0. CONTROL DE CAMBIOS

Versión	Fecha	Descripción de la modificación
1	31/05/2024	Creación del Documento

1. RESPONSABILIDAD

RESPONSABLE:	**Chief Compliance Officer** **Administrative & Logistics Manager**

2. CONTENIDO

2.1 Objetivo

Definir los lineamientos para los proveedores que tienen acceso a la información de Digisoc o que gestionen información en nombre de la organización y así cumplan con los requisitos de seguridad de la información adecuados para proteger dicha información contra el acceso no autorizado, divulgación, alteración, pérdida o destrucción.

2.2 Alcance

Esta política se aplica a todos los proveedores, contratistas y terceros que proporcionan servicios, productos o soporte a Digisoc y/o que tengan acceso a información confidencial de la organización.

2.3 Roles y Responsabilidades

Administrative & Logistics Manager: Realizar evaluaciones de riesgo de los proveedores.

Purchasing Analyst: comunicar los requisitos de seguridad de la información a los proveedores.

Administrative Analyst: comunicar los requisitos de seguridad de la información a los proveedores.

Chief Compliance Officer: Realizar auditorías de seguridad de la información de los proveedores; así como la supervisión y actualización de la presente política.

Proveedores, Contratistas y terceros:

- Cumplir con todos los requisitos de seguridad de la información establecidos en esta política, en los contratos y/o acuerdos correspondientes.
- Informar a Digisoc cualquier incidente de seguridad de la información que pueda afectar a la información de la organización.
- Permitir y cooperar con las evaluaciones y auditorías de seguridad de la información realizadas por Digisoc.
- Definir y entregar a Digisoc los contactos relevantes, incluida una persona de contacto para las cuestiones de seguridad de la información cuando aplique.
- Entrega de los mecanismos de evidencia y certificaciones para los requisitos de seguridad de la información relevantes relacionados con los procesos de los proveedores, contratistas y/o terceros; un informe independiente sobre la efectividad de los controles cuando aplique.

2.4 Definiciones

La Organización / Digisoc: hace referencia al grupo de compañías vinculadas accionariamente directa o indirectamente, las cuales se encuentran distribuidas en las siguientes sociedades: DigiSOC S.A.S, Digiware Seguridad del Ecuador S.A, DigiSEC Corp., Digiware del Perú SAC, Digiware Security LLC, Digiware de Chile S.A. Digiware de Guatemala S.A.

Evaluación de Riesgo: Proceso de identificación, análisis y evaluación de riesgos de seguridad de la información.

2.5 Políticas

Esta política establece las directrices y procedimientos que la organización seguirá para asegurar la protección de la información en todas las relaciones con proveedores, contratistas y terceros. La seguridad de la información es crucial para mantener la integridad, confidencialidad y disponibilidad de los datos y para cumplir con las regulaciones y estándares aplicables.

2.5.1 Directrices generales

a) El responsable de la gestión de compras de Digisoc comunicara la presente política a los proveedores, contratistas y terceros de forma periódica.
b) La organización implementara procesos para abordar los riesgos de seguridad de la información asociados con el uso de productos y servicios proporcionados por los proveedores, contratistas y/o terceros.
c) El Administrative & Logistics Manager y el Chief Compliance Officer realizan de forma periódica la concientización al personal de la organización que interactúe con el personal del proveedor, contratista y tercero sobre los lineamientos de la presente política, el acceso a la información y transferencia de la misma.

2.5.2 Tipos de proveedores

Digisoc para la selección y contratación de proveedores, contratistas y terceros ha definido el M-AD-01 Manual de proveedores y contratistas, donde se identifican los tipos de proveedores de acuerdo con el riesgo que representa para las operaciones y actividades de la organización:

- **Riego Alto:** Son proveedores, contratistas y/o terceros que, por su nivel de complejidad por su actividad, acceso a la información y/o acceso a las instalaciones físicas de la organización debe tener mayor seguimiento y adherirse a la presente política.

- **Riego Medio:** Proveedores, contratistas y/o terceros que por sus actividades deban acceder a las instalaciones de la organización se debe tener seguimiento y adherirse a la presente política.
- **Riego Bajo:** Proveedores, contratistas y/o terceros que por sus actividades deban acceder a las instalaciones de la organización se debe tener seguimiento y adherirse a la presente política.

2.5.3 Selección de los proveedores

a) Todos los proveedores deben ser evaluados en función de su capacidad para cumplir con los requisitos de seguridad de la información de la organización de acuerdo con los procedimientos P-AD-01 Compras Internas y P-AD-03 Compras Proyectos.
b) Se debe realizar una evaluación de riesgos de seguridad de la información antes de la contratación de nuevos proveedores de riesgo Alto que tengan acceso a la información y a las instalaciones de la organización.
c) La selección de los proveedores, contratistas y/o terceros será realizada con los lineamientos definidos en los procedimientos P-AD-01 Compras Internas y P-AD-03 Compras Proyectos.

2.5.4 Acuerdos con los proveedores

a) Los proveedores deben firmar acuerdos de confidencialidad o contratos que incluyan cláusulas específicas de seguridad de la información.
b) Los acuerdos deben incluir las obligaciones de ambas partes para cumplir los requisitos de seguridad de la información pertinentes.
c) Dentro de la propuesta o documento equivalente el proveedor, contratista y/o tercero debe incluir la descripción de cómo se accederá a la información y los métodos utilizados según aplique.
d) Digisoc determinará el nivel de clasificación de la información que será compartida de acuerdo con las POL-SI-08 Política de Transferencia de Información y POL-SI-12 Política de Clasificación y Manejo de Información.
e) Entre las partes se deben definir los requisitos legales, estatutarios, reglamentarios y contractuales, incluida la protección de datos, el manejo de la información de identificación personal (PII), los derechos de propiedad intelectual y los derechos de autor y una descripción de cómo se garantizará que se cumplan de acuerdo con el servicio recibido por Digisoc.
f) Definir el proveedor, contratista y/o tercero los procedimientos para la autorización y revocación de la autorización para el uso de la información de Digisoc.
g) Incluir clausulas de indemnización y remediación por incumplimiento de los requisitos por parte de los proveedores, contratistas y/o terceros según aplique.

h) En caso de que el proveedor, contratistas y/o tercero deba subcontratar alguna actividad para la prestación de los servicios a Digisoc este debe acogerse a los mismos controles y políticas de Seguridad de la Información.
i) Definir el proceso de resolución de defectos y resolución de conflictos.

2.5.5 Acceso a la Información

a) El acceso a la información y o a las instalaciones de Digisoc estará determinado conforme a la solicitud de compra definida por el proceso y/o área solicitante.
b) Se deben implementar controles de acceso adecuados para asegurar que solo el personal autorizado del proveedor tenga acceso a la información de la organización.
c) El acceso a la información deberá estar determinado por el principio del menor privilegio-
d) La transferencia de información se realizará conforme a la POL-SI-08 Política de Transferencia de Información.
e) El acceso a las instalaciones físicas de Digisoc serán programadas y debe contar con el acompañamiento del responsable de la recepción del servicio.
f) Los proveedores, contratistas y/o terceros que tengan acceso a las instalaciones físicas deben seguir los lineamientos de las G-SI-02 Normas de seguridad para visitantes.

2.5.6 Evaluación de Proveedores

Digisoc ha definido en los procedimientos P-AD-01 Compras Internas y P-AD-03 Compras Proyectos las directrices para la realización de la Evaluación a proveedores, contratistas y terceros de forma anual para servicios y productos.

2.5.7 Auditoria de Proveedores

La organización realiza seguimiento, revisión y auditoría a la prestación de los servicios de los proveedores críticos asociados a la seguridad de la información, los cuales son canales de comunicación, centros de datos, fabricantes de plataformas de controles de seguridad de la información y aplicación de comunicación interna.

La auditoría a los proveedores críticos asociados a la seguridad de la información es responsabilidad del Chief Compliance Officer, quien anualmente realizará la verificación de cumplimiento de criterios con el formato F-SI-12; en caso de que el proveedor no cumpla con los criterios auditados se notificará al proceso Gestión Administrativa y al proceso propietario del servicio.

2.5.8 Cambio de Proveedores

Los cambios en los servicios proporcionados por los proveedores, contratistas y/o terceros pueden tener un impacto significativo en la seguridad de la información de la organización. Es

fundamental gestionar estos cambios de manera efectiva para asegurar que cualquier modificación en los servicios no comprometa la integridad, confidencialidad o disponibilidad de la información.

a) Los cambios de proveedores, contratistas y/o terceros puede darse por alguno de los siguientes factores:
   - Precio
   - Resultados de la Evaluación y Auditoria
   - Incumplimiento en los acuerdos
   - Funcionalidad de los servicios
   - Obsolescencia
   - Otros

b) Evaluación de Impacto: Antes de implementar cualquier cambio en los servicios del proveedor, realizar una evaluación de impacto para identificar posibles riesgos y determinar las medidas necesarias para mitigarlos.

c) Notificación previa: Notificar a todas las partes interesadas sobre los cambios en relación al proveedor, contratista, tercero, producto y/o servicio según aplique.

d) Pruebas y Validación: Realizar pruebas y validaciones para asegurar que los cambios en los servicios no introduzcan vulnerabilidades o afecten negativamente la seguridad de la información.

e) Documentación de cambios: Mantener una documentación detallada de todos los cambios en los servicios y/o productos que incluyan la evaluación del impacto, decisión tomada y acciones implementadas.

f) Comunicación de Cambios: Comunicar los cambios aprobados a todas las partes interesadas, incluyendo el personal interno y otros proveedores que puedan verse afectados.

2.5.9 Cambios de los servicios por parte de los Proveedores, contratistas y/o terceros

Los proveedores, contratistas y/o terceros continuamente están realizando mejoras en sus productos y/o servicios y es por ello por lo que Digisoc ha establecido los siguientes lineamientos para las partes interesadas:

a) Digisoc debe verificar periódicamente el desempeño del servicio para verificar el nivel de cumplimiento de los acuerdos.

b) El proveedor, contratista y/o tercero debe comunicar los cambios realizados y que puedan afectar los servicios y productos recibidos por Digisoc.

c) Digisoc validara que los cambios efectuados por los proveedores, contratistas y/o terceros no afecten la prestación de los servicios ofrecidos; así como la alineación a la mejora continua de los servicios, los controles nuevos o modificados para resolver incidentes de seguridad de la información y mejorar la misma.

d) Identificar vulnerabilidades de seguridad de la información y gestionarlas por parte del proveedor, contratista y/o tercero en relación con el cambio ejecutado en los servicios y productos.

2.5.10 Evaluación de los Riesgos con los proveedores

La evaluación de riesgos de los proveedores, contratistas y terceros, así como de los servicios y productos adquiridos por Digisoc es un proceso fundamental para asegurar que los proveedores cumplan con los estándares de seguridad de la información de la organización.

Para la evaluación de los riesgos con los proveedores Digisoc ha definido los siguiente lineamientos para su realización:

a) Digisoc de forma anual identifica, evalúa y define los planes de tratamiento de los riesgos asociados a la gestión de compras incluyendo los proveedores, contratistas y terceros mediante la ejecución del procedimiento P-SG-06 Gestión de Riesgos.
b) Anualmente el área de Compras realiza la evaluación a los proveedores de bienes y/o servicios donde se revisa los riesgos individuales para cada uno.
c) Cuando la organización define un cambio de un proveedor y/o selección de un nuevo servicio el proceso de Gestión Administrativa y el área responsable realizan una evaluación general de los riesgos y afectaciones que puede llegar a tener la prestación de los servicios de Digisoc.

2.5.11 Seguridad de la Información en la cadena de suministro

La seguridad de la información en la cadena de suministro es esencial para garantizar que todos los proveedores, contratistas y/o terceros mantengan un nivel adecuado de seguridad de la información. La cadena de suministro incluye todas las entidades externas que proporcionan bienes y servicios que afectan directa o indirectamente a la organización.

a) Digisoc definirá los productos y/o servicios de TIC que se deba aplicar los controles de la cadena de suministro.
b) Según aplique se debe solicitar a los proveedores de productos TIC:
   - Información que describa los componentes de software utilizados en los productos.
   - Información sobre las funciones de seguridad implementados en el producto y la configuración requerida para su operación segura.

c) Digisoc contara con un proceso para el monitoreo y método aceptable para validar que los productos y servicios de TI recibidos cumplen con los requisitos de seguridad establecidos.
d) Se debe solicitar garantías de los productos TIC y que estas alcancen los niveles de seguridad requeridos.

e) Definir mecanismos de comunicación para compartir información sobre la cadena de suministro y cualquier posible problema y compromiso entre la organización y los proveedores.
f) Los productos de TIC deben adquirirse de fuentes acreditadas.

2.5.12 Terminación segura de la relación con el proveedor

La terminación de la relación con un proveedor debe gestionarse de manera que se proteja la información de la organización y se mitiguen los riesgos asociados. Este proceso asegura que los datos sean devueltos o destruidos de manera segura, y que los accesos y privilegios sean revocados adecuadamente.

Digisoc ha definido las siguientes directrices para la finalización de la relación con proveedores, contratistas y terceros:

a) Al momento de la finalización de la relación con los proveedores, contratistas y/o terceros se debe retirar la totalidad de los accesos a la información y los accesos físicos de la organización según corresponda.
b) Notificar al proveedor con antelación adecuada sobre la terminación de la relación y planificar las acciones necesarias para asegurar una transición segura.
c) Asegurar que toda la información de la organización en posesión del proveedor, contratista y/o tercero sea devuelta o destruida de manera segura y verificable.
d) Actualizar todos los registros de acceso y documentación de seguridad para reflejar la terminación de la relación con el proveedor.

ELABORÓ: Maria Ximena Uribe	**REVISÓ:** Maria Ximena Uribe	**APROBÓ:** John Galindo
CARGO: Chief Compliance Officer	**CARGO:** Chief Compliance Officer	**CARGO:** CEO