	POLITICA DE SEGURIDAD DE LA INFORMACION	VERSIÓN UNICA	Página I de I
		DISTRIBUCIÓN: UNICA COPIA EN LA RED	15-04-09

POLITICA: Seguridad de la Información.

Objetivo

Establecer niveles de seguridad en base al esquema normativo de seguridad de la información


Alcance

Se describen todas las normas, políticas y estándares que se aplicaran de manera obligatoria de parte del personal del Call Center, respecto a la seguridad informática para lograr un correcto uso de equipos de cómputo y aplicaciones tecnológicas


1. Personal autorizado.

1. Los funcionarios son capacitados en los temas de seguridad de la información.
2. El ingeniero crea los usuarios una vez se realice la solicitud por parte de Talento Humano, informando, campaña, nombre completo y ciudad, área, novedad de ingreso o retiro, fecha de creación y/o eliminación. La solicitud será atendida de manera inmediata. La clave debe tener mínimo catorce (14) caracteres, ser alfanumérica, debe tener números y letras, un carácter especial y mínimo una mayúscula.
3. Los funcionarios que tienen acceso a las bases de datos de cada campaña corresponden a los integrantes y coordinadores de cada campaña. Por lo tanto no tienen acceso lo demás integrantes de otra campaña.
4. El único que tiene acceso para realizar los respectivos backups es el Ingeniero de Sistemas. El cual lo realiza de manera diferencial y completa.
5. En caso de algún incidente o evento, como contingencia el Gerente custodia un sobre sellado las claves de acceso al cifrado del backup up, cabe resaltar que este sobre se abrirá, en el caso eventual que el Ingeniero no pueda emplearlas directamente.
6. Una vez se crea el usuario, el ingeniero valida roles y asigna los permisos al grupo de campaña.,

2. Control.

	POLITICA DE SEGURIDAD DE LA INFORMACION	VERSION UNICA	Página 2 de 1
		DISTRIBUCIÓN: UNICA COPIA EN LA RED	15-04-09

1. De acuerdo a los roles pre- establecidos, los Analistas de la campaña no tienen acceso a los siguientes dispositivos de salida:
 - USB
 - Quemador de CD
 - Internet
 - Messenger
 - Correo Electrónico
 - Redes Sociales
2. De acuerdo a los roles pre- establecidos Los coordinadores, no tienen acceso a los siguientes dispositivos de salida:
 - USB
 - Quemador de CD
 - Internet
 - Messenger
 - Redes Sociales
3. Está totalmente prohibido el uso de celulares, cámaras, portátiles por parte de los analistas de cartera y coordinadores.
 - Para el caso del correo electrónico, tendrán acceso solamente los coordinadores y los funcionarios del área administrativa (Gerencia, Administrativo, Tecnología, Recursos Humanos) .
 - En el caso de la campaña de ACH, por solicitud del cliente tiene acceso a correo electrónico los asesores de servicio.
4. Los coordinadores y el área Administrativos son los únicos habilitados para enviar impresiones y realizar escáner, los analistas no tienen este tipo de atributo.
5. Los analistas en el puesto de trabajo solo se cuenta con el equipo de Cómputo por lo tanto no tiene acceso a hojas y esferos que permitan la copia de algún tipo de información.
6. La impresora está conectada a un punto de red por lo tanto solo se puede configurar por un administrador.

	POLITICA DE SEGURIDAD DE LA INFORMACION	VERSIÓN UNICA	Página 3 de 1
		DISTRIBUCIÓN: UNICA COPIA EN LA RED	15-04-09

7. Solo se permite el acceso a áreas restringidas a personal debidamente carnetizado

3. Aclaraciones de la Seguridad de la Información.

- Como medida de seguridad y garantía de la efectividad, no se permite recibir ni realizar llamada personales.
- Cabe resaltar que se realiza monitoreo telefónico y se realiza grabación del 100% de las llamadas tanto inbaund como outbaund.
- Se tiene establecida en el contrato un acuerdo de confidencialidad, el cual se adjunta, firmado el día del ingreso y el cual posee copia cada empleado.

Cualquier incumplimiento por leve que sea de las políticas contenidas dentro del presente documento, será considerado como falta grave y por lo tanto tendrá lugar a su respectivo proceso disciplinario.