MANUAL DE CONTROL DE ACCESO

Aprobó: **Silverio Carmona** Jefe Oficina de TI	Reviso: **Miguel Zuluaga** Líder SIG	Elaboró: **Viviana Ortiz** Profesional Especializado	**Código:** APO_12_4_1_MA01 **Versión:** 10 **Clasificación:** Pública **Fecha:** 2019/08/12

TABLA DE CONTENIDO

1. INTRODUCCIÓN 3

2. OBJETIVOS 3

3. ALCANCE 3

4. DEFINICIONES 3

5. DIRECTRICES Y PREMISAS PARA EL MANEJO DEL DOCUMENTO 4

6. DESARROLLO DEL DOCUMENTO 4

PARTE I: ESTÁNDAR CONTROL ACCESO LÓGICO 4

PARTE II: ESTÁNDAR PARA EL CONTROL DE ACCESO FÍSICO 18

7. PROCESOS Y/O SUBPROCESO ASOCIADO 27

8. RESPONSABLES 27

9. TABLA DE DOCUMENTOS Y/O FORMATOS ASOCIADOS 27

1. INTRODUCCIÓN

En este manual se realiza un compendio de estándares que aplican para gestión y administración del control de acceso tanto lógico (sistemas de información) y físico en áreas seguras de procesamiento de información.

2. OBJETIVOS

- Describir los estándares iniciales a aplicar en la gestión y administración del control de acceso lógico en los sistemas de información de Positiva Compañía de Seguros S.A. con el fin de preservar los principios de seguridad y calidad de la información.

- Propiciar la seguridad en las instalaciones de Positiva Compañía de Seguros S.A., especialmente en sus áreas críticas.

3. ALCANCE

- El alcance de este documento se basa en los estándares mínimos para realizar Control de acceso lógico en los sistemas de información de Positiva Compañía de Seguros S.A.

- Este estándar involucra directamente a todo personal interno o externo de Positiva Compañía de Seguros S.A., que tenga acceso a las instalaciones Físicas de la misma.

4. DEFINICIONES

ACUERDO DE NIVEL DE SERVICIO: Es un contrato escrito entre un proveedor de servicio y su cliente con el objeto de fijar el nivel acordado para la calidad de dicho servicio. El acuerdo de nivel de servicio es una herramienta que ayuda a ambas partes a llegar a un consenso y definir aspectos claves como tiempos de respuesta, disponibilidad, documentación disponible, personal asignado al servicio, etc.

BIBLIOTECA DE SOFTWARE DEFINITIVO (DSL - Definitive Software Library): Contiene copia de todo el software instalado en el entorno de TI. Esto incluye no solo sistemas operativos y aplicaciones sino también controladores de dispositivos y documentación asociada. La biblioteca de software definitivo debe contener el histórico completo de versiones de un mismo software para proporcionar la versión necesaria en caso de que se deban implementar los planes de retirada de una versión.

CONTROL DE VERSIONES: Una versión, revisión o edición de un producto, es el estado en el que se encuentra en un momento dado en su desarrollo o modificación. Se llama control de versiones a la gestión de los diversos cambios que se realizan sobre los elementos de algún producto o una configuración de este.

ELEMENTO DE CONFIGURACIÓN: Es la unidad física y/o lógica parte de un conjunto mayor de elementos, producida o adquirida, que por sus características es distinguible de las demás y cuya evolución interesa administrar.

EQUIPO TECNOLÓGICO: Son los dispositivos que se emplean para ejercer funciones de prestación de servicio eficiente, para atención a los requerimientos.

INCIDENTE: Cualquier evento que no forma parte de una operación normal de un servicio y que causa o puede causar una interrupción o reducción de la calidad del servicio.

MESA DE AYUDA/SERVICIO (SERVICE DESK): Grupo de soporte de cara al usuario, que realiza la mayor porción del trabajo de soporte.

SOFTWARE: Se refiere a los programas utilizados en las instalaciones de Hardware.

USUARIOS ADMINISTRADORES (PRIVILEGIADOS): Para base de datos y aplicaciones, cuenta capaz de visualizar cualquier tipo de dato, interactuar con él, practicar insert, delete y update de estos, así como creación de objetos, con sentencias ejecutadas directamente en las tablas de bases de datos. Para servidores y sistemas operativos, cuenta capaz de visualizar cualquier tipo de dato, interactuar con él, practicar insert, delete y update de estos, con la capacidad de ejecutar cualquier sentencia a nivel de sistema operativo.

5. DIRECTRICES Y PREMISAS PARA EL MANEJO DEL DOCUMENTO

Este Manual es actualizado y aprobado única y exclusivamente por la Oficina de TI. Su uso y distribución debe ser de uso interno y para fines normativos de la Compañía. Prohibida su distribución sin previa autorización de la Oficina de TI.

6. DESARROLLO DEL DOCUMENTO

PARTE I: ESTÁNDAR CONTROL ACCESO LÓGICO

1. MARCO GENERAL

Los estándares generales de control de acceso lógico deben cumplirse para todos los sistemas de información que se desarrollen a partir de la publicación de estos estándares.

Para los sistemas de información que se encuentran en producción y que no cumplen con estos estándares generales, se seguirá con los establecidos en cada uno de ellos, pero cuando se realicen actualizaciones del sistema de información que involucren modificaciones al módulo de control de acceso, se deben acondicionar a los estándares generales determinados en el presente documento.

1.1 NOMENCLATURA PARA NOMBRES DE USUARIO DE POSITIVA COMPAÑÍA DE SEGUROS S.A.

- El nombre de Usuario de Red es el número de Cédula.

- El nombre de Usuario de Correo se usa el Nombre y Apellido en caso de ser Homónimos se usa el 2 apellido. Aplica primer nombre, punto primer apellido, si hay homónimo, primer nombre + inicial segundo nombre, punto + apellido.

1.1.1 Contraseñas para usuarios de dominio y sus aplicaciones enlazadas para Positiva Compañía de Seguros S.A.

El estándar para el manejo de claves de acceso al dominio correspondientes y las aplicaciones que se enlacen a este, para usuarios creados en directorio activo de Positiva Compañía de Seguros S.A. es:

- Tamaño mínimo de la clave: catorce (14) caracteres.
- Compuesta por: combinación que incluya números, letras (mayúsculas y minúsculas) y símbolos o caracteres especiales ($, %, &, *).
- La contraseña inicial emitida a un nuevo Usuario sólo es válida para la primera sesión. En ese momento, el Usuario debe escoger otra contraseña. El programa obliga a hacer cambio de la contraseña, teniendo en cuenta las características mencionadas antes.
- Vigencia máxima: cada un (1) año como máximo, el sistema solicitará el cambio de clave, la contraseña no debe ser igual a las últimas tres contraseñas utilizadas.

1.1.2 Contraseñas para usuarios de Positiva Compañía de Seguros S.A.

El estándar para el manejo de claves de acceso correspondientes a usuarios creados en las plataformas tecnológicas de Positiva Compañía de Seguros S.A. es:

- Tamaño mínimo de la clave: ocho (8) caracteres.
- Compuesta por: combinación que incluya números, letras (mayúsculas y minúsculas) y símbolos o caracteres especiales ($, %, &, *).
- La contraseña inicial emitida a un nuevo Usuario sólo es válida para la primera sesión. En ese momento, el Usuario debe escoger otra contraseña. El programa obliga a hacer cambio de la contraseña, teniendo en cuenta las características mencionadas antes.
- Vigencia máxima: cada treinta (30) días como máximo, el sistema solicitará el cambio de clave, la contraseña no debe ser igual a las últimas tres contraseñas utilizadas. Para algunas aplicaciones como SISE el tiempo de solicitud de cambio de contraseña es de 60 días.
- Bloqueo por intentos de acceso fallidos: después de cinco (5) intentos fallidos, la cuenta se bloquea y el usuario debe alertar al Administrador del Sistema, si se trata de acceso remoto vía VPN, la sesión debe ser inmediatamente desconectada. En algunos casos como MIDAS, SAP, IAXIS se bloquea con 3 intentos. Para las aplicaciones MIDAS, SISE y SIARP el bloqueo por intento fallido de contraseñas es permanente y solo se podrá desbloquear un usuario, realizando una validación directa con el administrador de cada aplicación.
- Para las aplicaciones MIDAS, SISE y SIARP no aplicará el historial de las ultimas contraseñas utilizadas.
- Las contraseñas predefinidas que traen los equipos nuevos tales como Routers, Switchs, etc., deben cambiarse de inmediato.
- Para las conexiones VPN se tiene un tiempo estimado de 30 minutos para la desconexión por inactividad de los usuarios a excepción de algunos grupos, debido a que ejecutan procesos extendidos que deben quedar corriendo y no pueden ser desconectados.

El uso de los anteriores parámetros es lo que se denomina generación de “claves fuertes”.

Parámetros Opcionales:

- Vigencia mínima: siete (7) días, antes de poder realizar un nuevo cambio.
- Cuando el estándar para claves de acceso no se pueda aplicar por incompatibilidades de especificaciones técnicas de las diferentes plataformas tecnológicas de Positiva compañía de Seguros S.A., se presentan excepciones las cuales son tratadas en el aparte donde se referencia el control de acceso a la plataforma específica.

1.1.2 Excepciones

Dentro de los procesos de la compañía se podrán encontrar las siguientes excepciones:

- Algunos procesos de la compañía como es el pago de nómina de pensionados, el cual se realiza finalizando cada mes, utiliza una herramienta de cifrado que requiere de un usuario para el acceso a carpetas donde se alojan los archivos de pagos; dada a la criticidad y teniendo en cuenta que el usuario es solamente utilizado por la herramienta, la contraseña de este no tendrá vencimiento, puesto que afectaría el proceso generando un alto impacto para Positiva.
- Para las APP y Kioscos las contraseñas podrán definirse alfanuméricas, mínimo de 6 dígitos, las cuales tendrán restricciones de complejidad como: no incluir el numero de la cedula, no incluir números seguidos, no incluir fecha de nacimiento, no incluir fechas relacionadas con el usuario, no incluir números repetidos seguidos, con el fin de no hacerlas tan frágiles; dado a que las APP y los Kioscos solo manejarán temas de consultas y transaccionalidad de baja criticidad, se genera la excepción.

1.2 APLICATIVOS

Para todos los aplicativos de la compañía se estima un tiempo de sesión por inactividad fijado en 10 Minutos, sin embargo, se presentan algunas particularidades para los siguientes aplicativos.

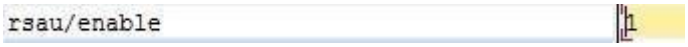
1.2.2 Parámetros de usuarios para SAP

Teniendo en cuenta que el sistema SAP requiere ser parametrizado adecuadamente para el manejo de contraseñas, se indican a continuación parámetros específicos sumados a los ya recomendados en el presente estándar:

- login/fails_to_user_lock = Este parámetro determina la cantidad de errores consecutivos en el ingreso de la contraseña a partir del cual se bloquea el usuario, el cual debe ser desbloqueado por el administrador salvo que el parámetro
- logins/failed_user_auto_unlock tenga un valor distinto de 0, por lo cual se debe mantener en 1.

- rdisp/gui_auto_logout = Mediante este parámetro se determina en segundos la cantidad de tiempo de inactividad antes que se terminé la sesión del usuario (0 deshabilitado). El valor definido es de 1800 segundos equivalente a 30 minutos.

- rsau/enable: activar el LOG de auditoria de seguridad, por lo cual el valor debe ser 1



- rsau/selection_slots: identifica el número de filtros para el registro de auditoria de seguridad; el valor recomendado es 2.

1.2.2.1 MONITOREO CUENTAS DE SAP

Con una periodicidad de un mes, se ejecutará la transacción RSUSR200 que permite mostrar cuando fue el último ingreso de los usuarios al sistema. Una vez se valide que los usuarios llevan más de 90 días sin uso de la cuenta, se procede a inactivarla hasta tanto no se reciba notificación de parte del área responsable.

Se debe generar un reporte mensual donde se listarán aquellos usuarios cuyo ingreso al sistema supere los 90 días con el fin de proceder a solicitar autorización de desactivación.

1.2.2.2 INTEGRACION DIRECTORIO ACTIVO - SAP

El usuario debe ingresar al dominio con sus credenciales tanto para el nombre como la contraseña existente, para los usuarios que tenga instalado el cliente de SAP-GUI deben acceder a SAP, por SAP Logon, los usuarios de SAP ingresarán de forma automática sin necesidad de volver a ingresar la clave, ya que hay una relación de confianza entre el directorio activo y SAP y aplica las reglas de Claves para usuarios de Positiva Compañía de Seguros S.A.

1.2.2.3 PERMISOS ESPECIALES PARA PERFILES PRIVILEGIADOS SAP

Para aquellos usuarios que requieren perfiles por defecto SAP_ALL, SAP NEW y SAP SYSTEM, deben ser autorizados por el área responsable justificando su uso, teniendo en cuenta las siguientes consideraciones:

- Usuarios que requieren Acceso a la Administración del sistema.
- Usuarios que requieren acceso a la configuración funcional del sistema.
- Usuarios que requieren generar y validar el licenciamiento de SAP.
- Usuarios que requieren apoyar la etapa de implementación de las funcionalidades.

1.2.3 Parámetros para usuarios SNP, SICO, GESPOS, SEGUIR, CUIDA1

Solo ingresan usuarios registrados según la nomenclatura presente.

1.2.4 SISE

SISE no cuenta con tiempo de inactividad para cerrar sesión, eso lo determina la BD, a través del tiempo que tiene el motor de base de datos Sybase de conexión, una vez se termina ese tiempo la conexión activa se desconecta. Lo cual genera que al intentar abrir otro modulo SISE genere una nueva conexión.

1.2.5 BI – Bussines Intelligent

BOC, no tiene como configurables tiempos de inactividad para cerrar sesión. Sin embargo, si cuenta con un timeout para la consulta a los modelos que se encuentran con conexión a HANA y este corresponde a 30 segundos.

1.3 Nomenclatura para nombres de usuario de correo electrónico de Positiva Compañía de Seguros S.A.

- El nombre del usuario en el correo electrónico se especifica de la siguiente manera: < nombre de cuenta >@< dominio > Se toma N° de ceula+@positiva.gov.co

- En Positiva compañía de Seguros el dominio puede tomar dos valores así:

    - positiva.gov.co ó
    - xxx.positiva.gov.co No conozco este ultimo

    Donde xxx identifica la regional. Ejemplo: drg = Dirección General, occ = Regional Occidente, ant = Regional Antioquia.

- En Positiva Compañía de Seguros S.A. el nombre de la cuenta debe cumplir los siguientes parámetros:

    - El nombre de la cuenta debe tener máximo (255) caracteres y mínimo cuatro (4) caracteres. - Su composición será: <Nombre1>, punto (.) y <Apellido1>, ejemplo: julio.florez para Julio Florez. Ok

    - Para usuarios con dos nombres, nombre1 y apellido1 iguales, se ingresan cronológicamente de la siguiente manera:
        El primero: < Nombre1>, punto (.) y <Apellido1> Ok
        El segundo: < Nombre2>, punto (.) y <Apellido1> Nombre1+inicialnombre2.apellido

    - Para usuarios con un solo nombre, nombre igual y apellidos iguales, se ingresan de la siguiente manera:

El primero: < Nombre1> punto (.) <Apellido1>
El segundo: < Nombre1> +<inicial del apellido1> punto (.) <Apellido1>

- Para más de dos (2) usuarios con nombres iguales y apellidos iguales, se ingresan de la siguiente manera:
  El primero: < Nombre1> punto (.) <Apellido1>
  El segundo: < Nombre2> punto (.) <Apellido1> Nombre1+inicialnombre2.apellido
  El tercero: < Nombre1> +<inicial del apellido1> punto (.) <Apellido1>
  El cuarto: < Nombre1> +<dos primeros digitos apellido1> punto (.) <Apellido1>

En el caso de más homónimos se realizarán las combinaciones entre nombres y apellidos correspondientes, manteniendo el orden cronológico de ingreso ok.

1.3.1 Claves de correo de Positiva Compañía de Seguros S.A.

El estándar para el manejo de claves de acceso correspondientes a usuarios de correo electrónico de Positiva Compañía de Seguros S.A. es:

- Tamaño mínimo de la clave: cuatro (4) caracteres. Tamaño máximo doce (12) caracteres.
- Compuesta por: combinación que incluya números, letras (mayúsculas y minúsculas) y símbolos o caracteres especiales ($, %, &, *).
- Al cambiar la clave, no se puede repetir la anterior.

1.3.2 Nomenclatura para nombres de usuario de redes externas

- El nombre del usuario en las redes externas se especifica de la siguiente manera: < nombre de cuenta > - < nombre de la empresa >

- El nombre de cuenta se deben seguir las siguientes reglas:

  - El nombre de la cuenta debe tener máximo (30) caracteres y mínimo cuatro (4) caracteres. - Su composición será: <Nombre1>, punto (.) y <Apellido1>, ejemplo: julio.florez para Julio Florez.

  - Para usuarios de una misma entidad con dos nombres, nombre1 y apellido1 iguales, se ingresan cronológicamente de la siguiente manera:
    El primero: < Nombre1>, punto (.) y <Apellido1>
    El segundo: < Nombre2>, punto (.) y <Apellido1>

  - Para usuarios de una misma entidad con un solo nombre, nombre igual y apellidos iguales, se ingresan de la siguiente manera:
    El primero: < Nombre1> punto (.) <Apellido1>
    El segundo: < Nombre1> +<inicial del apellido1> punto (.) <Apellido1>

- Para más de dos (2) usuarios de la misma entidad con nombres iguales y apellidos iguales, se ingresan de la siguiente manera:
  El primero: < Nombre1> punto (.) <Apellido1>
  El segundo: < Nombre2> punto (.) <Apellido1>
  El tercero: < Nombre1> +<inicial del apellido1> punto (.) <Apellido1>
  El cuarto: < Nombre1> +<inicial del apellido2> punto (.) <Apellido1>

En el caso de más homónimos se realizarán las combinaciones entre nombres y apellidos correspondientes, manteniendo el orden cronológico de ingreso

- El nombre de la empresa debe seguir las siguientes reglas:

  - El nombre de la empresa debe tener máximo (30) caracteres y mínimo cuatro (4) caracteres.

1.3.3 Controles de acceso y lugar de custodia de contraseñas de administración de diferentes recursos de TI

- Las contraseñas de administrador de ***dominio, administrador local de los servidores y equipos activos*** que conforman la infraestructura de la compañía se deberá cambiar cada 180 días o antes si por algún motivo de configuración sea necesario realizar este cambio, cada vez que se realice este procedimiento se debe cambiar el sobre sellado que se entrega a la Oficina de TI.

- Las contraseñas para algunas cuentas administradoras (privilegiadas) tendrán excepción en el cambio indicado en el párrafo anterior, debido a que, por lineamiento de servicios asociados, no es viable que se cambie de manera periódica, puesto que podría generar indisponibilidad afectando el servicio de la compañía.

- Las contraseñas de administración y/o altos privilegios de ***Bases de Datos*** se deberá cambiar cada 90 días o antes si por algún motivo de configuración sea necesario realizar este cambio, cada vez que se realice este procedimiento se debe cambiar el sobre sellado que se entrega a la Oficina de TI.

- Los funcionarios responsables de la administración del dominio, de los servidores, equipos activos y Base de datos que conforman la infraestructura de la compañía, deberán entregar en sobre sellado y firmado al jefe de la Oficina de TI los usuarios y contraseñas respectivos.

1.3.4 Cuentas Genéricas de Sistema Operativo Servidor y de Bases de Datos

- Las contraseñas de administrador local de los servidores, aplicaciones y equipos activos de la Compañía deben tener un tamaño mínimo de ocho (8) caracteres, compuesta por números, letras (mayúsculas y minúsculas) y símbolos o caracteres especiales ($, %, &, *).

- Los usuarios genéricos de Sistema Operativo Servidor y Bases de Datos se deshabilitarán en los casos que no afecte el desempeño de los equipos y los usuarios genéricos que por condición de la aplicación se deban crear, estarán registrados en una bitácora (archivo en Excel) que se encontrará ubicado en el FILE SERVER de la Oficina de TI.

- Las novedades de eliminación e inactivación de cuentas de usuario, estará a cargo de las dos (2) personas: administrador de Bases de Datos y administrador de Servidores, y el monitoreo de esta información la efectuará cada tres (3) meses la Oficina de TI.

- Los usuarios y contraseñas entregadas a los funcionarios Positiva, deben ser provistas por separado, es decir, se debe hacer entrega del usuario por un canal de comunicación de la compañía y la contraseña debe ser entregada de forma personal al usuario y en caso de que sea mediante un canal de comunicación, esta debe ir cifrada; bajo ningún circunstancia se hará entrega de formatos APO_12_1_2_FR02 Asignación de Cuentas y Claves para Usuarios Privilegiados de usuarios privilegiados a las entidades que así lo soliciten, estos formatos APO_12_1_2_FR02 Asignación de Cuentas y Claves para Usuarios Privilegiados únicamente estarán a disposición de la compañía cuando sea un caso de fuerza mayor.

1.3.5 Restricciones a los terceros prestadores de servicios para Positiva

- En general se deben aplicar todas las restricciones descritas en los numerales 4.1.1 a 4.1.6 para los terceros que, en virtud de la subscripción de contratos de prestación de servicios, ejerzan labores para POSITIVA.

- Se debe tener en cuenta las restricciones totales en cuanto a acceso administrativo a la infraestructura de aplicaciones, servidores y de comunicaciones a los terceros prestadores de servicio, y en caso de ser requerido por el tercero este tipo de acceso, se debe hacer en vigilancia y supervisión del administrador encargado de Positiva.

- En caso en que el contrato de servicios incluya la delegación expresa de la administración de la infraestructura por parte de POSITIVA al tercero prestador de servicios, esta se debe hacer solicitando un usuario temporal para el servicio y habilitando las condiciones de Auditoria y trazabilidad de acciones que realice el tercero en el sistema, y en todo caso el o los administradores de infraestructura de servidores, aplicaciones y dispositivos de comunicaciones de POSITIVA, deberán realizar seguimiento periódico de las actividades que el tercero realiza en la mencionada plataforma tecnológica.

1.3.6 Restricciones de claves para los sistemas de información

Debido a la vulnerabilidad que implica el uso de ciertas palabras como claves de acceso a sistemas de información, se define aquí, un conjunto de palabras que deben ser parametrizadas como prohibidas dentro de los sistemas misionales de Positiva S.A.

Admin	
Clave	Positiva123
password	Positiva2015
Colombia2015	Positiva2016
Colombia2016	Soporte01

Dic_2015	Soporte02
Dic_2016	Soporte100
Digi2014	Soporte123
Digi2015	Soporte2016
Digi2016	Soporte500
Positiva01	Soporte600
Positiva02	Soporte900

1.3.7 Estándar de Administración de Usuarios Administradores (Privilegiados) de Servidores y Bases de Datos

Para funcionarios de Positiva Compañía de Seguros S.A. y/o proveedores con contratos suscritos, a los cuales se les entrega la administración de acceso de los sistemas de información, Bases de Datos, sistemas operativos y redes de Positiva Compañía de Seguros S.A. (SA, ROOT, ADMIN), se les debe formalizar la entrega de este privilegio por medio del formato APO_12_1_2_FR02 Asignación de Cuentas y Claves para Usuarios Privilegiados donde se le indique la responsabilidad de uso de este tipo de rol administrativo y el cumplimiento de los estándares de control de cambios para realizar las labores administrativas, de mantenimiento e incidentes emergentes.

Cuando se requiera asignar a un funcionario de Positiva Compañía de Seguros S.A y/o proveedores con contratos suscritos, un rol correspondiente a usuarios con perfil de administrador (ejecución de tareas de mantenimiento y/o administración del motor de base de datos en procesos como reorganización de bases de datos, actualización de estadísticas, creación de objetos, etc) y/o usuarios con permisos de modificación de datos (insert, delete, update) directamente sobre los tablas, el Administrador de la Base de Datos garantizará el debido monitoreo y registros de las acciones que desarrolle el funcionario a quien se le asigne este privilegio.

Los usuarios registrados en la base de datos tendrán roles acordes a los siguientes perfiles y bajo el siguiente alcance:

- Administrador (SA rol): Sólo quien ejerza este rol tendrá la contraseña del SA y podrá realizar las tareas definidas para un Administrador de Bases de Datos (DBA).

- Operador: Puede realizar tareas de ejecución de scripts o de archivos por lotes y los permisos sobre los objetos de bases de datos serán asignados por el DBA acorde a las necesidades operativas y/o funcionales que establezca la OTI en el formato de Creación de usuarios existente.

- Funcional: Los funcionarios de la OTI que desempeñan funciones técnicas sobre las aplicaciones de Positiva y que requieran tener permisos de modificación de datos (insert, delete, update) directamente sobre las tablas, podrán construir objetos de bases de datos (procedimientos almacenados, vistas, etc) para que el DBA los aplique. Este procedimiento será acorde a lo definido en la herramienta de Gestión de Incidentes (Aranda) para el proceso de Control de Cambios existente.

La Oficina de Tecnología y de la Información se encargará de custodiar en sobres cerrados cada una de estas cuentas y claves administrativas y solo bajo procedimientos de control de cambios y controles de

cambios de emergencia serán entregadas a los encargados de administración de los sistemas para las labores requeridas, y posterior al suceso de emergencia, se volverá a formalizar la entrega de esta clave a la custodia de la Oficina de TI por medio del formato APO_12_1_2_FR02 Asignación de Cuentas y Claves para Usuarios Privilegiados.

De igual forma, el mismo procedimiento se debe realizar con cuentas de servicio de las aplicaciones, que deban tener permisos administrativos sobre el sistema operativo de los servidores.

Los usuarios y contraseñas entregadas a los funcionarios Positiva, deben ser provistas por separado, es decir, se debe hacer entrega del usuario por un canal de comunicación de la compañía y la contraseña debe ser entregada de forma personal al usuario y en caso de que sea mediante un canal de comunicación, esta debe ir cifrada; bajo ningún circunstancia se hará entrega de formatos APO_12_1_2_FR02 Asignación de Cuentas y Claves para Usuarios Privilegiados de usuarios privilegiados a las entidades que así lo soliciten, estos formatos APO_12_1_2_FR02 Asignación de Cuentas y Claves para Usuarios Privilegiados únicamente estarán a disposición de la compañía cuando sea un caso de fuerza mayor.

1.3.8 Controles de acceso y lugar de custodia de contraseñas de administración de diferentes recursos

- Las contraseñas de administrador de dominio, administrador local de los servidores y equipos activos que conforman la infraestructura de la compañía se deberá cambiar cada 180 días o antes si por algún motivo de configuración sea necesario realizar este cambio, cada vez que se realice este procedimiento se debe cambiar el sobre sellado que se entrega a la Oficina de TI.

- Las contraseñas para algunas cuentas administradoras (privilegiadas) tendrán excepción en el cambio indicado en el párrafo anterior, debido a que, por lineamiento de servicios asociados, no es viable que se cambie de manera periódica, puesto que podría generar indisponibilidad afectando el servicio de la compañía.

- Los funcionarios responsables de la administración del dominio, de los servidores y equipos activos que conforman la infraestructura de la compañía, deberán entregar en sobre sellado y firmado al jefe de la Oficina de TI los usuarios y contraseñas respectivos.

- Los usuarios contratados con terceros en el directorio activo no caducarán su contraseña, debido a que se realizará la depuración de forma trimestral.

1.4 Estándares para Módulos de Seguridad en los Sistemas de Información

Todos los sistemas de información deben contar con un módulo de seguridad que permita la realización de actividades de control de acceso al sistema y con las siguientes características:

- Creación y actualización de usuarios.
- Creación y establecimiento de contraseñas.
- Creación y establecimiento de perfiles o roles de acceso

- La asignación de permisos a los usuarios para el acceso a la información.
- Archivos de auditoría donde se registren las actividades de creación y actualización de usuarios.
- Autenticación de usuarios ante el sistema de información. - Herramienta de monitoreo de los archivos de auditoría.

2. ESTÁNDARES DE PERFILES DE ACCESO A POSITIVA COMPAÑÍA DE SEGUROS S.A.

En Positiva Compañía de Seguros S.A. se establece los siguientes tipos de perfiles o roles de acceso, con los cuales debe contar un sistema de información:

TIPO DE PERFIL DE ACCESO	DESCRIPCION
A. Rol administrador de usuarios	*Corresponde a los sistemas de información que cuentan con un funcionario encargado del módulo de administración de usuarios y de quien dependen las actividades de:* *- Registro y actualización de usuarios.* *- Registro y actualización de contraseñas.* *- Registro y actualización de permisos.* *- Asignación de permisos a los usuarios.*
A. Rol Operador (RO)	*Corresponde a los sistemas de información que cuentan con un funcionario encargado de la ejecución de procesos como:* *- Procesos de Respaldo.* *- Ejecución de programas específicos.*
A. Rol Usuario (RU)	*Corresponde a los sistemas de información que cuentan con funcionarios encargados de la ejecución de la funcionalidad del sistema de información.* *Estos se clasifican en:* • ***Administrativo**: Personal administrativo que accede a las aplicaciones para autorizaciones. Sus permisos se basan en la modificación y consulta de la información a través de los sistemas.* • ***Operativo:** Personal encargado de la operación del negocio con funcionalidad específica del trámite requerido. Sus permisos se basan en la inserción, modificación y consulta de la información a través de los sistemas.* • ***Técnico:** Personal que soporta la solución a los requerimientos técnicos propios de la aplicación. Sus permisos se basan en la modificación y consulta de la información a través de los sistemas.* • ***Genérico:** personal con consulta pública del trámite. Sus permisos se basan exclusivamente en la consulta.*
A. Rol Múltiple (RM)	*Corresponde a los sistemas de información que cuentan con la facilidad de agrupar funcionarios por diferentes actividades y crear roles diferentes a los mostrados en este estándar.*

- Los administradores de los aplicativos archivarán evidencia de recibo por parte de los usuarios y como medida de control de seguridad de los privilegios asignados.

- Un usuario puede tener asociado uno o varios roles, dependiendo de las responsabilidades o actividades propias del cargo.

3. ESTÁNDAR DE TIPO DE CONTROL DE ACCESO

Positiva Compañía de Seguros S.A. tendrá una clasificación general de acceso que permita especificar el tipo de acceso con el que cuenta o contará un sistema de información particular. Los tipos de control de acceso establecidos son:

TIPO DE CONTROL DE ACCESO	FORMA DE ACCESO
A. Control de Acceso Directo Aplicativo: Corresponde a los sistemas de información que dependen únicamente de su módulo de acceso para controlar sus actividades de registro y actualización de usuarios, registro y actualización de claves de acceso, registro y actualización de permisos y la autenticación del acceso sobre el propio sistema.	*Acceso al aplicativo* *Rol en el sistema aplicativo* *Horario de aplicativo*
B. Control de Acceso Indirecto: Corresponde a los sistemas de información que dependen del sistema operativo para controlar sus actividades de autenticación del acceso.	*Acceso al sistema Operativo* *Acceso al aplicativo* *Rol de aplicativo* *Horario de aplicativo*
C. Control de Acceso Directo Sistema Operativo: Corresponde a los sistemas de información ligados al sistema operativo de la máquina para el registro y actualización de usuarios, registro y actualización de claves de acceso, registro y actualización de permisos y la autenticación del acceso sobre el propio sistema.	*Acceso al sistema operativo* *Rol en el sistema operativo* *Horario del sistema operativo*
D. Control de Acceso Directo Terceros: Corresponde a los sistemas de información cuya administración depende de terceros con relación contractual con Positiva Compañía de Seguros S.A. y quienes cuentan con su propio sistema de control de registro y actualización de usuarios, registro y actualización de claves de acceso, registro y actualización de permisos y la autenticación del acceso, para funcionarios de Positiva Compañía de Seguros S.A.	*Acceso al aplicativo del tercero* *Rol de aplicativo del tercero* *Horario de aplicativo del tercero*

La Oficina de TI implementará un control de horario para acceso a la red lo cual permite monitorear y restringir el acceso fuera de horario laboral.

4. ESTÁNDAR DE TIPO DE USUARIOS

Positiva Compañía de Seguros S.A. tendrá una clasificación general de usuarios que permita identificar el nivel y el alcance de cada funcionario con respecto al sistema de administración de usuarios. Los tipos de control de acceso establecidos son:

TIPO DE USUARIO	DESCRIPCION	ALCANCE
Usuario Interno (Cliente)	Funcionarios normales de Positiva Compañía de Seguros con más o menos privilegios que harán uso de los recursos de los sistemas de información.	Estos usuarios tendrán acceso monitoreado a los sistemas de información de Positiva Compañía de Seguros. • Sistemas transaccionales. • Sistemas Administrativos. • Sistemas Gerenciales. • Sistemas de información externos con los que Positiva Compañía de Seguros tiene convenio contractual Podrán actualizar o consultar información de acuerdo con los privilegios que se les otorga.
Usuario Externo (Cliente)	Pueden ser clientes de Positiva Compañía de Seguros o terceros con relación contractual con Positiva Compañía de Seguros con más o menos privilegios que harán uso de los recursos de los sistemas de información del Positiva Compañía de Seguros.	Estos usuarios tendrán acceso monitoreado a los sistemas de información de Positiva Compañía de Seguros. • Sistemas transaccionales. • Sistemas Administrativos. • Sistemas Gerenciales. • Sistemas de información externos con los que Positiva Compañía de Seguros tiene convenio contractual. Podrán actualizar o consultar información de acuerdo con los privilegios que se les otorga.
Usuario Técnico Interno (Servidor)	Funcionarios de Positiva Compañía de Seguros S.A. a los cuales se les entrega la administración de acceso de los sistemas de información, a los sistemas operativos y redes de Positiva Compañía de Seguros S.A. (SA, ROOT, ADMIN).	Estos usuarios podrán: - Crear usuarios. - Actualizar usuarios. - Asignar permisos y roles. - Asignar claves iniciales de acceso.
Usuario Técnico Externo (Servidor)	Funcionarios externos a Positiva Compañía de Seguros a los cuales se les entrega la administración de acceso de sistemas particulares de información, sistemas operativos o redes de propiedad de Positiva Compañía de Seguros S.A. Funcionarios de entidades externas a Positiva Compañía de Seguros, poseedoras de sistemas de información a los cuales ingresan funcionarios de Positiva Compañía de Seguros S.A.	Estos usuarios podrán: • Crear usuarios. • Actualizar usuarios. • Asignar permisos y roles. • Asignar contraseñas iniciales de acceso.
Usuario Técnico De Convivencia (cliente o servidor)	Son usuarios especiales que se utilizan para la ejecución de servicios específicos, conectividad entre aplicativos y ejecución de procesos entre otros.	Estos usuarios siempre tendrán un responsable en las áreas técnicas.

5. ADMINISTRACIÓN PRIVILEGIADA DE SERVIDORES

Dados los perfiles descritos en el punto 4, donde se establecen roles delegados para la administración de sistemas operativos y servicios instalados, el administrador de la infraestructura de servidores, formalizará por medio del formato APO_12_1_2_FR02 ASIGNACIÓN DE CUENTAS Y CLAVES PARA USUARIOS PROVILEGIADOS, la delegación de administración de servicios o del sistema operativo, con el funcionario o tercero que lo requiera (previa justificación y aprobación en comité de control de cambios), donde quedará constancia del rol de administración delegado y la asignación o el cambio de clave del usuario creado para la delegación, con la definición del rol suministrado y la firma del funcionario o tercero que recibe, formato que quedará para custodia de seguridad informática.

6. ADMINISTRACIÓN Y CONTROL DE ROLES Y PERFILES

En cumplimiento con la Política de Control de Acceso de TI (específicamente numeral 4.6.5 - Revisión de Derechos de Acceso de Usuarios), el área dueña de la información que hace parte de los procesos en los diversos aplicativos misionales de Positiva Compañía de Seguros, deberá definir y actualizar la matriz de roles y perfiles de acceso a los aplicativos, en virtud de que es ella quien maneja con claridad la clasificación de la información y el flujo de esta en los procesos que involucran el aplicativo, y es quien puede determinar quién y en qué forma puede acceder a los módulos del sistema. Cada área dueña de la información deberá autorizar el personal con acceso, relacionando cada funcionario en su matriz de roles y perfiles y enviando el formato de solicitud a la Oficina de TI con la asignación de permisos para que estos sean asignados operativamente.

La Oficina de TI se encargará de enviar a cada área en forma trimestral los listados de las personas autorizadas a los módulos y el perfil de acceso relacionado a cada persona, para que el área valide la pertinencia de esos permisos e indique a la Oficina de TI, como área operativa, para que inhabilite el personal no autorizado.

Así mismo, una vez sea notificada la Oficina de TI sobre novedades de personal, se cancelará inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización, se desvincularon de Positiva Compañía de Seguros S.A. o sufrieron la pérdida o robo de sus credenciales de acceso a los sistemas de información.

La operación de los módulos de creación y modificación de usuarios (de acuerdo con los cambios solicitados sobre roles y perfiles de los sistemas de información), los realizará la Oficina de TI de forma progresiva, de acuerdo con las delegaciones que realicen cada una de las áreas de negocio.

7. INACTIVACIÓN TEMPORAL Y DEFINITIVA DE USUARIOS:

Con el objetivo de mantener los criterios de seguridad de la Información a través de los sistemas de información, la Oficina de TI propenderá por el control de acceso a los usuarios cuando estos sean reportados por la Gerencia de Talento Humano con Retiros Temporales (vacaciones, suspensiones, licencias e incapacidades superiores a 5 días) o Retiro definitivo.

El Paz y Salvo que se emite por parte de la Oficina de TI sobre la Inactivación de control de acceso lógico sólo se hará efectivo si existe previa notificación por parte de la Gerencia de Talento Humano.

Respecto a la Inactivación de accesos a terceros, los supervisores de contrato deben notificar a la Oficina de TI el retiro oportuno. Mientras esta condición no se presente, dichos supervisores serán los responsables sobre los posibles accesos o actividades que se realicen con usuarios y claves de acceso de terceros en este periodo.

8. DEPURACIÓN DE USUARIOS:

La Oficina de TI, realizará mensualmente una depuración de usuarios que se encuentren inactivos en la red por un periodo mayor a tres (3) meses para el Dominio, Correo, SIARP, SISE, SAP y SNP.

PARTE II: ESTÁNDAR PARA EL CONTROL DE ACCESO FÍSICO

1. MARCO GENERAL

Todas las áreas e instalaciones de POSITIVA Compañía de Seguros S.A., que contengan o realicen procesamiento de información deben contar con controles adecuados para evitar el acceso físico no autorizado, el daño o interferencia a la información de la organización.

2. PARÁMETROS DE SEGURIDAD FÍSICA

- El perímetro del sitio que contiene instalaciones de procesamiento o información sensible debe tener solidez física (muros sólidos y puertas exteriores con mecanismos de control de acceso por medio de tarjetas con código de acceso o vigilantes).

- Las instalaciones físicas deben proporcionar una estructura que prevenga la observación audio y visual externa, y esté conforme con todos los códigos locativos de construcción del edificio para la estabilidad estructural (paredes externas, paredes internas, techos y puertas).

- se debe establecer un área de recepción con personal u otros medios para controlar el acceso físico al lugar o edificación; el acceso a los sitios y edificaciones debería estar restringido únicamente al personal autorizado;

- Las paredes que rodean las áreas sensibles deben extenderse desde el piso hasta el techo. Esta altura debe prevenir la entrada no autorizada y reducir al mínimo la contaminación del medio ambiente.

- Las áreas sensibles deben utilizar mecanismos apropiados del control de acceso (por ejemplo: cerraduras, alarmas, barras, cámaras de vigilancia, etc.), para prevenir el acceso no autorizado.

- Se debe instruir a todo el personal autorizado sobre los requisitos de seguridad del(as) área(s) a donde se va a ingresar y de los procedimientos de emergencia a ser aplicados. Se debe generar un registro de la capacitación, que evidencie su posterior verificación.

- Las instalaciones informáticas se deberían equipar con puertas de seguridad que se abran a través de medios de autenticación (tarjetas de aproximación, sistemas biométricos, claves de acceso) y que habiliten una alarma audible cuando permanezcan abiertas.

- El acceso principal y las áreas de atención al público de Positiva Compañía de Seguros S.A. deben contar con cámaras de seguridad o circuito cerrado de televisión (CCTV) para monitoreo del personal, funcionarios o visitantes que accedan a estas áreas. Los registros de monitoreo realizados por las cámaras de vigilancia o CCTV en las áreas de acceso principal y de atención al público de Positiva Compañía de Seguros S.A deben conservarse al menos por 8 meses.

- Los registros de las grabaciones deben conservarse en lugares adecuados para protegerlos del deterioro y de amenazas físicas y ambientales. Si las grabaciones se realizan en cintas de video o cassette, estos deben resguardarse en cajas fuertes o gabinetes con llave y restringir su acceso a personal no autorizado. Si las grabaciones son realizadas en formato digital, se deberían resguardar en servidores seguros con acceso lógico restringido y realizar copias de respaldo con igual o mayor

- Los equipos y dispositivos tecnológicos que son utilizados para soportar las funciones críticas del negocio deben estar en un área de acceso restringido y separadas del ambiente de las oficinas.

3 FUNCIONARIOS

- Cada ingreso o salida de Positiva Compañía de Seguros S.A., debe ser registrado por todos los funcionarios única y exclusivamente con la respectiva tarjeta de aproximación que le entrega Coordinación Administrativa o la Administración del edificio en portería.

- Ningún funcionario debe prestar su tarjeta de aproximación a otro funcionario ni a terceros o proveedores.

- Todo funcionario que reciba una visita de terceros debe efectuar acompañamiento desde el momento del ingreso del visitante hasta su retiro de las instalaciones de Positiva Compañía de Seguros S.A. Así mismo, debe firmar la ficha de ingreso que se asigna en la portería.

- Funcionario que no tenga tarjeta de acceso para ingresar a la dirección general o a las instalaciones que requieran autenticación como tarjetas de aproximación o lectores biométricos, deben ingresar siguiendo el mismo protocolo de visitantes.

- El uso del carné por parte de los funcionarios es obligatorio en las instalaciones de Positiva Compañía de Seguros S.A., y prioritaria en los centros de cómputo y áreas tecnológicas sensibles.

- Los funcionarios deben ingresar sólo a las áreas asignadas y autorizadas. En caso de requerir su ingreso a áreas sensibles, éste debe ser planeado y autorizado con anticipación, en todo caso debe estar acompañado por la persona responsable del área a donde ingresa.

- Se deben cumplir las políticas y estándares en referencia a la salida y entrada física de soportes de información (impresos, cintas y disquetes, CDS, etc.), así como de los responsables de cada área.

- El acceso físico a las oficinas en fines de semana y en horarios no hábiles debe registrase y controlarse de acuerdo con las políticas de seguridad de Positiva Compañía de Seguros S.A.

- Es muy importante que se ejecute el proceso de autorización establecido por parte de Positiva Compañía de Seguros S.A. y que se realicen revisiones aleatorias sobre las actividades que las personas desarrollan durante estos periodos de tiempo.

- Se debe establecer una lista de personal con ingreso permanente, la cual deberá ser aprobada exclusivamente por la Vicepresidencia Financiera y Administrativa de Positiva Compañía de Seguros S.A.

4. VISITANTES

- El ingreso a las áreas de Positiva Compañía de Seguros S.A., debe ser aprobado por un funcionario de la Compañía, quien será el responsable del visitante mientras permanezca en las instalaciones de Positiva Compañía de Seguros S.A.

- Todos los visitantes, sin excepción alguna deben identificarse y registrarse en el área de recepción de Positiva Compañía de Seguros S.A.

- Todo el personal de terceros contratados para ejecutar o realizar tareas dentro de las instalaciones, recintos u oficinas de Positiva Compañía de Seguros deben ser identificados como visitantes y deben cumplir con los controles de acceso físico e identificación establecidos.

- Todo visitante debe portar una identificación visible, con su respectiva tarjeta de aproximación que le permitirá dirigirse únicamente al piso donde está ubicada la persona que va a visitar, y una ficha que debe ser firmada por el funcionario quien recibió la visita y será entregada en la recepción al momento de la salida de las instalaciones de Positiva Compañía de Seguros S.A. previo reclamo de su documento que dejo al ingresar.

- Los visitantes que se encuentren sin acompañamiento o cualquiera que no lleve identificación visible, deben ser evacuados de dichas áreas y reportar al área de seguridad.

- Es responsabilidad de los funcionarios visitados, verificar que los dispositivos que los visitantes porten con ellos a Positiva Compañía de Seguros S.A. no lleven información de este.

- Se debe restringir el acceso a las áreas sensibles por parte del personal, de los proveedores o de mantenimiento, solo a los casos en que sea requerido y autorizado. Aun con acceso autorizado, se debe registrar el acceso y se deben controlar sus actividades por parte del funcionario visitado (especialmente en zonas de datos sensibles).

- Se deben cumplir las políticas y estándares en referencia a la salida y entrada física de soportes de información (impresos, cintas y disquetes, CDS, etc.), así como de los responsables de cada área.

4.1 Formato de acceso a visitantes

El formato para el ingreso de visitantes debe contener como mínimo los siguientes datos y debe ser diligenciado por el funcionario visitado:

- Nombre Entidad.
- Nombre funcionario a quien visita. Nombre del visitante.
- Autorizado por:
- Firma de funcionario a quien visitó.
- El piso u oficina para visitar.
- Fecha y hora de ingreso.
- Fecha y hora salida.

5. CONTROL DE ACCESO FÍSICO

Se deben considerar los siguientes aspectos de control:

- El acceso físico a áreas restringidas debe ser controlado. Visitantes y personal de servicio que no esté autorizado a entrar regularmente, deben ir acompañados por la persona responsable de su visita. El personal con autorización a entrar en las áreas restringidas debe ser informado por el administrador del área de los riesgos de seguridad implícitos.

- El acceso debe ser monitoreado regularmente para identificar accesos no autorizados y para confirmar que los controles de acceso son efectivos.

- Las áreas de empleados deben ser diseñadas para proteger la confidencialidad de la información y para controlar el acceso a los recursos de información de Positiva Compañía de Seguros S.A.

- Se deben descontinuar o modificar oportunamente los privilegios de acceso físico autorizados a la terminación, transferencia o cambio en las funciones de un individuo. Para esto la Gerencia de Recursos Humanos debe informar a la Oficina de TI periódicamente sobre los cambios realizados en el personal.

- Los controles de acceso a áreas restringidas deben ser cambiados periódicamente y cuando el control haya sido comprometido.

- Todo el personal que ingresa a las instalaciones de Positiva Compañía de Seguros S.A, debe utilizar la técnica de identificación definida en un lugar visible, si es empleado, tercero o contratista, debe portar el carné, si es visitante deberá portar la identificación que Positiva Compañía de Seguros así disponga.

- El personal de limpieza, de mantenimiento de las instalaciones y personal similar debe pasar por los mismos sistemas de control de acceso que los empleados, funcionarios, visitantes o usuarios, y deben cumplir con los protocolos y políticas de acceso definidas.

- Todos los equipos de cómputo y comunicaciones que sean o no propiedad de Positiva Compañía de Seguros S.A. (equipos en alquiler o propiedad de los terceros), sin excepción, deben ser registrados a su ingreso y salida de las instalaciones, como de cada una de las áreas restringidas a las que tuviese acceso.

- Todo el personal de Positiva Compañía de Seguros S.A. que realice actividades de prestación de servicios al público en general debe portar una identificación clara y visible como chalecos con el logo y nombre de Positiva Compañía de Seguros y carné de identificación de la entidad.

- Se debe restringir el acceso de personas no autorizadas a los mostradores, recepciones y oficinas que prestan servicios a los clientes. Para ello, se debe contar con puertas con acceso que usen llaves, tarjetas de aproximación o controles biométricos.

- Todos los envíos, entregas y artículos personales transportados hacia y desde las instalaciones de Positiva Compañía de Seguros S.A, deben estar sujetos a inspección por parte del personal de seguridad física o vigilancia de Positiva Compañía de Seguros S.A.

- Se debe usar un sistema de control de acceso que deje registro individual de las entradas y salidas de las áreas restringidas.

- Se deben realizar pruebas periódicas a todos los sistemas de seguridad presentes en Positiva Compañía de Seguros S.A.

- Se debe conceder el acceso controlado al personal de servicio de soporte en áreas sensibles o críticas.

6. SEGURIDAD DE OFICINAS, RECINTOS E INSTALACIONES

- La dirección física de las áreas de Positiva Compañía de Seguros S.A como centros de cómputo, tesorería y proveedores externos que manejen información de este, debe ser confidencial y sólo se divulgará a aquellos empleados y terceros (contratistas, proveedores y practicantes) de Positiva Compañía de Seguros S.A. que así lo requieran.
- Toda entrada o salida a instalaciones que requieran autenticación como tarjetas de aproximación o lectores biométricos debe ser marcada por parte de funcionarios o visitantes, así la puerta esté abierta.

- Se debe realizar revisiones periódicas de los niveles de acceso y autorizaciones a las áreas de seguridad de Positiva Compañía de Seguros S.A., esto aplica a todo el territorio nacional. Se dejarán los registros necesarios que evidencien que dichos procesos funcionan correctamente. De igual forma se corroborará a través de revisiones periódicas de auditoría.

- Los directorios telefónicos internos que identifican localizaciones de las instalaciones del centro de cómputo o de las áreas sensibles o críticas de Positiva Compañía de Seguros S.A no deben ser fácilmente accesibles por el personal no autorizado.

- Las áreas de Positiva Compañía de Seguros S.A que involucren riesgo de acceso o daño a la información que administran, deberían estar separadas de zonas o de áreas que almacenen

líquidos inflamables o estén en riesgo de inundaciones e incendios. Por tanto, no deben estar ubicadas cerca de un sótano o en un último piso, ni tampoco debe contar con ventanas al exterior.

- Las áreas de Positiva Compañía de Seguros S.A. que involucren riesgo de acceso ó daño a la información que administran, deben estar provistas de sistemas de control de acceso, monitoreo de área, sistemas de detección, control de incendios, detección de intrusos y todos aquellos sistemas que garanticen la continuidad del servicio y seguridad de la información.

- Todas las actividades de instalaciones técnicas o materiales que se realicen en las áreas de Positiva Compañía de Seguros S.A. que procesen información deben seguir los estándares correspondientes y asignación de espacio, ubicación y demás requerimientos físicos una vez hayan tenido previa autorización por el Administrador del Centro de Cómputo.
  Las actividades de mantenimiento preventivo o correctivo en las áreas de Positiva Compañía de Seguros S.A. que involucren riesgo de acceso de la información que administran deben ser coordinadas por el Administrador del área correspondiente.

- Se deben programar y realizar pruebas del funcionamiento de manera periódica a todos los sistemas de control de acceso y de seguridad física en las áreas de Positiva Compañía de Seguros S.A. que involucren riesgo de acceso a la información. Estas pruebas deben ser realizadas por los administradores de área correspondientes o por los proveedores de servicios cuando las instalaciones sean externas a Positiva Compañía de Seguros S.A.

- Las instalaciones, oficinas y recintos de Positiva Compañía de Seguros que ofrezcan servicios y productos a sus clientes, deberían contar con los elementos mínimos de accesibilidad para personas con discapacidad o movilidad reducida tales como:

    - Ascensores (para edificios que cuenten con más de un nivel).
    - Rampas de acceso a las instalaciones y oficinas de atención al público.
    - Puertas de acceso adecuadas para la circulación de sillas de ruedas. o Sitios de parqueo para personas con discapacidad o Pisos bien materializados, para evitar caídas y tropiezos.
    - Las escaleras deben contar con pasamanos a alturas adecuadas.
    - Los baños deberían contar con espacio suficiente para ubicar la silla de ruedas o muletas
    - al costado de los sanitarios.

- Cualquier movimiento de medios magnéticos de las áreas de Positiva Compañía de Seguros S.A. que involucren riesgo de acceso a la información debe ser reportado, registrado y coordinado con el administrador del área correspondiente. Se debe utilizar el estándar VA-OD-EMMI-01 estándar para el manejo de medios de la información e intercambio de la información definido por Positiva Compañía de Seguros S.A.

- Todos los empleados y terceros (contratistas, proveedores) que tengan acceso a las áreas de Positiva Compañía de Seguros S.A. donde se procesa información, son responsables por el buen funcionamiento y estado de los sistemas de información e instalaciones.

- Se debe tener un inventario específico de las áreas de Positiva Compañía de Seguros S.A. que procesan, almacenan o transmiten información, así como de los medios y equipos asignados, al igual que un procedimiento para destruir o reutilizar los mismos.

- Las áreas de Positiva Compañía de Seguros S.A. que procesan almacenan o transmiten información se deben equipar con sistemas de alarmas físicos. Cuando están activados, estos sistemas deben alertar automáticamente al personal apropiado.

- Las entradas restringidas y salidas de emergencia deben ser protegidas con sistemas de alarma de emergencia.

- Los recursos tecnológicos críticos que procesan almacenan o transmiten información no deben tener acceso público. Se deben localizar en lugares o zonas alejadas al público o personal no autorizado. En lo posible las áreas de oficina no deben permanecer solas, especialmente durante horas de almuerzo en que existen mayores riesgos de pérdida de elementos.

- Las puertas y ventanas deben quedar bloqueadas cuando no hay vigilancia. Debería considerarse la posibilidad de agregar protección externa a las ventanas, en particular las que se encuentran al nivel del suelo.

- Los recursos de procesamiento de la información de Positiva Compañía de Seguros S.A. deben estar separados de los recursos de procesamiento de terceros (contratistas y proveedores).

7. LOCALIZACIÓN DE IMPRESORAS, COPIADORAS Y MÁQUINAS DE FAX

- Para prevenir el acceso, la duplicación y la transmisión no autorizada de información confidencial, todas las impresoras, copiadoras, y máquinas de fax se deben situar en áreas seguras.

- los documentos que contengan información sensible o clasificada se deberían retirar inmediatamente de las impresoras.

- No se debe dejar información sensible o crítica en los dispositivos de impresión como copiadoras, impresoras y máquinas de fax ya que se puede permitir el acceso de personal no autorizado.

8. CONTROLES AMBIENTALES

- Las áreas de procesamiento de datos deben estar protegidas de amenazas potenciales como fuego, humo, agua, polvo, vibraciones, agentes químicos o radiaciones electromagnéticas.

- Se deberían instalar dispositivos de detección y protección adecuados, por ejemplo: controles de temperatura y humedad, detectores y alarmas de calor, humo y humedad; sistemas de extinción de incendios; salidas de emergencia; suelo falso para respiración de equipos y cableado, además equipo de extinción de incendios.

- Los materiales combustibles o peligrosos se deberían almacenar a una distancia prudente de las áreas seguras o sensibles. Los suministros de oficina y otros materiales, no se deben almacenar en áreas seguras.

- El papel y los combustibles deben ser almacenados en lugares aislados en contenedores y en pequeñas cantidades.

- Los controles de seguridad física y ambiental deben ser acordes con las regulaciones existentes de fuego y seguridad, así como los requerimientos contractuales de los seguros contratados.

9. SEGUROS

- Deben existir seguros para proteger las instalaciones, áreas, equipos y elementos ubicados en Positiva Compañía de Seguros S.A. que procesan, almacenan, o transmiten información crítica. Así mismo, los terceros (proveedores y contratistas), que almacenen, transmitan o procesen información de Positiva Compañía de Seguros S.A. deben contar con este tipo de seguros.

- Los seguros deben considerar el cubrimiento mínimo de: los costos de reposición de recursos informáticos, costos de interrupción del negocio y reembolso a Positiva Compañía de Seguros S.A., por costos en la restauración de las operaciones y pérdidas de ganancias asociadas.

- Los contratos con proveedores que tengan acceso a la información de Positiva Compañía de Seguros S.A. deben contemplar pólizas de cumplimiento y confidencialidad.

10. TRABAJO EN ÁREAS SEGURAS

Se consideran áreas seguras cualquiera de los lugares o zonas de Positiva Compañía de Seguros, en la cual se procese, transmita o almacene información crítica o sensible.

Se debe solicitar permiso de acceso de los empleados y terceros (proveedores y contratistas) que realicen trabajos o actividades en las áreas seguras definidas por Positiva Compañía de seguros S.A.

La solicitud de autorización de acceso a las áreas seguras debe contar como mínimo con la siguiente información por cada empleado:

- Fecha de solicitud
- Nombres y Apellidos de empleado
- N° de identificación
- Fecha de ingreso
- Descripción de las funciones a realizar
- Tiempo estimado de la realización de actividades
- Detalle de los equipos o dispositivos que se ingresan
- El personal interno o externo que realiza trabajos para Positiva Compañía de Seguros S.A. solo debe conocer la existencia de las áreas seguras con base en la necesidad de sus funciones.

- Se debe supervisar el trabajo en áreas seguras por motivos de seguridad para evitar actividades maliciosas tales como robo, interferencia, destrucción, alteración, acceso y distribución no autorizada de información.
- No se permite el acceso de equipos de fotografía, video, audio, USB u otras formas de registro y almacenamiento de información a las áreas de Positiva Compañía de Seguros S.A. que procesan, almacenan o transmiten información, salvo con autorización especial.

11. INGRESO AL CENTRO DE CÓMPUTO Y ÁREAS TECNOLÓGICAS SENSIBLES

- Solo el personal autorizado (interno o externo) por la Oficina de TI podrá tener acceso a las áreas donde se encuentren ubicados los sistemas de información dispositivos de almacenamiento, dispositivos de comunicación y otras áreas tecnológicas definidas como sensibles por Positiva Compañía de Seguros S.A.

- Los accesos a estas áreas deben ser controlados, autorizados y registrados, mediante bitácoras o registros que demuestren la trazabilidad de los sitios e información a que se tuvo acceso.

- Las autorizaciones deben efectuarse sólo con propósitos específicos y definidos con anterioridad. Se exceptúan accesos por fuerza mayor, pero deben ser autorizados y registrados por funcionarios directivos del área a donde se ingresa. El ingreso debe contar con acompañamiento y registro en las bitácoras correspondientes.

- Todo funcionario que ingrese al centro de cómputo así esté autorizado, debe registrarse mediante el sistema de autenticación instalado (tarjeta de aproximación o biométrico), es decir, si ingresan dos funcionarios autorizados los dos deben marcar el ingreso y la salida correspondiente.

- Todo visitante o funcionario no autorizado que ingrese al centro de cómputo debe registrarse en las bitácoras correspondientes y debe contar con acompañamiento.

- A los centros de cómputo y áreas tecnológicas sensibles los funcionarios y visitantes no deben ingresar dispositivos como videograbadoras, cámaras fotográficas, grabadoras, sniffers, analizadores de datos, celulares con cámara, iPOD´s, USB´s a menos que exista una autorización formal de la Oficina de TI y con propósitos específicos definidos con anterioridad.

- Todo el personal de mantenimiento que tenga acceso a los centros de cómputo y áreas tecnológicas sensibles deben estar acompañados y portar identificación.

4.11 ÁREAS DE ENTREGA Y RECIBO DE ELEMENTOS, EQUIPOS O INFORMACIÓN

- Se debe restringir el acceso desde el exterior a las áreas de entrega y recibo de elementos, equipos e información dispuesta por Positiva Compañía de Seguros.

- No se deben almacenar en las áreas de entrega y recibo equipos o medios de TI que puedan contener información sensible y todo equipo nuevo o usado de TI en tránsito, tiene que almacenarse apropiadamente y mantenerse en zonas seguras en todo momento.

- Todos los elementos, equipos o información que realicen su ingreso por las áreas de entrega y recibo se deben registrar.

- Las áreas de entrega y recibo de elementos se deberían diseñar manera tal que los suministros puedan ser descargados sin que el personal que realiza la entrega acceda a otros sectores del edificio.

- Se debe Inspeccionar todo el material entrante para descartar peligros potenciales antes de ser trasladado a zonas de almacenamiento o el lugar de uso.

7. PROCESOS Y/O SUBPROCESO ASOCIADO

- Gestión de Servicios de TI o Control de Servicios de TI

8. RESPONSABLES

- Oficina de TI o Profesional Especializado.

9. TABLA DE DOCUMENTOS Y/O FORMATOS ASOCIADOS

Documentos y/o Formatos Asociados		
N°	**Nombre del Documento y/o Formato asociado**	**Código del Documento sin versión**
1	Solicitud de Usuarios	APO-12-4-1-FR03

10. CONTROL DE CAMBIOS

Control de Cambios				
N°	**Descripción del Cambio**	**Fecha del Cambio**	**Quien Aprueba el Cambio**	**Versión Anterior**
1	Se ajusta el manual de acuerdo con la reestructuración que tuvo la Compañía a finales del año 2016.	09/06/2017	Jefe OTI	n/a
2	Se ajusta el alcance de roles y perfiles describiendo los privilegios de acceso establecidos para las bases de datos y servidores, se actualizó en el manual el tiempo de inactivación de las sesiones para los sistemas diferentes a SAP, y se incluyen parámetros para VPN y tiempos de inactividad.	11/10/2017	Jefe OTI	1
3	Dado a que para el cifrado de archivos en SNP se requiere de un usuario que no caduque puesto que afectaría mensualmente el cargue de archivos, se genera actualización del manual de control de acceso aclarando lo anterior.	31/01/2018	Jefe OTI	2
4	Se incluye ítem sobre el historial de contraseñas, y se actualiza el ítem relacionado con la duración del bloqueo de contraseñas.	26/03/2018	Jefe OTI	3
5	Se ajustan algunos conceptos respecto al manejo del control de acceso de la Compañía.	25/04/2018	Jefe OTI	4
6	Se actualiza el Manual respecto al manejo de las cuentas consideradas como privilegiadas.	27/07/2018	Jefe OTI	5
7	Se Ajusta la definición sobre cuentas privilegiadas.	01/08/2018	Jefe OTI	6
8	Se ajustan los numerales 1.3.4 y 1.3.7 frente a la entrega de usuarios y contraseñas privilegiadas.	25/02/2019	Jefe OTI	7
9	Se ajusta el numeral 1.1 incluyendo un nuevo aparte de configuración de contraseña para dominio y sus aplicaciones enlazadas.	09/05/2019	Jefe OTI	8
10	Se ajustan definiciones de periodicidad de depuración y periodicidad de informe de usuarios roles y perfiles.	12/08/2019	Jefe OTI	9

BIBLIOGRAFÍA

- INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Information Technology. Service Management. Part 1: Specification. Geneva: ISO, 2005, 16 p. (ISO/IEC 20000-1).

- INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Information Technology - Service Management - Part 2: Code of Practice. Geneva: ISO, 2005, 34 p. (ISO/IEC 20000 - 2:2005 (E)).

- INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Information Technology. Security Techniques. Code of Practice for Information Security Management. Geneva: ISO/IEC, 2005, 107 p (ISO / IEC 27002:2005 (E)).