FIANZA LTDA
ASESORES FINANCIEROS

POLITICAS DE CALIDAD FIANZA LTDA.

AGENDA

FIANZA LTDA
ASESORES FINANCIEROS

1. Reglamento Políticas Internas para Contact Center.
2. Política de Cambio de Claves.
3. Política Control de Acceso
4. Política Back Up
5. Política de Manejo de Información
6. Política de Permisos
7. Política de Seguridad de la Información
8. Política de Usuarios
9. Política Bloqueo de Equipos.

FIANZA LTDA
ASESORES FINANCIEROS

OBJETIVO

"Describir las normas para proteger la seguridad de la información en el área del Contact Center."

- ✓ Informar las políticas y normas de convivencia y el manejo que los funcionarios o usuarios deben dar a los recursos del Contact Center, así como también sus responsabilidades en cuanto a la utilización de los mismos.

PÓLITICA CAMBIO DE CLAVES

FIANZA LTDA
ASESORES FINANCIEROS

1. Cuando se crea el usuario, se configura el sistema para que la primera vez que ingrese el usuario inmediatamente le pida cambio de clave.

2. La clave debe tener mínimo catorce caracteres , ser alfanumérica, tener números y letras, un carácter especial y minino una mayúscula

3. El sistema se configura para que pida cambio de clave cada 28 días, una vez se haya creado el usuario.

4. A los 3 intentos fallidos se bloquea automáticamente la clave.

PÓLITICA CAMBIO DE CLAVES

FIANZA LTDA
ASESORES FINANCIEROS

5. Las claves no deben corresponder al número de cédula ni al nombre

6. En el momento de la creación de las claves el sistema está configurado para que no permita aplicar las últimas 4 claves registradas en el sistema.

- *La única persona autorizada para crear y eliminar usuario es el Ingeniero de Sistemas, previa solicitud de Talento Humano.*

POLITICA DEL CONTROL DE ACCESO

FIANZA LTDA
ASESORES FINANCIEROS

Parámetros Generales:

El ingreso a la empresa está restringido por medio de un control de acceso biométrico. Para su uso se debe cumplir con los siguientes políticas:

1. Ningún funcionario podrá tener acceso a la empresa antes de las 6:20 a.m. ni después de las 8:45 p.m. debido a que el control biométrico está configurado para bloquearse fuera del rango horario descrito anteriormente.
preferencial…

2. Todos los funcionarios deberán registrar su huella al salir o ingresar a las instalaciones de la empresa, ya que estos registros serán usados para medir hora de entrada, salida, breaks, etc. Es imprescindible que por cada entrada o salida la huella quede en el sistema, por lo tanto no se admitirá que su acceso no quede consignado, aludiendo que el primer funcionario que entró lo hizo.
llamada…

3. Si por algún motivo el personal de la empresa debe laborar en un horario diferente al estipulado, deberá informarlo ante recursos humanos por lo tanto ser autorizado, para que el personal de sistemas configure el control biométrico.

POLITICA DEL CONTROL DE ACCESO

FIANZA LTDA
ASESORES FINANCIEROS

Parámetros Generales:

El ingreso a la empresa está restringido por medio de un control de acceso biométrico. Para su uso se debe cumplir con los siguientes políticas:

4. El personal que padezca enfermedades como dermatitis o cualquier otro impedimento para la utilización de la huella, deberá usar una clave de 5 a 7 dígitos, la cual por ningún motivo deberá ser compartido a otros integrantes de la empresa

5. La omisión de estas políticas, puede conllevar a descuentos o sanciones si se evalúa que el funcionario no registra sus entradas o salidas.

6. Las puertas deben permanecer cerradas todo el tiempo.

7. Solo tendrán acceso a cada área el personal autorizado.

POLITICA DEL CONTROL DE ACCESO

FIANZA LTDA
ASESORES FINANCIEROS

Parámetros Generales:

El ingreso a la empresa está restringido por medio de un control de acceso biométrico. Para su uso se debe cumplir con los siguientes políticas:

8. Solo tendrán acceso al Datacentero el personal del área de Tecnología, mediante acceso biométrico.

9. Si se hace necesario alguna visita externa al datacenter debe diligenciar la bitácora de ingreso donde queda registrado fecha, hora de ingreso y salida y motivo por el que ingresa. El visitante ingreso en compañía de personal autorizado.

10. Diariamente, el coordinador y auditoria y formación, validará el informe de entradas y salidas para confirmar el cumplimiento de la política.

11. El acceso a los visitantes de Fianza, se realizará con autorización previa, donde se le suministrará, carnet de visitante con presentación de documento personal.

POLÍTICA DE BACK UP

FIANZA LTDA
ASESORES FINANCIEROS

De acuerdo con las políticas de seguridad de la información, y con la disposición de un servidor que ofrece la posibilidad del manejo de información en forma centralizada; se ha diseñado un plan de backup de la información mediante tareas programadas del sistema operativo, que abarca un mantenimiento seguro de la información critica disponible en la base de datos mediante la transferencia de información a archivos nativos los cuales son almacenados en formato ZIP en una partición segura (raid 0) del disco duro del servidor y en nuestro dispositivo de almacenamiento externo NAS.

El backup protege la información contra daños de software y hardware. Esta conformado en 2 partes explicadas a continuación.

Backup Diferencial:

Realizado de Lunes a Sábado a las 1:30 p.m y a las 9:30 p.m. Una parte del disco duro almacena toda la información empleada durante el día, manteniendo la información de los días anteriores. Al final de la semana se contiene un backup de lo trabajado desde el lunes hasta el sábado.

Backup Completo Semanal:

Realizado el Domingo a las 11 p.m. Tomando el archivo de backup diferencial explicado en el punto anterior. Se realiza un backup de la información trabajada durante los últimos seis meses.

POLÍTICA DE BACK UP

FIANZA LTDA
ASESORES FINANCIEROS

- Los archivos en formato ZIP disponibles se pueden volver a cargar en la base de datos en caso de pérdida o daño de la información. Solo personal autorizado dispone de las contraseñas necesarias para su tratamiento y manipulación. Los archivos con antigüedad superior a 1 año son removidos del disco duro principal y se almacenan en disco externo en forma manual, con el fin de liberar espacio en disco duro.

- Estos backups se realizan dos veces al día, se mantiene la NAS dentro del centro de cómputo, el cual permanece bajo llave fuerte dentro de la empresa, una copia la custodia el Gerente de la empresa.

POLÍTICA MANEJO DE LA INFORMACIÓN

FIANZA LTDA
ASESORES FINANCIEROS

1. ¿Quién recibe las bases de datos?

- ✓ Las bases de datos son recibidas por el Coordinador de cada campaña
- ✓ El aplicativo para desencriptar las bases se encuentra únicamente instalado en el equipo del Coordinador de la campaña correspondiente.
- ✓ Las claves para desencriptar las bases son exclusivamente de uso del coordinador las cuales son modificadas mensualmente, en casos de presentarse alguna eventualidad, caso fortuito o accidente. El gerente custodia con sobre sellado estas claves.

2. ¿Qué se hace con las bases de datos?

- ✓ Una vez desencriptadas las bases se realiza el respectivo cargue en el Servidor.
- ✓ Cada campaña tiene asignada una carpeta a la cual solo tiene acceso el Coordinador y los Analistas que pertenezcan a la campaña y el auditor formador.
- ✓ El coordinador realiza el reparto de la cartera para cada Analista, el cual tiene al interior de cada campaña una carpeta con su nombre.

Aclaraciones del Manejo de la Información

- ✓ Cada campaña maneja su carpeta en el servidor a la cual solo tiene acceso el Coordinador y los integrantes de la campaña.
- ✓ El único computador que tiene instalado el programa para la apertura de las bases de datos es el del coordinador, el cual también se maneja con clave por lo tanto solo él tiene acceso tanto a su equipo de cómputo como al software para desencriptar las bases.
- ✓ La única persona autorizada para organizar y acceder a las bases de datos es el Ingeniero de Sistemas.
- ✓ Los únicos computadores que cuentan acceso al Outlook es el de los coordinadores, auditores formadores y administrativos los cuales a su vez, deben copiar los correos enviados al gerente de la empresa.

POLITICA DE PERMISOS

FIANZA LTDA
ASESORES FINANCIEROS

1. Administradores

*Es un grupo de seguridad del dominio local, el cual tiene acceso completo y sin restricciones al equipo o al dominio. A este grupo solamente pertenece el Ingeniero de Sistemas y en caso de algún accidente, evento o caso fortuito el Gerente de la empresa.

2. Usuarios

*Es un grupo de seguridad del dominio local y no pueden hacer cambios accidentales ni intencionados en el sistema. Solamente pueden ejecutar las aplicaciones certificadas pero no las heredadas. A este grupo pertenecen los Analistas y los Coordinadores. (Se anexa mapa de grupos y usuarios del directorio activo).

"El Ingeniero es quien aplica los niveles de seguridad de acuerdo a instrucciones precisas de Recursos Humanos."

POLITICA DE PERMISOS

FIANZA LTDA
ASESORES FINANCIEROS

1. Acceso a Perfil Administradores

*Este grupo tiene la opción de instalar o modificar cualquier software o aplicativo y configuraciones internas del computador.

2. Acceso a Perfil Usuarios

*Este grupo solo puede acceder a los programas del Equipo (office y el aplicativo de la cartera que corresponda) y a la carpeta de la campaña que pertenezca, la cual se encuentra ubicada en el Servidor.

"La única persona autorizada para acceder a las bases de datos es el ingeniero de sistemas"

POLÍTICA
SEGURIDAD DE LA INFORMACIÓN

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

POLÍTICA
SEGURIDAD DE LA INFORMACIÓN

- 2. Está <u>Totalmente Prohibido</u> el uso de celulares, cámaras, portátiles por parte de los analistas de cartera y coordinadores.

POLÍTICA
SEGURIDAD DE LA INFORMACIÓN

- **3. 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 tienen acceso a correo electrónico los asesores de servicio."

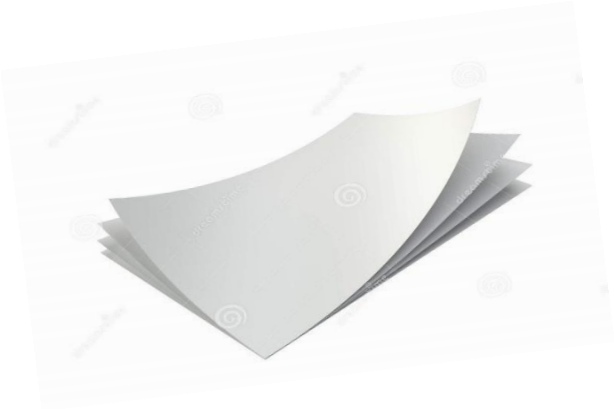
POLÍTICA
SEGURIDAD DE LA INFORMACIÓN

- 4. Los coordinadores y el área Administrativos son lo únicos habilitados para enviar impresiones y realizar escáner, los analistas no tienen este tipo de atributo.

"La impresora está conectada a un punto de red por lo tanto solo se puede configurar por un administrador."

POLÍTICA
SEGURIDAD DE LA INFORMACIÓN

- **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.**



POLÍTICA SEGURIDAD DE LA INFORMACIÓN

- **6. Solo se permite el acceso a áreas restringidas a personal debidamente carnetizado.**

POLÍTICA
SEGURIDAD DE LA INFORMACIÓN

- **7. Como medida de seguridad y garantía de la efectividad, no se permite recibir ni realizar llamada personales.**

POLÍTICA
SEGURIDAD DE LA INFORMACIÓN

08. Cabe resaltar que se realiza monitoreo telefónico y se realiza grabación del 100% de las llamadas tanto inbaund como outbaund.

POLÍTICA
SEGURIDAD DE LA INFORMACIÓN

09. 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.

POLÍTICA DE USUARIOS

FIANZA LTDA
ASESORES FINANCIEROS

El responsable de la asignación de usuarios y claves es el Agente de soporte técnico. El cual llevará el siguiente procedimiento para asignación de los mismos.

1. 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 catorce caracteres, ser alfanumérica, debe tener números y letras, un carácter especial y minino una mayúscula.

2. Una vez se crea el usuario, el agente de soporte técnico, lo une a un grupo, crea un clave y se asigna permisos de usuario.

3. A su vez el agente de soporte técnico, envía a los coordinadores de campaña el usuario y clave, de cada Analista que ingresa.

4. Cuando se retire algún funcionario de la compañía, se informa por parte de Talento Humano e inmediatamente el Ingeniero de sistemas procede a la eliminación del usuario. De tal forma que no se permite el acceso una vez se ha notificado el retiro del empleado.

- Después de 3 intentos fallidos, El usuario quedará bloqueado automáticamente.
- Para el desbloqueo del mismo, el coordinador de campaña solicitará por medio de un ticket el desbloqueo del mismo.

POLÍTICA BLOQUEO DE EQUIPOS

- ✓ Como proceso de inducción de la compañía se socializan las políticas entre las cuales se encuentran el bloqueo del Equipo el cual claramente señala que en el momento en el que se ausente del puesto de trabajo, independientemente del motivo se debe dar bloqueo al equipo con Control+Alt+Supr .

- ✓ En caso de olvido o de algún evento que impida el bloqueo manual por parte del funcionario, el sistema está configurado del tal forma que automáticamente se bloquea el equipo al término de 2 minutos.

- ✓ Al momento de instalación de los Equipos, el Ingeniero de Sistema configura el sistema se bloquee automáticamente al término de 2 minutos de inactividad.

Lock Computer (WIN-L)

PRESENTACIÓN PERSONAL

FIANZA LTDA

***POLITICA PRESENTACIÓN PERSONAL**, ESTA APLICA PARA TODO EL PERSONAL DE LA COMPAÑÍA SIN EXCEPCIÓN ALGUNA

- ✓ DE LUNES A JUEVES **NO** ES PERMITIDO EL USO DEL JEAN INCLUYE FALDAS, CHAQUETAS SHORTS (SOLO SE PERMITE EL DÍA VIERNES, SABADO, O EXCEPCIONES EN LAS QUE SE AUTORIZA CON PREVIO AVISO)
- ✓ NO SE PERMITE EL USO DE PIERCINGS, EXPANSIONES (OREJAS) Ó TATUAJES A LA VISTA.
- ✓ PARA EL CASO DE LOS HOMBRES EL CABELLO DEBE SER CORTO Y ESTAR AFEITADOS.
- ✓ PARA EL CASO DE LAS MUJERES SE DEBE HACER USO DE MAQUILLAJE Y ACCESORIOS DISCRETOS
- ✓ EVITAR LA MANGA SISA Y TRANSPARENCIAS.
- ✓ NO SE PERMITE EL USO DE SANDALIAS PARA EL CASO DE LAS MUJERES.
- ✓ EVITAR EL USO DE LAS FALDAS CORTAS Y SI SE USA DEBE IR CON MEDIAS APROPIADAS.
- ✓ NO SE PERMITE EL USO DE TENNIS. (SOLO SE PERMITE EL DÍA SÁBADO, O EXCEPCIONES EN LAS QUE SE AUTORIZA CON PREVIO AVISO.
- ✓ EL VESTUARIO NO NECESARIAMENTE ES VESTIDO SASTRE, PERO SI DEBE SER FORMAL

USO DE CARNET: TODO EL PERSONAL DEBE PORTAR EL CARNET EN UN LUGAR VISIBLE, SI POR ALGUNA RAZÓN NO LO PORTA, SERÁ DEVUELTO A TRAERLO.

"LA IMAGEN ES IMPORTANTE Y POR TAL RAZÓN LA IMPORTANCIA EN EL CUMPLIMIENTO DE NORMAS COMO ESTÁS, ESO LE IMPRIME SERIEDAD A NUESTRO TRABAJO; ES NECESARIO QUE TRANSMITAMOS LA INFORMACIÓN AL PERSONAL A CARGO; RECUERDEN QUE LOS LÍDERES Y ÁREAS ADMINISTRATIVAS DAN EJEMPLO PARA EL CUMPLIMIENTO DE LA NORMA."

FIANZA LTDA
ASESORES FINANCIEROS

“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.”

CIRCULARES FINANCIERAS

CIRCULAR 052 DE 2012

- Gestionar seguridad de la información usando como referencia los lineamientos de la ISO 27001.
- Envío de información a clientes en condiciones de seguridad.
- Dotar de seguridad los equipos y redes.
- Estar libre de software malicioso.
- Proteger claves y evitar claves compartidas. (Deben ser únicas y personalizadas).
- Instalación de programas y dispositivos únicamente por personal autorizado.
- Grabar llamadas que conllevan a la consulta o actualización.
- Software con soporte del fabricante o proveedor.
- Información que viaja debe ser cifrada por h.w. de próposito especifico o s.w. combinado.
- Bloquear el acceso a internet.

CIRCULAR 048 DE 2008

- Informar a los consumidores financieros de manera clara, precisa y completa, las políticas y mecanismos implementados por cada entidad para efectuar la gestión de cobranza.
- Abstenerse de realizar cobro alguno por concepto de gastos de cobranza prejudicial sin haber desplegado una actividad real encaminada efectivamente a dicha gestión
- Dejar constancia documental de las gestiones realizadas para la recuperación de cartera y de la información que se suministró a los deudores.
- Efectuar las gestiones de cobro de manera respetuosa y en horarios adecuados para los consumidores financieros.

GUIAS SAC, SARO, SARLAFT

SISTEMA ATENCIÓN AL CONSUMIDOR FINANCIERO "SAC"

"Es el Sistema de Atención al Consumidor Financiero, en el cual se desarrolla y adoptan políticas, procedimientos y controles para garantizar la adecuada Atención y Protección al Consumidor Financiero."

SISTEMA DE ADMINISTRACIÓN DE RIESGO OPERATIVO (SARO)

¿Qué es el **RIESGO?**

Es la posibilidad de que se produzca un resultado desfavorable en relación con un resultado esperado. Además s toda situación o circunstancia que pueda afectar el logro de los objetivos organizacionales y por tanto la creación de valor de la entidad.

¿QUÉ ES EL RIESGO OPERATIVO? (R.O)

"Es la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones; en el recurso humano, los proceso, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos que tengan la capacidad de incidir en el desarrollo del negocio del Banco. Incluye el riesgo legal y reputacional."

Riesgo Legal:

Es la posibilidad de pérdida en que incurriría el Banco al ser sancionado u obligado a indemnizar daños como resultado del incumplimiento de normas o regulaciones contractuales.

Riesgo Reputacional:

Es la posibilidad de pérdida en que incurriría el Banco por desprestigio, mala imagen publicidad negativa, cierta o no, respecto de la institución y sus practicas de negocios, que cause perdida de clientes, disminución de ingresos o proceso judiciales.

¿QUÉ ES EL SARO?

El sistema de Administración de Riesgo Operativo es el conjunto de elementos diseñados para identificar, medir y controlar los riesgos operativos al interior del Banco con el fin de mejorar la gestión de los procesos y de la operación de la entidad, de acuerdo con los principios fundamentales de productividad y eficiencia en los procesos, y la cantidad del servicio al cliente.

"La Superintendencia Financiera de Colombia mediante la Circular Externa 048 del 27 de Diciembre de 2006 estableció el Sistema de Administración de Riesgo Operativo (SARO) para las entidades sometidas a su inspección y vigilancia en la medida en que estas en desarrollo de sus operaciones, se exponen al Riesgo Operativo (RO)."

OBLIGACIÓNES

En desarrollo del SARO, el banco espera de los terceros que realizan parte de los proceso del banco, que:

Dispongan de los elementos mínimos de un sistema de gestión de riesgos Operativos, a saber:

- Documentación de los procesos
- Niveles de segregación de funciones
- Capacitación permanente a los funcionarios
- Control sobre la información, la calidad y los resultados del proceso(s) o producto(s) entregado(s) al banco.
- Planes de contingencia y continuidad de negocio
- Seguridades físicas e informáticas
- Pólizas de seguro para atender las coberturas propias de su negocio.

OBLIGACIÓNES

En desarrollo del SARO, el banco espera de los terceros que realizan parte de los proceso del banco, que:

Dispongan de los elementos mínimos de un sistema de gestión de riesgos Operativos, a saber:

- Capacitar de manera permanente a los funcionarios de acuerdo con los lineamientos dados por el Banco.
- Informen al Banco situaciones que pueden generar riesgo operativo en el desarrollo del servicio de corresponsalía y sugieran los controles o los cambios a los procesos para mitigarlos.
- Controlen la información, la calidad y los resultados del proceso o producto entregado al Banco.
- Atiendan las visitas de verificación del banco cuando así se requiera.

SISTEMA DE ADMINISTRACIÓN DE RIESGO DE LAVADO DE ACTIVOS Y FINANCIACIÓN DEL TERRORISMO (SARLAFT)

El **RLAFT** es la posibilidad de pérdida o daño que puede sufrir una entidad vigilada por su propesión a ser utilizada directamente o a través de sus operaciones como instrumento para el lavado de activos y/o canalización de recursos hacia la realización de actividades terroristas, o cuando se pretenda el ocultamiento provenientes de dichas actividad.

NORMATIVIDAD

“La Superintendencia Financiera de Colombia mediante la Circular Básica Jurídica, actualizada en el año 2016 por la Circular Externa 055 del 22 de diciembre de 2016 estableció el Sistema de Administración del Riesgo de Lavado de Activos y de la Financiación del Terrorismo (SARLAFT), para las entidades sometidas a su inspección y vigilancia en la medida en que estas en desarrollo de sus operaciones, se exponen al Riesgo de Lavado de Activos y de la Financiación del Terrorismo (LA/FT).”

OBLIGACIÓNES

En desarrollo del SARLAFT, se espera de los Proveedores de Cobranzas que participen de alguna manera con las operaciones que realizan por su intermedio las clientes que:

- Dispongan de los elementos mínimos de un sistema de gestión de riesgos de LA/FT, a saber:

- Capacitación permanente a los funcionarios
- Control sobre la completitud de la información diligenciada por los clientes.
- Informar a la entidad cuando se identifiquen acuerdos de pago en efectivo cuando se trate de sumas que igualen o superen los $10mm.

FIANZA LTDA

"La calidad nunca es un accidente, siempre resulta de cuatro cosas:
intención, esfuerzo sincero, dirección inteligente y talento"

W. Foster