Política de Seguridad de la Información

Código de autenticidad y verificación:

ae8bcb8c2add1a32920883aee1ce3826db58d1c227ccba634663ba337789641b

Certificado de Constancia de Conservación (.con)

Nombre del Documento:	01_Politica_de_Seguridad_de_la_Información.docx		
Versión:	1.00	**Fecha de la versión:**	07/Ene/2021
Nivel de Confidencialidad:	Información Pública		

Creado por:	**Aprobado por:**
FIRMA	FIRMA
Manuel Alejandro Landeros Mendoza	**Julio César Culebro González**

Historial de Modificaciones

FECHA	VERSION	CREADO POR	DESCRIPCION DE LA MODIFICACION
07/01/2021	1.00	Manuel Alejandro Landeros Mendoza	Creación del Documento

Tabla de contenido

1. Aspectos Generales

1.1 Definición de la Seguridad de la Información

En CG SYSTEMS INGENIERIA DE SOFTWARE SA DE CV, la Seguridad de la Información consiste en proveer las bases de consistencia, protección adecuada y preservación de la confidencialidad, integridad y disponibilidad de los activos de información pertenecientes a la empresa. Estableciendo una serie de políticas y estándares de control que garantizan los niveles de seguridad necesarios para minimizar el riesgo que puedan ocasionar posibles interrupciones o daños en los servicios brindados a los clientes.

1.2 Marco de Referencial de Seguridad de la Información

Las políticas y estándares de seguridad en CG SYSTEMS INGENIERIA DE SOFTWARE SA DE CV se apegan a las siguientes normas o controles de Seguridad de la Información:

- ISO/IEC 27001:2013. "Sistema de Gestión de Seguridad de la Información".
- Matriz de Controles de Seguridad publicada por el SAT para aspirantes a Proveedores de Controles Volumétricos.

1.3 Normatividad y legislación vigente aplicable a la empresa

- Matriz de Controles de Seguridad publicada por el SAT para aspirantes a proveedores de Controles Volumétricos.
- Ley Federal de Protección de Datos Personales
- Código Fiscal de la Federación
- Resolución Miscelánea Fiscal

1.4 Roles y Responsabilidades de la Seguridad de la Información

Actividades / Áreas	DG	SOP	DESA	ADMON
Creación del documento	A	I	R	I
Revisión de la Política de Seguridad de Información	A	I	R	I
Publicación del documento	I	I	R	I
Documentar desviaciones y establecer controles compensatorios	A	I	R	I
Implementación de la política	A	I	R	I
Revisión de la Política de Seguridad de la Información	A	I	R	I

DG: Director General. DESA: Líder de Desarrollo. SOP: Líder de Soporte. ADMON: Coordinador Administrativo.
R: Responsable. A: Aprobador. C: Consultado. I: Informado.

1.5 Medidas disciplinarias en caso de incumplimientos a la política.

Ante el incumplimiento de las Políticas y Estándares de Seguridad establecidos en CG SYSTEMS INGENIERIA DE SOFTWARE SA DE CV, ya sea deliberada o inconscientemente, la incidencia debe ser referida al Director General para su análisis y la aplicación de las sanciones correspondientes, de acuerdo con los documentos denominados "***Medidas Disciplinarias***" y **"Reglamento interior de trabajo"**.

1.6 Compromiso de la Dirección y Presupuesto

La Dirección General de la empresa CG SYSTEMS INGENIERIA DE SOFTWARE SA DE CV, ha establecido como parte de la estrategia de crecimiento y madurez de la empresa, la implementación de un modelo de la Seguridad de la Información que sea respaldada por políticas y estándares internacionales. Es por ello que la

Seguridad de la Información es considerada como algo fundamental, por lo que es indispensable contar con los controles, políticas y estándares necesarios que permitan a la empresa asegurar la continuidad del negocio, minimizar los riesgos comerciales y maximizar el retorno de las inversiones y las oportunidades comerciales.

Es por ello que se establece como prioridad el establecimiento de un presupuesto para seguir los mejores lineamientos y controles de la Seguridad de la Información para la empresa CG SYSTEMS INGENIERIA DE SOFTWARE SA DE CV y sus colaboradores.

1.7 Revisión Periódica de la Política de la Seguridad de la información

Cada política y estándar de Seguridad debe revisarse y actualizarse con base a un programa predefinido, requiriendo al menos una revisión semestral a partir de su implementación formal. Dicha programación quedará a cargo del Líder de Desarrollo de CG SYSTEMS INGENIERIA DE SOFTWARE SA DE CV, tomando en cuenta durante la revisión de cada política de seguridad, la evaluación de los siguientes factores:

- Cambios a la estructura organizacional preestablecida
- El efecto de los cambios a la infraestructura y ambiente técnico.
- Iniciativas o directrices de negocio, nuevas o emergentes
- Iniciativas o directrices tecnológicas, nuevas o emergentes
- Factores técnicos o de negocio que afecten o cambien el resultado de las evaluaciones de riesgo previas.

Mas allá de lo anterior se establecen ciertos periodos con el fin de realizar revisiones periódicas y auditorías internas a la Política de Seguridad de la Información, y lograr con ello una mejora continua a la seguridad de la empresa, para ello se define el siguiente calendario:

	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC
Auditoría Interna		X						X				
Revisión de Políticas implementadas			X						X			
Implementación de los cambios a las Políticas				X						X		

Periodicidad de Revisión a las Políticas de Seguridad de la Información

2. Lineamientos de la Política de Seguridad de la Información

La implementación de las Políticas de Seguridad es responsabilidad del Líder de Desarrollo en CG SYSTEMS INGENIERIA DE SOFTWARE SA DE CV. Así mismo, todos los colaboradores de la empresa son responsables de mantener el nivel de seguridad de la información requerido dentro del ámbito de su puesto de trabajo.

2.1 Publicación y Comunicación

Las políticas y estándares de Seguridad que se establezcan en CG SYSTEMS INGENIERIA DE SOFTWARE SA DE CV, deben ser clasificados, comunicados y publicados de tal forma que no puedan modificarse por

personal no autorizado. Debe ser indispensable el uso de técnicas de comunicación para asegurar que las políticas sean relevantes, accesibles y de fácil comprensión para el lector a quien se dirigen. Se deberán realizar talleres y/o platicas de concientización con el todo el personal, con el fin de mantener una cultura de seguridad.

2.2 Controles Compensatorios

Cuando existan circunstancias únicas por las cuales no sea posible cumplir con los requisitos de una política y/o estándar de Seguridad, ya sea parcialmente o en su totalidad, se debe documentar la desviación y establecer los controles compensatorios, los cuales deberán ser revisados y aprobados por el Director General.

2.3 Auditoría y revisión de la Política de Seguridad de la Información

La revisión de la correcta implementación y apego a las políticas vigentes se realizará por un tercero especializado en revisiones de Seguridad de la Información. La validación debe incluir una verificación del cumplimiento técnico llevada a cabo y supervisada por personal técnicamente calificado para validar la configuración de los activos de información, el escaneo y evaluación de vulnerabilidades, así como las pruebas de penetración adecuadas.

2.4 Lineamientos para asegurar la Confidencialidad, Integridad y Disponibilidad de la información ubicada en la infraestructura del proveedor de servicios en la nube.

En las situaciones en que se requiera contratar servicios de tratamiento o resguardo de activos de información tales como servicios en la nube, se deberá verificar que el proveedor cuenta con mecanismos y controles de seguridad adecuados que permitan garantizar la Integridad, confidencialidad y disponibilidad de la información de CG SYSTEMS INGENIERIA DE SOFTWARE SA DE CV que ahí se resguarden.

Sera indispensable que los proveedores de servicio contratados se apeguen y estén certificados en cualquier estándar internacional de seguridad de la información, preferentemente al ISO/IEC 27001:2013, para con ello cumplir a cabalidad con Confidencialidad, Integridad y Disponibilidad que se requieran en algún proceso de la empresa.

De la anterior se determina que todo servicio en la nube que sea contratado por CG SYSTEMS INGENIERIA DE SOFTWARE SA DE CV deberá contar al menos con:

- **Niveles de Servicio** que garanticen la disponibilidad de los servicios proporcionados por el proveedor, se recomienda un nivel mayor al 99.0%.
- **Controles de Acceso Restringido** a los activos de información confiados y a su centro de datos de manera física y lógica que permitan establecer una confianza de confidencialidad sobre los servicios contratados.
- **Controles Criptográficos de transmisión y almacenamiento** que ayuden a mantener la confidencialidad en la transmisión de información.
- **Controles que permitan el uso correcto de la información almacenada**, impidiendo el acceso no autorizado a la misma para su modificación y salvaguardando a su vez la misma para su recuperación en todo momento.
- **Controles de Copias de Seguridad** en sus sistemas.
- **Controles para Reportes y Atención a Problemas y/o Incidentes** presentados en sus servicios.

2.5 Política de Seguridad para proveedores

Los proveedores o terceros que presten sus servicios a la empresa CG SYSTEMS INGENIERIA DE SOFTWARE SA DE CV que contemplen la gestión, transformación o transmisión de información propios de la empresa o sus clientes deben conocer, aceptar y cumplir las políticas de seguridad de la información definidas por CG

SYSTEMS INGENIERIA DE SOFTWARE SA DE CV. En caso de conflicto entre las políticas de seguridad de la Información de la empresa y las políticas de seguridad de los proveedores o terceros se acordarán políticas comunes de seguridad de la información y formalizarán mediante un documento formal suscrito por un representante de ambas partes, que permitan cumplir los requisitos necesarios para garantizar la protección de la confidencialidad, integridad y disponibilidad de la información de la rama judicial.

De esta forma, los riesgos asociados al permitir cualquier tipo de acceso a los activos de información de la organización o sus clientes por parte de terceros deben ser considerados y es por ello que deben existir los contratos necesarios que estipulen los controles de seguridad que deben cumplir para proteger la confidencialidad, disponibilidad e integridad de los activos de información de CG SYSTEMS INGENIERIA DE SOFTWARE SA DE CV, y en los casos que aplique, de sus clientes.

2.6 Aspectos Contractuales de Seguridad de la Información para Proveedores

Los proveedores que presten algún servicio a la empresa y que tengan acceso a activos de información o a la infraestructura de redes y sistemas de la empresa, deben conocer y cumplir, en todo momento las políticas de seguridad. De lo anterior deberá ser necesario que cualquier prestación de servicio relacionada con los procesos y sistemas de control volumétrico tengan:

2.6.1 Cláusulas de confidencialidad

Todos los contratos que formalice la empresa con un prestador de servicios y cuyo servicio esté relacionado con el proceso de Controles Volumétricos, deberá contar realizar los acuerdos de confidencialidad firmados por los representantes legales de las empresas proveedoras de servicios, para asegurar que la información y los activos de información de la empresa a los que se tengan acceso durante la relación laboral y después, no se divulgue sin autorización, ni sea utilizada o modificada en perjuicio de la Institución. El área Jurídica, debe asegurarse de que en los contratos se incluya lo anterior.

2.6.2 Cláusulas de auditoría de servicios

CG SYSTEMS INGENIERIA DE SOFTWARE SA DE CV, debe supervisar, revisar o auditar periódicamente, la provisión de los servicios que ofrecen los terceros. Los proveedores tienen la obligación de entregar a la Institución, oportunamente, la evidencia digital necesaria en caso de incidentes de seguridad o aquella que les sea requerida.

2.6.3 Cláusulas de seguridad de la información

Todos los contratos que formalice la empresa con un prestador de servicios, deben incluir una cláusula específica que asegure el cumplimiento a la política de seguridad de la información y los cambios que de ésta se deriven, durante el periodo de vigencia del contrato.

Todos los requisitos de seguridad de la información deben establecerse y acordarse con cada proveedor que pueda acceder, procesar, almacenar, transmitir, o proveer los componentes de la infraestructura de TI para la información de la empresa, asegurando el cumplimiento de los lineamientos que apliquen, de esta política.

En caso de requerirse el trabajo de un tercero en las instalaciones de la Institución o bien su acceso remoto a las redes y sistemas de la Institución, debe existir un responsable por parte de la empresa que solicite los accesos requeridos por el tercero. Los accesos de terceros a servicios de la Institución (red, aplicaciones, equipos, bases de datos e información) deben estar autorizados y acordes a los perfiles de funciones creados para tal efecto. El acceso físico a los inmuebles de la Institución por parte de terceros debe registrarse en bitácoras (entrada y salida), y el responsable del proyecto acompañará al proveedor en todo momento durante la visita.

2.6.4 Cláusulas de patente, marcas y derechos de autor

Se debe considerar en los acuerdos de contratación de un tercero, además de los requisitos establecidos por el área competente de la Institución los siguientes puntos que permitan mantener los derechos de patente, marcas y derechos de autor tanto de la empresa como del proveedor:

- Compromiso por parte de los terceros de no incurrir o participar en ningún tipo de actividad sospechosa o dañina para las instalaciones, información y/o la operación de la Institución.
- Cláusulas de restricción para el copiado y acceso a la información.
- Cubrir los requerimientos para control de accesos y procedimientos de autorización para acceder a los activos de información de la Institución (tecnológicos e información).

2.6.5 Transferencia de derechos y obligaciones

Se tienen que mantener políticas y procedimientos que aseguren, en todo momento, el nivel de calidad del servicio y la seguridad e integridad de la información; lo anterior, con especial énfasis cuando la empresa contrate la prestación de servicios con proveedores externos para el procesamiento y almacenamiento de dicha información. Cualquier contratación de servicios que esté directamente involucrados con el proceso de controles volumétricos deberán establecerse acuerdos de niveles de servicio (SLA) y acuerdos de niveles de operación (OLA).

2.7 Política de Clasificación de la Información

Se establece que es necesario asegurar que la información recibe un nivel de protección apropiado de acuerdo con su importancia para CG SYSTEMS INGENIERIA DE SOFTWARE SA DE CV, dado el impacto que pudiera tener la información si llegaran a afectarse en su integridad, disponibilidad y confidencialidad, así como el tratamiento que se le debe dar a la misma de acuerdo con valor que tiene para el negocio.

Esta política aplica para toda la información de CG SYSTEMS INGENIERIA DE SOFTWARE SA DE CV contenida en cualquier tipo de medio físico, electrónico, visual, sonoros, electromagnético o en otros tipos de soporte de almacenamiento. Los detalles de la misma se deben revisar en el documento "**08_Política_de_Clasificación_de_la_Información.docx**".

2.8 Política de Uso de Contraseñas

El uso de las contraseñas permite a los activos o recursos informáticos realizar una identificación positiva o negativa de un usuario, al determinarse por definición intrínseca que las contraseñas solo deben ser conocidas por el usuario propietario de la cuenta de acceso, se deben establecer buenas prácticas de uso y composición de las contraseñas.

A todo personal de la empresa CG SYSTEMS INGENIERIA DE SOFTWARE SA DE CV que se le asigne un identificador de usuario tanto para uso personal o de procesos será el responsable de la creación y configuración de su contraseña de acuerdo a los detalles de la política que deben revisarse en el documento **"15_Politica_de_Uso_de_Contraseñas.docx".**

2.9 Política de Uso Desentendido

Cualquier equipo de cómputo perteneciente a CG SYSTEMS INGENIERIA DE SOFTWARE SA DE CV y que tenga acceso a los recursos tecnológicos de la empresa, nunca debe permanecer sin ser utilizado por el usuario responsable durante un tiempo considerable, ya que los equipos informáticos que parezcan abandonados resultan un riesgo para el acceso no autorizado y para el robo o pérdida de información que pudiera ser muy importante para la empresa. Es por ello que para evitar este tipo de riesgos se de revisar a detalle la política especificada en el documento **"15_Politica_de_Equipo_Desatendido.docx".**

2.10 Política de Escritorio Limpio y Pantalla Despejada

Se establece que todo el personal de la empresa CG SYSTEMS INGENIERIA DE SOFTWARE SA DE CV, debe mantener un escritorio limpio, libre de cualquier información sensible para la empresa, misma que pudiera ser tomada para realizar con ella acciones que pongan en riesgo los activos de la empresa. De igual manera se debe mantener una pantalla despejada que no muestra información digital mientras no se encuentre en uso por el usuario asignado.

Todo lo anterior es necesario con el objetivo de aplicar las buenas prácticas de atención a un escritorio limpio, dar presencia y perspectiva correcta de la empresa y salvaguardar toda aquella información sensible, para lograrlo se deben acatar los detalles de esta política definidos en el documento **"17_Escritorio_limpio_y_pantalla_despejada.docx"**.

2.11 Política de Eliminación de Derechos de Acceso

Todo personal que sea dado de baja, que concluya con su contrato laboral con la empresa o bien que por su desarrollo profesional dentro de la empresa cambie de puesto, deberá perder todo acceso a los activos de CG SYSTEMS INGENIERIA DE SOFTWARE SA DE CV, que le hubieron sido otorgados en algún momento.

Los detalles de esta política deben revisarse en el documento **"18_Eliminación_de_Derechos_de_Acceso"**.

2.12 Política de Uso Aceptable de Activos

Dado que los recursos tecnológicos utilizados en la empresa, y la información manejada a través de los mismos, son propiedad de la empresa CG SYSTEMS INGENIERIA DE SOFTWARE SA DE CV, y solamente pueden ser utilizados para propósitos debidamente autorizados y relacionados con las operaciones de la misma, se establecen ciertos lineamientos específicos para cada activo, los cuales se detallan y deben ser revisados en el documento **"23_ Política_de_Uso_Aceptable_de_Activos_y_de_la_informacion.docx"**

2.13 Política de Gestión de Incidentes de Seguridad

Los incidentes de seguridad son sucesos y/o eventos tecnológicos que contravienen las políticas de seguridad de la información y/o que generan acciones en contra de los principios de disponibilidad, integridad y confidencialidad de la información.

Por lo que, se debe establecer un entorno confiable, eficiente e integro que permita una respuesta y un seguimiento a los incidentes que se pudieran presentar, estos detalles se deberán revisar en el documento **"28_Politica_de_Gestion_de_Incidentes_de_Seguridad_de_la_Información"**.

2.14 Política de Control de Accesos

El control de la información y los procesos de aprovisionamiento, deben ser controlados sobre la base de los requisitos y seguridad necesarios para el cumplimiento de las funciones de cada colaborador o proceso, es por ello que se debe administrar correctamente el ciclo de vida de los usuarios, desde la creación de cuentas, asignación de roles y permisos necesarios hasta su operación diaria.

Por lo anterior se especifica el detalle de esta política en el documento **"44_Política_de_Control_de_Accesos".**