidad de su cadena de suministro. Entre los principales riesgos destacan:

**Ciberataques a la infraestructura de manufactura**, lo que podría paralizar la producción y generar pérdidas económicas.

**Interrupciones en la cadena de suministro**, causadas por vulnerabilidades en los proveedores de software y hardware.

**Brechas de seguridad en vehículos conectados**, que podrían exponer a los clientes a ataques remotos o manipulación de software.

**Filtración de datos confidenciales**, afectando la propiedad intelectual y la información de clientes y socios comerciales.

**Accesos no autorizados a sistemas internos**, facilitados por credenciales débiles o falta de controles de acceso adecuados.

Para mitigar estos riesgos, se han diseñado e implementado una serie de controles técnicos, administrativos y físicos que refuerzan la postura de ciberseguridad de Chevrolet.

# ****RECOMENDACIONES****

Para fortalecer aún más la seguridad de la empresa, se recomienda la adopción de las siguientes medidas estratégicas:

## ****Auditorías de seguridad regulares****

Realizar pruebas de penetración en sistemas internos y vehículos conectados para detectar vulnerabilidades antes de que puedan ser explotadas.

Evaluar periódicamente el cumplimiento de normas de ciberseguridad como **ISO/IEC 27001, ISO/SAE 21434 y UNECE WP.29**.

Auditar proveedores para garantizar que cumplen con los estándares de seguridad exigidos.

## ****Simulaciones de ataques controladas (Red Teaming y ejercicios de respuesta a incidentes)****

Organizar simulaciones de **ataques de ransomware y phishing** para evaluar la preparación del equipo de TI y los empleados.

Desarrollar ejercicios de **respuesta a incidentes de ciberseguridad** para mejorar la capacidad de reacción ante amenazas reales.

Implementar **escenarios de crisis** donde se pongan a prueba los protocolos de continuidad del negocio.

## ****Actualización constante de sistemas y políticas de seguridad****

Aplicar parches y actualizaciones de software de manera regular en todos los sistemas digitales y vehículos conectados.

Revisar y reforzar las políticas de seguridad interna, estableciendo procedimientos de gestión de accesos y control de credenciales más estrictos.

Adoptar herramientas de **inteligencia artificial para la detección de anomalías** y la identificación proactiva de posibles amenazas.

## ****Concienciación y capacitación en ciberseguridad****

Continuar con programas de formación dirigidos a empleados, ejecutivos y proveedores, con especial énfasis en la prevención de ataques de ingeniería social.

Implementar campañas de sensibilización sobre la importancia de la seguridad digital y las mejores prácticas en la protección de datos.

## ****Refuerzo de la seguridad en la cadena de suministro****

Exigir controles de ciberseguridad más estrictos a terceros que proveen software, hardware y servicios digitales.

Establecer **protocolos de respuesta a incidentes conjuntos** con proveedores clave para minimizar el impacto de ciberataques en la cadena de suministro.

Con la implementación de estas recomendaciones, Chevrolet podrá **fortalecer su postura de ciberseguridad, garantizar la continuidad operativa y reducir los riesgos asociados a la digitalización y conectividad de su ecosistema empresarial y vehicular**.

# BIBLIOGRAFÍA

# Ananth A. Jillepalli, F. T. (2017). Security Management of Cyber Physical Control Systems Using NIST SP 800-82r2. En *IWCMC 2017 : the 13th International Wireless Communications & Mobile Computing Conference : June 26-30, 2017, Valencia, Spain* (págs. 1-7). Estados Unidos : IEEE.

* Da Silva, M. M.-H. (2023). Automated ICS template for STRIDE Microsoft Threat Modeling Tool. *HAL OPEN SCIENCE*, 1-7.
* Hammami, A. (2024). The Art of Threat Modeling. *Journal of Computer Sciences and Informatics*, 1-11.
* Hentea, M. (2021). C: Critical Infrastructures Concepts. En *Creación de un programa de seguridad eficaz para los recursos y sistemas de energía distribuida.* Estados Unidos : Hentea, Mariana.
* Kurii, Y. I. (2023). ISO. 27001. ANÁLISIS DE CAMBIOS Y CARACTERÍSTICAS DE CUMPLIMIENTO DE LA NUEVA VERSIÓN DE LA NORMA . *Ciberseguridad: Educación , Ciencia, Técnica Volumen 3*, 1-10.
* Nogués López, J. (2023). *Solución de ciberseguridad aplicada al vehículo conectado.* España : Univertitad Obaerta de Catalunya.