	Sistema Integrado de Gestión			
ATENTO	PO-COM-01	Seguridad de la Información con Proveedores	v.03	10.09.2024
Elaborado por:	José Israel Ayala – jefe de procesos			10.09.2024
Revisado por:	Alvaro Herrera – jefe de Compras Javier Leandro Suarez – Gerente de Tecnología			10.09.2024
Aprobado por:	Miguel López - director País			10.09.2024

1. TABLA DE EDICIONES

N° Versión	Modificación	Fecha
V.01	Edición Inicial	06.06.2019
V.02	Se realiza revisión de la política, se corrigen los nombres de las políticas de referencias y actualización del elaborador y revisor de la política.	18.02.2021
v.03	Se realiza revisión general de la política	10.09.2024

2. OBJETIVO Y ALCANCE

Definir y dar a conocer a nuestros proveedores y a los diferentes procesos de la organización las políticas de seguridad de la información de compras de Atento Colombia, creando conciencia acerca de la importancia de preservar la seguridad de la información y generando el compromiso por parte de nuestros proveedores para garantizar la confidencialidad, integridad y disponibilidad de la información.

El presente documento aplica a todos los proveedores que prestan servicios a Atento Colombia y que tienen acceso físico o remoto a sitios, equipos y dispositivos que procesan información clasificada en la compañía como reservada o restringida, las políticas aplican y son de estricto cumplimiento desde la negociación, durante la vigencia del contrato y sus correspondientes prórrogas.

3. REFERENCIAS

- P-14 Política de Compras.
- PO TEC SEG 001 Seguridad de la información
- PR TEC SEG 031 Identificación y reporte de incidentes de seguridad de la información.
- PR TEC SEG 050 Gestión de Incidentes de Seguridad de la Información
- PR TEC 001 Administración de cambios.

4. VOCABULARIO

N°	Concepto	Descripción
01	Evento o incidente de seguridad de la información	Acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información, que compromete la confidencialidad, integridad o disponibilidad, así como la legalidad y confiabilidad de esta.
02	Eventos 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 la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.
03	Incidente	Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. También se define como un ataque electrónico deliberado a los sistemas de comunicaciones o procesamiento de información.
04	Información Reservada	Información de alta sensibilidad que debe ser protegida. El acceso a ella debe tener límites, aún dentro de Atento. Su modificación o divulgación sin autorización puede perjudicar seriamente a la empresa y/o sus clientes, impactando negativamente las finanzas, la reputación e incumpliendo compromisos legales o contractuales.

05	Información Restringida	Información sensible que puede ser interna de un área específica de Atento o referente a un proyecto. Solamente tendrá acceso controlado un grupo reducido de personas, ya que su difusión puede poner en peligro el buen término de una operación o afectar negativamente los intereses de la compañía, sus clientes o empleados.
06	Información Uso Interno	Información que no es sensible si es divulgada dentro de Atento, pero que puede causar un impacto negativo a la empresa, sus clientes o empleados; Otorgando ventajas competitivas si es conocida externamente. Su circulación está limitada a funcionarios de Atento y contratistas.

5. DESARROLLO

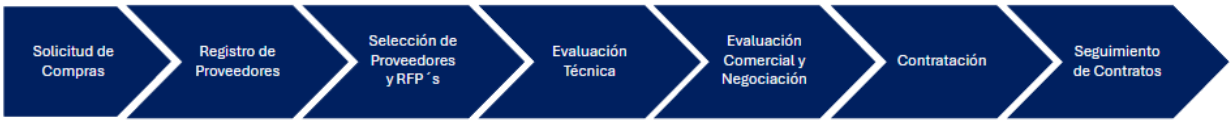
5.1 Consideraciones Generales

➢ **Tipos De Proveedores**

- **Proveedores sin acceso a información restringida.** Proveedores que brindan bienes o servicios pero que por el tipo de prestación no requieren acceso a información restringida de la compañía, entre ellos se encuentran las empresas de servicios públicos, servicios generales, mantenimiento de infraestructura (no relacionado con tecnología o redes de comunicación), proveedores de alimentos, etc.
- **Proveedores de servicios tecnológicos.** Aquellos que nos ofrecen servicios como alojamiento web, emisión de certificados, servicio de pasarelas de pago, servicios de almacenamiento en la nube, servicios de soporte informático (tanto presencial como remoto), etc.
- **Suministradores de productos tecnológicos.** Incluyen todos aquellos dónde adquirimos los dispositivos, los componentes hardware y las aplicaciones informáticas.
- **Proveedores de servicios no tecnológicos pero que acceden a datos corporativos.** Tales como proveedores de servicios de auditoría, servicios jurídicos o legales, servicios financieros, viajes, transporte, publicidad y marketing, etc.

➢ **Proceso Y Ciclo De Vida De Relaciones Con Proveedores**

Atento a definido la política P-14 Política de Compras, en donde se establece la gestión de la relación con proveedores y su ciclo de vida:



➢ **Tipos De Acceso Permitidos A Proveedores**

Nuestros proveedores, en función del producto o servicio que suministran, pueden tener acceso a los siguientes tipos de información definidas por Atento Colombia: Reservada, Restringida, Uso Interno y Publica, el área solicitante y el área de compras deberán definir los controles adecuados para proteger la confidencialidad, integridad y disponibilidad de la información que manipule o a la que tenga acceso el proveedor. Los controles pueden ser uno o una combinación de los siguientes:

- Cláusula de confidencialidad durante la negociación.
- Cláusula o acuerdo de confidencialidad en el contrato.
- RFP.
- Control de cambios – En caso de mantenimientos o implementaciones que puedan afectar plataformas críticas.
- Autorizaciones según acceso permitido.

Otros controles específicos son:

- **Gestión De Prevención De Riesgos De Proveedores**
  Atento puede solicitar información sobre la gestión de prevención de riesgos a sus proveedores, como la matriz de riesgos, la política de gestión de prevención de riesgos, entre otros, si considera que se trata de un proveedor crítico, por la clasificación de información que maneja o el tipo de acceso permitido.

5.2. Acceso A Zonas Seguras O Restringidas

Los proveedores que ingresan a áreas identificadas como seguras dentro de las instalaciones de Atento Colombia en las cuales se procesa información crítica del negocio deben proporcionar sus datos para el correspondiente registro en el libro o minuta de control de acceso al sitio y estar siempre con el acompañamiento y supervisión del responsable del proceso.

Durante su permanencia en las zonas seguras los proveedores deben mantener un óptimo comportamiento y tener el cuidado requerido con los recursos tecnológicos, sistema eléctrico y cableado de red. Estos elementos deben ser protegidos rigurosamente ante cualquier riesgo de daño accidental o intencional. Por lo tanto, se deben tomar las precauciones necesarias con el manejo de líquidos, fuentes de combustión o cualquier otro elemento que pueda causar algún tipo de accidente.

Está prohibido el ingreso de celulares, cámaras, dispositivos USB, discos duros externos o cualquier otro dispositivo que pueda permitir el registro y/o extracción de información que se procesa en estas áreas. Ningún proveedor podrá sin previa autorización escrita o solicitud por parte del encargado o responsable por parte de Atento Colombia realizar instalaciones, desconexiones, modificaciones, reubicaciones y reparaciones de equipos de cómputo, líneas de comunicación o telefónicas, o cualquier elemento de la infraestructura tecnológica perteneciente a la Compañía.

Se deben evitar situaciones riesgosas, como fumar, comer o beber cerca de los computadores o equipos tecnológicos que puedan afectar el buen funcionamiento de los equipos ubicados dentro de nuestras instalaciones.

Ningún equipo o dispositivo informático de propiedad de Atento Colombia o que se encuentre bajo su responsabilidad como servidores, switches, routers, impresoras, computadores, discos duros, etc., podrá ser retirado de las instalaciones físicas de la Compañía, a menos que esté autorizado en forma previa y escrita por parte de la Gerencia de Tecnología.

5.3. Acceso A Equipos Y Servidores

Los usuarios y contraseñas asignados al Proveedor o a sus representantes para ingreso a dispositivos, equipos y servidores sobre los cuales prestan sus servicios deben estar registrados en los sistemas de Atento Colombia con su respectiva información de soporte. Dichas credenciales son de uso personal e intransferible. Por ningún motivo se deben compartir o prestar a terceras personas.

El proveedor debe mostrar en todas sus acciones operativas un comportamiento profesional y ético, abstenerse de utilizar sus conocimientos y capacidades técnicas para facilitar accesos no autorizados o hacer vulnerable la plataforma tecnológica de Atento Colombia.

Es responsabilidad del proveedor velar por el buen estado de los equipos de cómputo y/o dispositivos que le asigne la Compañía para el cumplimiento de su gestión.

5.4. Acceso A Redes

No está permitido el ingreso a las redes y servidores internos de Atento Colombia por parte de proveedores y clientes desde sitios remotos haciendo uso de redes públicas o redes propias instaladas y administradas por ellos o por terceros.

En situaciones en las cuales se requiera que el proveedor utilice y conecte a la red de Atento Colombia equipos de su propiedad para el desempeño de sus funciones dentro de las instalaciones de la Compañía, se debe contar con la correspondiente aprobación por parte del área de seguridad de la información y garantizar el cumplimiento de los requisitos mínimos de seguridad como son:

- Sistema operativo actualizado y parchado a nivel de seguridad.
- Sistema antivirus instalado y actualizado, última versión del navegador a internet y no tener instalado software que permita realizar actividades ilícitas o ajenas a la prestación del servicio.

El acceso remoto a las redes y sistemas de Atento Colombia por parte de los proveedores se debe realizar mediante el uso de una VPN Site to Client que utilice como control de acceso doble factor de autenticación.

La VPN y los permisos de conexión requeridos deben ser solicitados a través del líder del proceso en Atento, con su respectiva justificación y su aprobación estará sujeta a la previa revisión del cumplimiento de requisitos internos y firma de los acuerdos de confidencialidad respectivos por parte del proveedor.

5.5. Uso De Software Y Licenciamiento

Está prohibido instalar software que no se encuentre debidamente licenciado y/o autorizado por parte de Atento Colombia. En caso de tratarse de software en demostración, es necesario contar con un documento de autorización emitido por el fabricante o distribuidor autorizado y la aprobación previa y de forma escrita de la Gerencia de Tecnología.

No se permite instalar o copiar software sin autorización de la Gerencia de Tecnología. El software licenciado por Atento Colombia sólo puede ser utilizado en equipos propiedad de la de la Compañía o que estén bajo su control.

El proveedor es responsable y debe tener constancia del permiso de uso de todo el software instalado en los equipos que le pertenezcan y que se encuentren dentro de las instalaciones de Atento Colombia para la gestión de la actividad contratada.

5.6. Correo Electrónico Y Transferencia De Información

El medio de comunicación y la transferencia de información clasificada como pública (No confidencial), entre Atento y sus proveedores se debe realizar a través de cuentas de correo electrónico corporativo, es decir pertenecientes al dominio del proveedor o al dominio de Atento Colombia. En ningún caso se deben utilizar cuentas personales o de dominios como Gmail, Hotmail, yahoo, entre otras, para realizar intercambio de información.

Cuando se requiera transferir información clasificada como, restringida o reservada, es necesario acordar e implementar mecanismos de encripción sólidos que garanticen la seguridad de los datos transferidos por correo electrónico, ya que la información viaja por redes públicas no seguras.

Otra alternativa es transferir los datos haciendo uso de un sitio FTPS. El sitio FTPS debe contar con los controles de acceso de usuarios, con asignación de cuentas de acceso personalizadas y deben estar definidos los permisos de lectura, escritura y eliminación para cada Usuario. Si es posible, se debe tener un control a nivel de direcciones IP de origen, utilizadas por Atento o el proveedor, con el fin de que se pueda diferenciar y controlar el acceso al servidor y solamente se suba al sitio información relacionada con el negocio.

El repositorio debe ser utilizado para almacenar información de manera temporal, es decir solamente debe funcionar como mecanismo de trasferencia entre las partes y no de solución de almacenamiento permanente.

5.7. Continuidad Del Servicio

El proveedor está obligado a diseñar, documentar, implementar, probar y mantener actualizado en forma periódica un plan de continuidad de negocio que garantice la prestación de los servicios contratados con Atento Colombia. El plan debe contar con los recursos y procedimientos necesarios para afrontar y controlar eventos adversos que puedan generar interrupción o alto impacto en los servicios prestados.

- **Cumplimiento Regulatorio**

  Los proveedores deben cumplir con las políticas de seguridad, leyes, regulaciones y normas nacionales e internacionales referentes a la seguridad de la información que apliquen dentro del alcance y objeto de los servicios contratados con Atento.

  Ante cualquier violación de las disposiciones especificadas en la normatividad descrita, Atento Colombia se reserva el derecho de tomar las medidas, legales y pecuniarias a que haya lugar, que podrían incluso llevar

a la terminación y/o cancelación de contratos o vínculos comerciales y de cualquier otra naturaleza, que se mantenga con el proveedor. Los daños y perjuicios que el proveedor, ocasione a Atento Colombia, en desarrollo de la presente obligación, serán reconocidos y pagados directamente por el proveedor, totalmente a sus expensas. Por otra parte, el proveedor se obliga a resarcir a Atento Colombia, defenderlo y ampararlo ante cualquier responsabilidad, daño o perjuicio, por causa de reclamos o demandas que surjan en ocasión al incumplimiento a lo aquí establecido.

- **Acceso A Documentos Del Área Jurídica**
  El área jurídica de Atento Colombia maneja, entre otros documentos, contratos, información litigiosa y contenciosa con clientes y proveedores para información que se comparte con proveedores debe existir cláusula de confidencialidad en los contratos.

5.8. Información Compartida En Auditorías Externas O Internas
Debe existir cláusula o acuerdo de confidencialidad con el proveedor.

5.9. Procesos Y Procedimientos Para Hacer Seguimiento Del Cumplimiento De Los Requisitos De Seguridad De La Información.
El área solicitante del servicio o producto deberá realizar seguimiento al cumplimiento de los requisitos de seguridad de la información y reportar eventos o incidentes de seguridad generados por el proveedor de llegar a evidenciarlos.

5.10. Manejo De Incidentes Y Contingencias Asociadas Con El Acceso De Proveedores
En el caso de detectarse alguna incidencia o evento de seguridad, se seguirá PR TEC SEG 031 Identificación y reporte de incidentes de seguridad de la información, PR -TEC SEG 050 Gestión de Incidentes de Seguridad de la Información

6. Revisión De La Política

Esta política será revisada mínimo cada doce meses con el fin de asegurar la vigencia y el cumplimiento. También se encuentra dispuesta a modificaciones ante cambios en la estructura organizacional para la administración de la seguridad, siempre y cuando cuente con la revisión del comité de seguridad y/o aprobación del director País.