




MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

ADAMANTINE

ADAMANTINE 	CONFIDENCIALIDAD Documento y material que diseña y realiza Grupo ADAMANTINE sobre el que tiene derechos de propiedad. De conformidad a lo dispuesto en el artículo 87-D de la Ley General de Organizaciones y Actividades Auxiliares de Crédito, queda prohibido divulgar el contenido o reproducir parte o el total del documento, sin mencionar y reconocer que Grupo ADAMANTINE es el legítimo dueño y tener una autorización por escrito para tal acción.		
	Versión: 1.0	Vigente a partir de: 15-07-2019	Próxima revisión: 15-07-2020


AUTORIZACIONES MANUAL DE POLÍTICAS DE SEGURIDAD

Firma Responsable del Procedimiento

Nombre: Gerardo Enrique Butron Medina

Puesto: Gerente de Infraestructura TI

Firma y Fecha:

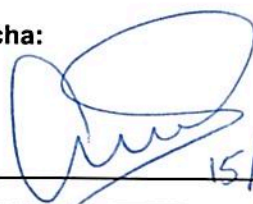
 15/07/2019

Firma de quien Autoriza


Nombre: Andres Medina Aguilar

Puesto: Subdirector de Sistemas


Firma y Fecha:


 15/07/2019

Firmas de Autorización

Nombre	Cargo	Fecha de Firma	Firma
Miguel Lopez Sainz	Director de Finanzas	15/07/19	

Firma de Involucrados y área que elabora

Nombre	Cargo	Fecha de firma	Firma
Diana Karina Velázquez Pérez	Analista de Procesos	15/07/2019	

ADAMANTINE 	CONFIDENCIALIDAD Documento y material que diseña y realiza Grupo ADAMANTINE sobre el que tiene derechos de propiedad. De conformidad a lo dispuesto en el artículo 87-D de la Ley General de Organizaciones y Actividades Auxiliares de Crédito, queda prohibido divulgar el contenido o reproducir parte o el total del documento, sin mencionar y reconocer que Grupo ADAMANTINE es el legítimo dueño y tener una autorización por escrito para tal acción.		
Versión: 1.0	Vigente a partir de: 15-07-2019	Próxima revisión: 15-07-2020	Código: MAP-DAM-0304

I. OBJETIVO

Establecer los lineamientos necesarios para contar con la protección de la información y los bienes informáticos que garantice la continuidad de los sistemas de información, minimizar los riesgos en caso de un incidente o falla, proteger los bienes informáticos de la empresa y la tecnología utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con la finalidad de mantener la confidencialidad, integridad y disponibilidad de la información

Para ser efectiva y aplicable la presente política de seguridad de la información se deberá contar con el apoyo de la Alta Dirección.


El incumplimiento a las políticas de seguridad de la información tendrá como resultado la aplicación de sanciones, de acuerdo a la magnitud y características de las políticas incumplidas.

II. ESPECIFICACIONES GENERALES

2.1 Revisión de la Política de Seguridad de la Información

1. Todos los colaboradores que usen o intercambien información de la empresa, deben de dar cumplimiento a las políticas de seguridad de información establecidas en este documento.
2. El responsable de seguridad de la información es la Subdirección de Sistemas, a la Gerencia de Infraestructura de TI como la parte ejecutora de acciones o modificaciones en temas de seguridad informática y el Subdirector de sistemas como autorizador para la toma de decisiones.
3. El Gerente de Infraestructura, realizará revisiones de las políticas que lo requieran con la finalidad de garantizar el cumplimiento de la misma, considerando los siguientes criterios:
 - a) Cuando ocurra un incumplimiento a las políticas de seguridad descritas en este manual
 - b) Cuando se hagan observaciones derivadas de Auditorías Externas o internas
 - c) Cuando se detecten amenazas o vulnerabilidades de los sistemas de información
 - d) A solicitud de las autoridades regulatorias para dar cumplimiento de las disposiciones
4. Todos los colaboradores deben brindar apoyo para la revisión y cumplimiento de las políticas y requisitos de seguridad aplicables.



	<p align="center">CONFIDENCIALIDAD</p> <p>Documento y material que diseña y realiza Grupo ADAMANTINE sobre el que tiene derechos de propiedad. De conformidad a lo dispuesto en el artículo 87-D de la Ley General de Organizaciones y Actividades Auxiliares de Crédito, queda prohibido divulgar el contenido o reproducir parte o el total del documento, sin mencionar y reconocer que Grupo ADAMANTINE es el legítimo dueño y tener una autorización por escrito para tal acción.</p>		
<p>Versión: 1.0</p>	<p>Vigente a partir de: 15-07-2019</p>	<p>Próxima revisión: 15-07-2020</p>	<p>Código: MAP-DAM-0304</p>

2.2 Infraestructura de la Seguridad de la Información

2.2.1 Asignación de Responsabilidades en Materia de Seguridad de la Información

1. La política de seguridad de la información es de aplicación obligatoria para todos los Colaboradores de la empresa, cualquiera que sea su posición, el área a la cual se encuentre asignado y cualquiera que sea su nivel de las tareas que desempeñe, por lo que deberán registrarse bajo el criterio de confidencialidad, integridad y disponibilidad con base a los acuerdos firmados al momento de ingresar a la Z<empresa.
2. La Dirección General y la Subdirección de Sistemas aprueban esta política y son los únicos facultados para la autorización de sus modificaciones

2.2.2 Acuerdos de Confidencialidad

1. Para proteger la información se deberán firmar acuerdos de confidencialidad y de no divulgación tanto a los colaboradores como a terceros, para proteger aquella información que se considere sensible y confidencial, considerando los siguientes criterios:
 - a) No divulgar ni comunicar información sensible o técnica a terceros
 - b) Impedir la copia o revelación de información sensible o confidencial a terceros
 - c) Restringir el acceso a la información confidencial o sensible en la medida que sea razonable para en cumplimiento de sus tareas
 - d) Considerar las sanciones correspondientes en caso de incumplimiento

2.3 Relaciones con Terceros


2.3.1 Identificación de Riesgos del Acceso a Terceras Partes

1. Deberá realizarse una evaluación de riesgos por parte del responsable-administrador del bien o servicio informático que provee el acceso y en conjunto con el responsable de seguridad de la información identificarán cuales son los controles específicos que deberán de usarse antes de conceder el acceso a un tercero.

Los aspectos mínimos a considerar son:

- a) El tipo de acceso: lógico y/o físico
- b) El valor del recurso o bien informático al que se dará acceso



ADAMANTINE 	CONFIDENCIALIDAD Documento y material que diseña y realiza Grupo ADAMANTINE sobre el que tiene derechos de propiedad. De conformidad a lo dispuesto en el artículo 87-D de la Ley General de Organizaciones y Actividades Auxiliares de Crédito, queda prohibido divulgar el contenido o reproducir parte o el total del documento, sin mencionar y reconocer que Grupo ADAMANTINE es el legítimo dueño y tener una autorización por escrito para tal acción.		
Versión: 1.0	Vigente a partir de: 15-07-2019	Próxima revisión: 15-07-2020	Código: MAP-DAM-0304

- c) Los privilegios de acceso a la información que serán otorgados y monitoreados
- d) La protección de datos personales en caso de acceso a los sistemas de información

2.4 Administración de Equipos de Computo

2.4.1 Uso aceptable de los Equipos de Cómputo

1. El uso de los equipos de cómputo, deberá cumplir como mínimo los siguientes criterios:
 - a) Los colaboradores deberán usar los equipos de acuerdo con las presentes políticas de seguridad de la información
 - b) Evitando la pérdida de la información sensible o confidencial manejada por el usuario
 - c) Reportando cualquier pérdida, robo o extravío de los equipos

2.5 Terminación de relación laboral o cambio de puesto de trabajo

2.5.1 Devolución de Activos

1. Es responsabilidad de los colaboradores que terminen su relación laboral con la empresa o que cambien su puesto de trabajo hacer la correcta devolución del equipo de cómputo que se le haya asignado y deberá ser entregado al equipo de Soporte TI.

2.5.2 Baja de los privilegios de acceso


1. El Gerente de Infraestructura TI deberá cerciorarse y validar que se dieron de baja los privilegios y cuentas de acceso a aquellos colaboradores que sean dados de baja definitivamente de los sistemas y servicios, la validación periódica de la baja de accesos y privilegios, lo cual permitirá reducir los riesgos de intrusiones o daños a la información sensible y confidencial.

2.6 Seguridad física y ambiental

2.6.1 Áreas Seguras

1. Es responsabilidad de la Gerencia de Infraestructura TI validar que el Centro de Datos mantenga las condiciones adecuadas para garantizar la operación de todos los elementos tecnológicos y asegurar la continuidad de las actividades críticas de la empresa.
2. La seguridad física para el Centro de Datos, se llevará a cabo por medio de mecanismos de control de acceso con base a la lista de Colaboradores autorizados.



ADAMANTINE 	<p align="center">CONFIDENCIALIDAD</p> <p>Documento y material que diseña y realiza Grupo ADAMANTINE sobre el que tiene derechos de propiedad. De conformidad a lo dispuesto en el artículo 87-D de la Ley General de Organizaciones y Actividades Auxiliares de Crédito, queda prohibido divulgar el contenido o reproducir parte o el total del documento, sin mencionar y reconocer que Grupo ADAMANTINE es el legítimo dueño y tener una autorización por escrito para tal acción.</p>		
Versión: 1.0	Vigente a partir de: 15-07-2019	Próxima revisión: 15-07-2020	Código: MAP-DAM-0304

2.7 Seguridad de los equipos

2.7.1 Protección de Equipos

1. La medida para proteger los equipos de cómputo, son las siguientes:
 - a) Utilizar medidas para proteger los equipos como son el uso de contraseñas al arranque de equipo
 - b) Bloquear periféricos que permitan la salida de información sensible o confidencial

2.7.2 Seguridad de los equipos fuera de las Instalaciones

1. Para el caso de aquellos colaboradores que requieran usar sus equipos fuera de las instalaciones u oficinas, deberá entregar al área de vigilancia el formato de Entrada y Salida de equipo debidamente requisitado y autorizado.

2.7.3 De la atención y seguimiento a la información


1. Para evitar el uso indebido de la información, se deberán seguir las siguientes medidas:
 - a) Evitar la pérdida u olvido de información sensible confidencial en equipos o medios de almacenamiento portátiles ya sea personales o de proveedores.
 - b) Evitar dejar información sensible o confidencial en impresoras, equipos multifuncionales, etc., o cualquier otro medio electrónico o impreso.

2.8 Administración de Comunicaciones y Operaciones

1. En caso de que los Colaboradores que usen o intercambien información, detecten algún incidente, deberán registrarlo en el sistema de tickets para su correcta atención.

2.8.1 Gestión de Instalaciones Externas

1. En el caso de contar con instalaciones externas para la continuidad del negocio, y los planes de pruebas o plan de recuperación de desastres, el sitio alternativo para la operación deberá cumplir con los siguientes criterios:

ADAMANTINE 	<p align="center">CONFIDENCIALIDAD</p> <p>Documento y material que diseña y realiza Grupo ADAMANTINE sobre el que tiene derechos de propiedad. De conformidad a lo dispuesto en el artículo 87-D de la Ley General de Organizaciones y Actividades Auxiliares de Crédito, queda prohibido divulgar el contenido o reproducir parte o el total del documento, sin mencionar y reconocer que Grupo ADAMANTINE es el legítimo dueño y tener una autorización por escrito para tal acción.</p>		
Versión: 1.0	Vigente a partir de: 15-07-2019	Próxima revisión: 15-07-2020	Código: MAP-DAM-0304

- a) Usar las mismas políticas de seguridad de la información
- b) Mantener el mismo nivel de operación de los servicios de TI y del negocio
- c) Evitar la pérdida o daño de la información en las instalaciones externas

2.9 Mantenimiento

2.9.1 Resguardo de la Información

1. Es responsabilidad del Gerente de Infraestructura TI
 - a) Realizar los respaldos correspondientes previo a que se efectúe el mantenimiento y mantener los respaldos bajo resguardo en lugar seguro
 - b) Registrar cualquier cambio en la configuración del equipo al que se le realice el mantenimiento

2.10 Administración de la Red

2.10.1 Controles de Redes

1. Es responsabilidad del Gerente de Infraestructura administrar y llevar el control de las redes y comunicaciones, por lo que no se permitirá que otra área sin autorización contrate, administre o instale dispositivos o servicios que interfieran con la red y la infraestructura de la empresa.
2. Sólo el Gerente de Infraestructura, será quien tenga los mecanismos de activación de puertos, conexiones y comunicaciones de la infraestructura de red.

2.11 Administración y Seguridad de los Medios de Almacenamiento

2.11.1 Administración de Medios Informáticos Removibles:


1. Los puertos USB , lectores de CD, infrarrojo, bluetooth y cualquier unidad de almacenamiento externa de todos los equipos deben estar deshabilitados.

2.12 Intercambios de Información y Software

2.12.1 Seguridad del Correo Electrónico

1. Se deberá identificar los tipos y medidas de seguridad que se establecerán en el uso de correo electrónico corporativo, por parte de la Subdirección de Sistemas y el Gerente de



	<p align="center">CONFIDENCIALIDAD</p> <p>Documento y material que diseña y realiza Grupo ADAMANTINE sobre el que tiene derechos de propiedad. De conformidad a lo dispuesto en el artículo 87-D de la Ley General de Organizaciones y Actividades Auxiliares de Crédito, queda prohibido divulgar el contenido o reproducir parte o el total del documento, sin mencionar y reconocer que Grupo ADAMANTINE es el legítimo dueño y tener una autorización por escrito para tal acción.</p>		
<p align="center">Versión: 1.0</p>	<p align="center">Vigente a partir de: 15-07-2019</p>	<p align="center">Próxima revisión: 15-07-2020</p>	<p align="center">Código: MAP-DAM-0304</p>

Infraestructura TI, para cumplir con las políticas de seguridad de información descritas en este manual

2.12.2 Política de Correo Electrónico

1. La siguiente política aplica para todos los colaboradores que hagan uso de correo electrónico de la empresa:
 - a) No podrán hacer uso de correo electrónico para fines personales o que pongan en riesgo la imagen, confidencialidad o valores de la empresa.
 - b) Se deberán filtrar aquellos mensajes o cadenas tipo spam para evitar la saturación o pérdida del servicio por parte del administrador de correo electrónico.
 - c) No se permite el envío de correos masivos o cadenas cuyo contenido sean ventas, propaganda política, contenido adulto, software o programas anexos, que puedan poner en riesgo los sistemas, equipos y/o la operación del negocio.
 - d) En caso de requerir la transferencia de archivos de gran tamaño deberán solicitar a la Subdirección de Sistemas el apoyo para realizar esta transmisión de manera segura.

2.12.3 Otras Formas de Intercambio de Información


1. Se deberán cumplir los siguientes criterios para el intercambio de información que pertenezca, se genere y sea propiedad de la empresa:
 - a) Cuidar y proteger la información sensible o confidencial
 - b) Evitar compartir datos personales de colaboradores y/o clientes
 - c) Utilizar medios electrónicos seguros proporcionados y monitoreados por la Gerencia de Infraestructura y Subdirección de Sistemas

2.13 Control de Accesos

2.13.1 Requerimientos para el Control de Accesos

1. Será responsabilidad del Gerente de Infraestructura implementar los controles de acceso a la información y a la infraestructura.
2. Llevar a cabo el monitoreo de todos los accesos de los colaboradores y proveedores a los



	<p style="text-align: center;">CONFIDENCIALIDAD</p> <p>Documento y material que diseña y realiza Grupo ADAMANTINE sobre el que tiene derechos de propiedad. De conformidad a lo dispuesto en el artículo 87-D de la Ley General de Organizaciones y Actividades Auxiliares de Crédito, queda prohibido divulgar el contenido o reproducir parte o el total del documento, sin mencionar y reconocer que Grupo ADAMANTINE es el legítimo dueño y tener una autorización por escrito para tal acción.</p>		
<p>Versión: 1.0</p>	<p>Vigente a partir de: 15-07-2019</p>	<p>Próxima revisión: 15-07-2020</p>	<p>Código: MAP-DAM-0304</p>

sistemas de información.

- Sólo se otorgarán los accesos a aquellos sistemas que por las funciones del negocio sea necesario.

2.14 Administración de Accesos de Usuarios

2.14.1 Administración de Contraseñas Críticas

- Para la administración de cuentas y contraseñas críticas como las de los sistemas de servidores para el negocio, equipos de telecomunicaciones y seguridad, se deberán entregar y resguardar dichas cuentas y contraseñas por el Subdirector de Sistemas y el Gerente de Infraestructura TI, como medida preventiva en caso de pérdida o extravío, principalmente en caso de contingencia o riesgo inminente de falla en los servicios críticos de la operación de la empresa.

2.15 Responsabilidades del Usuario


2.15.1 Uso de Contraseñas

- Todos los colaboradores serán responsables del uso correcto de las contraseñas que les sean proporcionadas de los sistemas, equipos de computo y aplicativos para el desempeño de sus tareas y deberán cumplir lo siguiente:
 - No se permite prestar o compartir ninguna contraseña entre usuarios o terceros por ninguna razón técnica, operativa o administrativa.
 - Resguardar la confidencialidad de sus contraseñas, por lo que no deberán estar almacenadas en archivos de texto, anotadas en papel, libretas o cuadernos de notas y queda estrictamente prohibido sean visibles en notas pegadas en monitores, teclados o escritorios.

2.15.2 Equipos Desatendidos en las Áreas de Usuarios

- Para la protección de la información sensible o confidencial, será responsabilidad de los usuarios no dejar sus sesiones activas en su equipo de cómputo sin haberlo bloqueado.
- Evitar dejar su equipo desatendido, en caso que requiera moverse de su lugar deberá bloquearlo.



ADAMANTINE 	<p align="center">CONFIDENCIALIDAD</p> <p>Documento y material que diseña y realiza Grupo ADAMANTINE sobre el que tiene derechos de propiedad. De conformidad a lo dispuesto en el artículo 87-D de la Ley General de Organizaciones y Actividades Auxiliares de Crédito, queda prohibido divulgar el contenido o reproducir parte o el total del documento, sin mencionar y reconocer que Grupo ADAMANTINE es el legítimo dueño y tener una autorización por escrito para tal acción.</p>		
Versión: 1.0	Vigente a partir de: 15-07-2019	Próxima revisión: 15-07-2020	Código: MAP-DAM-0304

2.16 Control de Acceso a la Red

2.16.1 Política de Utilización de los Servicios de Red


1. Es responsabilidad de los Colaboradores de la empresa apegarse al control de acceso para la navegación web
2. Todo acceso a los servicios de red deberá estar justificado, autorizado y se limitará a las funciones o tareas que los usuarios tengan que realizar.


2.16.2 Autenticación de Usuarios para Conexiones Externas

1. Los servicios que requieren de conexiones externas deberán otorgarse sólo en caso de que esté plenamente justificado y autorizado el acceso.
2. Las conexiones externas por su naturaleza deberán estar limitadas en tiempo y recursos, por lo que deberán tener un tiempo de vigencia, para ampliar el periodo de uso deberán revisarse los permisos y tareas solicitadas
3. El Gerente de Infraestructura deberá implementar los mecanismos necesarios para la autenticación de usuarios en el caso de las conexiones externas o remotas, de acuerdo a las medidas de seguridad informática con base a las tecnologías que sean implementadas.

2.16.3 Acceso a Internet

1. El control de acceso a Internet estará a cargo de la Gerencia de Infraestructura por lo que establecerán los criterios de operación necesarios para el uso adecuado de este servicio.
2. Sólo se permitirá el acceso a Internet a aquellos usuarios que por sus funciones lo requieran previa autorización y justificación.
3. Se sancionará a aquellos colaboradores que infrinjan o evadan las medidas de seguridad haciendo uso indebido del acceso a Internet.
4. Se deberán usar herramientas automatizadas para el filtrado de contenido web, detección y bloqueo de intrusos, protección contra virus y sus variantes, como malware, spyware. etc.



ADAMANTINE 	CONFIDENCIALIDAD Documento y material que diseña y realiza Grupo ADAMANTINE sobre el que tiene derechos de propiedad. De conformidad a lo dispuesto en el artículo 87-D de la Ley General de Organizaciones y Actividades Auxiliares de Crédito, queda prohibido divulgar el contenido o reproducir parte o el total del documento, sin mencionar y reconocer que Grupo ADAMANTINE es el legítimo dueño y tener una autorización por escrito para tal acción.		
Versión: 1.0	Vigente a partir de: 15-07-2019	Próxima revisión: 15-07-2020	Código: MAP-DAM-0304

2.17 Trabajo Remoto.

2.17.1 Trabajo Remoto

1. La Subdirección de Sistemas sólo autorizará actividades de trabajo remoto, a aquellos colaboradores que soliciten y justifiquen que el acceso será estrictamente por cuestiones laborales, para lo cual deberá implementar los mecanismos de seguridad tomando en cuenta la necesidad de acceso remoto a los sistemas internos y protegiendo la confiabilidad e integridad de la información a la que se accederá y los medios de comunicación para el acceso a los sistemas.

2.18 Administración de la Continuidad del Negocio


2.18.1 Proceso de la Administración de la Continuidad

1. El Gerente de Infraestructura TI implementará un proceso controlado para el desarrollo y mantenimiento de la continuidad de los servicios críticos en la operación del negocio. El cuál deberá contemplar los siguientes aspectos clave de la administración de la continuidad:
 - a) Comprensión de los riesgos que enfrenta la empresa en términos de probabilidad de ocurrencia e impacto, incluyendo la identificación y priorización de los procesos críticos de del negocio
 - b) Comprensión del impacto que una interrupción puede tener en los procesos de negocio.
 - c) Elaboración y documentación de planes de continuidad del negocio de conformidad con la estrategia de continuidad acordada.

2.18.2 Elaboración e Implementación de los Planes de Continuidad de las Actividades

1. Es responsabilidad del Gerente de Infraestructura realizar pruebas y actualizar los planes de continuidad cuya periodicidad mínima será una vez al año



ADAMANTINE 	<p align="center">CONFIDENCIALIDAD</p> <p>Documento y material que diseña y realiza Grupo ADAMANTINE sobre el que tiene derechos de propiedad. De conformidad a lo dispuesto en el artículo 87-D de la Ley General de Organizaciones y Actividades Auxiliares de Crédito, queda prohibido divulgar el contenido o reproducir parte o el total del documento, sin mencionar y reconocer que Grupo ADAMANTINE es el legítimo dueño y tener una autorización por escrito para tal acción.</p>		
Versión: 1.0	Vigente a partir de: 15-07-2019	Próxima revisión: 15-07-2020	Código: MAP-DAM-0304

III. CONTROL DE CAMBIOS

Versión	Fecha de Actualización	Descripción del Cambio

