Política General de Seguridad de la Información

ELABORADO POR	REVISADO POR	APROBADO POR
Nombre: Victor Hurtado	**Nombre:** Sebastián Galvis	**Nombre:** Jhon Edison Marín
Cargo: Analista TI	**Cargo:** Coordinador de Infraestructura	**Cargo:** Gerente de Tecnología Digital

Contenido

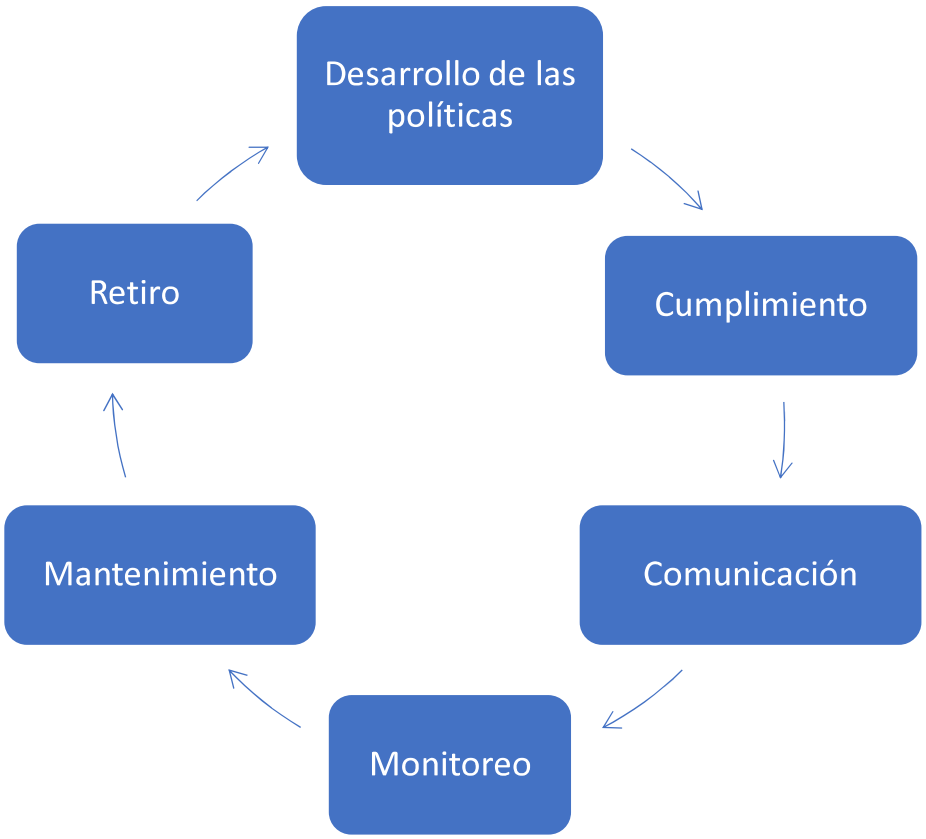
INTRODUCCIÓN

YOKOMOTOR, en adelante la empresa, reconoce la importancia de la información que gestiona, debido a que es uno de los activos más significativos para su funcionamiento y que ésta puede ser de naturaleza legal, estratégica, financiera, operativa y en algunos casos corresponder a datos personales de practicantes, empleados, proveedores, contratistas o grupos de valor.

De igual manera, es consciente de las amenazas que enfrenta la información y de las consecuencias a las que se expone la empresa cuando no cuente con las medidas de seguridad y protección adecuadas. En ese sentido, la empresa debe tener una visión general de los riesgos de seguridad digital que pueden afectar la seguridad y privacidad de la información, donde se podrán establecer controles y medidas efectivos, viables y transversales con el propósito de realizar el aseguramiento de la disponibilidad, integridad y confidencialidad tanto de la información del negocio como de los datos de los practicantes, empleados, proveedores, contratistas y grupos de valor. Es indispensable que la empresa realice una adecuada identificación, clasificación, valoración, gestión y tratamiento de los riegos de seguridad que puedan afectar la información de la entidad, con el propósito de implementar medidas y controles efectivos que permitan estar preparados ante situaciones en las que se vea comprometida tanto la seguridad física y lógica de su información.

Teniendo en cuenta lo anterior, el presente Manual tiene como finalidad establecer los principios orientadores en seguridad que buscan garantizar la disponibilidad, integridad, confidencialidad, privacidad, continuidad, autenticidad y no repudio de la información de YOKOMOTOR, así como dar lineamientos para la aplicación de mecanismos que eviten la vulneración de la seguridad y privacidad de la información, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información – SGSI. La seguridad de la información es para la empresa, una labor prioritaria que anima a todos a velar por el cumplimiento de las políticas establecidas en el presente documento.

METODOLOGÍA



Desarrollo de las políticas: Se crean las políticas, se definen los roles y responsabilidades de quienes revisan, aprueban.

Cumplimiento: Fase mediante la cual todas las políticas escritas deben estar implementadas y relacionadas a los controles de seguridad de la Información, esto con el fin de que exista consistencia entre lo escrito en las políticas versus los controles de seguridad implementados y documentados.

Comunicación: Fase mediante la cual se da a conocer las políticas a los funcionarios, contratistas y/o terceros de la Entidad. Esta fase es muy importante toda vez que del conocimiento del contenido de las políticas depende gran parte del cumplimiento de estas.

Monitoreo: Se monitorean para determinar la efectividad y cumplimiento de éstas, a través de indicadores para verificar de forma periódica y con evidencias que la política funciona y si debe o no ajustarse.

Mantenimiento: Esta fase es la encargada de asegurar que la política se encuentra actualizada, integra y que contiene los ajustes necesarios y obtenidos de las retroalimentaciones.

Retiro: Fase mediante la cual se hace eliminación de una política de seguridad en cuanto esta ha cumplido su finalidad o la política ya no es necesaria en la Entidad. Esta es la última fase para completar el ciclo de vida de las políticas de seguridad y requiere que este retiro sea documentado con el objetivo de tener referencias y antecedentes sobre el tema.

ELABORADO POR	REVISADO POR	APROBADO POR
Nombre: Victor Hurtado	**Nombre:** Sebastián Galvis	**Nombre:** Jhon Edison Marín
Cargo: Analista TI	**Cargo:** Coordinador de Infraestructura	**Cargo:** Gerente de Tecnología Digital

1. OBJETIVO

Establecer lineamientos necesarios, con el fin de fortalecer la gestión de Seguridad y privacidad de la Información de YOKOMOTOR, enmarcados en la implementación de un Sistema de Gestión de Seguridad de la Información, basado en la identificación y valoración de los riesgos asociados a ella, propendiendo por la protección de su confidencialidad, integridad, disponibilidad, privacidad, continuidad y autenticidad.

2. ALCANCE

Los lineamientos contenidos en el presente documento son aplicables para todos los aspectos administrativos y de control que deben ser cumplidos por los practicantes, empleados, proveedores, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con la YOKOMOTOR a través de la recolección, procesamiento, almacenamiento, recuperación, intercambio y consulta de información, con personal interno o externo, en el desarrollo de la misión y el cumplimiento de sus objetivos estratégicos.

3. DEFINICIONES

Activo: Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas) que tienen un valor para la entidad.

Activo crítico: Instalaciones, sistemas y equipos los cuales, si son destruidos, o es degradado su funcionamiento o por cualquier otro motivo no se encuentran disponibles, afectarán el cumplimiento de los objetivos estratégicos de YOKOMOTOR.

Administración de Riesgos: Se entiende por administración de riesgos, como el proceso de identificación, control, minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar la información o impactar de manera considerable la operación. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la entidad.

Análisis de Impacto al Negocio (BIA): Es una metodología que permite identificar los procesos críticos que apoyan los productos y servicios claves, las interdependencias entre procesos, los recursos requeridos para operar en un nivel mínimo aceptable y el efecto que una interrupción del negocio podría tener sobre ellos.

Autenticidad: Busca asegurar la validez de la información en tiempo, forma y distribución. Así mismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

Alta Dirección: Persona o grupo de personas que dirigen y controlan al más alto nivel una entidad (director general, gerente general, jefe administrativo).

Control: Son todas aquellas políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

Confiabilidad de la Información: Es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Confidencialidad: Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

Datos sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

Disponibilidad: Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Evento de seguridad de la información: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o falla de salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

Estándar: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.

Guía: Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares, buenas prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.

Incidente de Seguridad: Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazar la seguridad de la información.

Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Integridad: Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

Mejor Práctica: Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.

Política: Declaración de alto nivel que describe la posición de YOKOMOTOR sobre un tema específico.

Privacidad de la información: El derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de Gobierno Digital la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Procedimiento: Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los

procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la entidad, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro del a dependencia donde ellos se aplican.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales. Conjunto de aplicaciones que interactúan entre sí para apoyar un área o proceso del Ministerio.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

4. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La empresa YOKOMOTOR, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido a proteger, preservar y administrar la confidencialidad, integridad, disponibilidad y no repudio de la información de la entidad, mediante una gestión integral de riesgos, implementación de controles físicos y digitales, previniendo incidentes y dando cumplimiento a los requisitos legales y reglamentarios, orientados a la mejora continua, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la compañía.

Para asegurar la dirección estratégica se establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información así:

- Minimizar la materialización del riesgo en la ejecución de los procesos de la empresa.
- Cumplir con los principios de seguridad de la información (Disponibilidad, Integridad y Confidencialidad).
- Mantener la confianza de sus clientes, socios, empleados y accionistas.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los aprendices, empleados, proveedores de YOKOMOTOR.
- Verificar de manera periódica el cumplimiento de las políticas de seguridad de la información.
- Garantizar la continuidad del negocio frente a incidentes de seguridad de la información.
- Propender para que todos los aprendices, empleados, proveedores y terceros cumplan con las políticas, lineamientos, y buenas prácticas de seguridad de la información establecidas aquí.

5. POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

A continuación, se establecen 12 principios de seguridad que soportan el SGSI de YOKOMOTOR:

1. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.
2. YOKOMOTOR protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
3. YOKOMOTOR protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
4. YOKOMOTOR protegerá su información de las amenazas originadas por parte del personal.
5. YOKOMOTOR protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
6. YOKOMOTOR controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
7. YOKOMOTOR implementará control de acceso a la información, sistemas y recursos de red.
8. YOKOMOTOR garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
9. YOKOMOTOR garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
10. YOKOMOTOR garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
11. YOKOMOTOR garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.
12. YOKOMOTOR garantiza en su proceso de contratación que el empleado asuma el compromiso de manejar la información confidencial de la empresa de manera segura y responsable, no se prohíbe el uso de dispositivos móviles personales con fines corporativos, sin embargo, el empleado debe recibir la asesoría continúa brindada por el departamento de TI sobre las mejores prácticas para el uso responsable y actualización de la seguridad de sus dispositivos.

El incumplimiento a la política de Seguridad y Privacidad de la Información traerá consigo, las consecuencias legales que apliquen a la normativa de la compañía, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

5.1 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

5.2 GESTION DE ACTIVOS

Identificación de Activos

Clasificación de Activos

Etiquetado de información:

Toda información producida o recibida en el desarrollo de las funciones de las áreas de YOKOMOTOR deber ser clasificada para ser debidamente protegida de acceso no autorizado, modificación, divulgación o destrucción sin importar el origen de la misma (equipos de cómputo, servidores de archivos, archivadores de oficina, comunicaciones verbales, etc.)

Niveles de seguridad para la información:

La siguiente clasificación establece los niveles para la información según el carácter de acceso, y el cual se debe tener en cuenta para el control, consulta y divulgación de la misma

Categoría	Descripción	Ejemplos	Posibles Impactos
Publica (Cuando todas las personas pueden ver esa información)	Información de origen interno o externo que puede ser consultado por cualquier funcionario o persona externa.	Convocatorias, Campañas de responsabilidad social, Campañas a clientes, PBX, ubicación de oficinas.	· Ningún impacto. Mínimos inconvenientes si no está disponible. · Temporalmente, no genera impactos negativos sobre la compañía
Protegido (para información de nivel de confidencialidad más bajo)	Aquella información de carácter corporativa y que puede ser consultada por cualquier funcionario, pero no por una persona externa	Material educativo, estructura de la organización, datos de contacto, planes y programas de bienestar, políticas de la compañía, procedimientos, formatos.	● Perdida de la seguridad de la información de la compañía. ● Procesos jurídicos por divulgación de información. ● Sabotaje ● Deterioro de la reputación. ● Perdida de la confianza en las actividades. ● Perdida de la privacidad de individuos.
Confidencial (para niveles medios de confidencialidad)	Aquella información relacionada a los procesos y actividades de un área que es consultada únicamente por los funcionarios correspondientes a esta, este tipo de información presenta riesgo de impacto alto o significativo para la compañía, su reputación y operaciones.	Información de proveedores, pagos, activos fijos, estados de cartera, pqrs, manifiestos de importación.	· Perdida de la privacidad de datos individuales y corporativos.
Legal / Información privilegiada ***(Información confidencial relacionada con el área legal)***	Aquella información o comunicaciones relacionadas a los procesos del área jurídica de la compañía, este tipo de información presenta riesgo de impacto alto o significativo para la compañía, su reputación y operaciones.	Solicitudes de asesoramiento legal, contratos, PQR's, procesos jurídicos, documentos preparados a solicitud de o por un abogado.	Perdida o divulgación de información legal · Acceso de terceros a información privilegiada de información exclusiva de los abogados como parte del secreto Profesional

ELABORADO POR	REVISADO POR	APROBADO POR
Nombre: Victor Hurtado	**Nombre:** Sebastián Galvis	**Nombre:** Jhon Edison Marín
Cargo: Analista TI	**Cargo:** Coordinador de Infraestructura	**Cargo:** Gerente de Tecnología Digital

Altamente Confidencial (cuando el nivel de confidencialidad de la información sea elevado)	Toda información sensible para la compañía y que no se ha puesto a disposición de los empleados o terceros; para poder ser consultada se requiere de autorización por parte de un vicepresidente, gerente o jefe líder de proceso o área.	Cifras de ventas,Pedidos de vehículos y repuestos, nuevoslanzamientos, estrategiascomerciales, usuarios, contraseñas, firmas digitales,e, historias laborales.	· Publicación de información legal con terceros a la empresa · Perdida o divulgación de información confidencialmente

Devolución de los Activos

Gestión de medios removibles

Disposición de los activos

Dispositivos móviles

5.3 CONTROL DE ACCESO

Control de acceso con usuario y contraseña

Suministro del control de acceso

Gestión de Contraseñas

Perímetros de Seguridad

Áreas de Carga

5.4 NO REPUDIO

Trazabilidad

Retención

Auditoría

5.5 PRIVACIDAD Y CONFIDENCIALIDAD

Ámbito de aplicación

Excepción al ámbito de aplicación de las políticas de tratamiento de datos personales

Principios del tratamiento de datos personales

Principio de la Legalidad

Principio de finalidad

Principio de libertad

Descripción Del Equipo Que Manejará Los Incidentes

Aspectos Legales

5.10 CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

Política De Escritorio Limpio

Política De Uso Aceptable

Ética Empresarial

3. CONTROL DE CAMBIOS

VERSIÓN	FECHA	MODIFICACIONES REALIZADAS
01	28/11/2023	Primera edición
02	26/08/2024	Se agrega niveles para la información según el carácter de acceso